Aug-01-22

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®

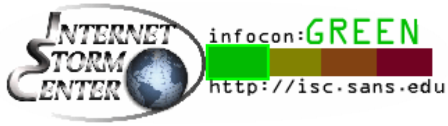
CYBER WEEKLY AWARENESS REPORT

August 1, 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

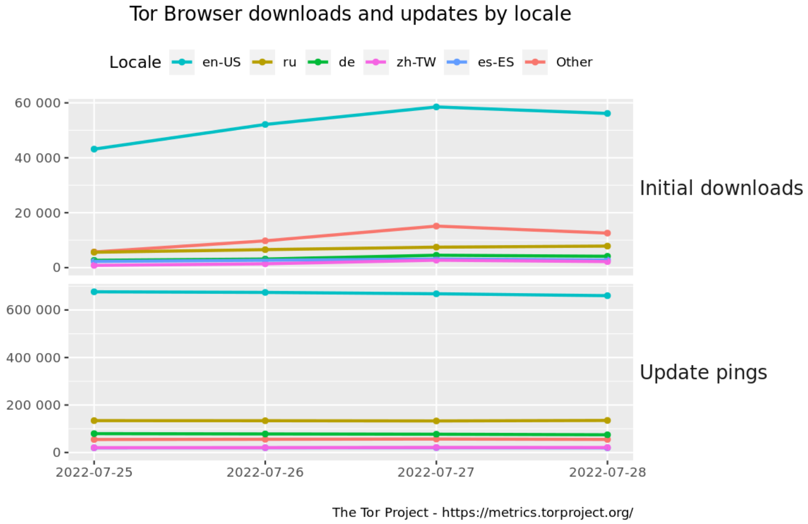


The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

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

* Threat Actors Pivot Around Microsoft's Macro-Blocking In Office
* JPMorgan, UBS Among Trio Accused Of Shoddy ID Theft Protection
* Ransomware Hit The American Dental Association
* BreachForums Booms On The Back Of Billion Record Chinese Data Leak
* US Court System Suffered Incredibly Significant Attack - Sealed Files At Risk
* US Puts $10 Million Bounty On North Korean Cyber Crews
* FileWave Fixes Bugs That Left 1,000+ Orgs Open To Ransomware
* Microsoft Exposes Tactics Of European Mercenary Spyware Broker
* Inside The Energy Department's 10-Year Plan To Reshape Cybersecurity In The Sector
* Discovery Of New UEFI Rootkit Exposes An Ugly Truth: The Attacks Are Invisible To Us
* Woman Tells Congress What It's Liked To Be Hacked By NSO's Pegasus
* Messaging Apps Tapped As Platform For Cybercriminal Activity
* Time Between Vulnerability Disclosures To Exploits Is Shrinking
* T-Mobile To Pay $500 Million For One Of The Largest Data Breaches In US History
* Russia Is Quietly Ramping Up Its Internet Censorship Machine
* LockBit Ransomware Claims Pwn Of Italy's Tax Agency
* European Cops Helped 1.5 Million Decrypt Ransomwared Computers
* Hardcoded Password In Confluence Has Been Leaked On Twitter
* DIY Collective Embeds Abortion Pill Onto Business Cards, Distributes Them At Hacker Conferences
* DoJ Approves Google's Acquisition Of Mandiant
* Microsoft Again Reverses Course, Will Block Macros By Default
* Didi Slapped With $1.1B Fine For Breaching China Data Security Laws
* Elon Musk's Tesla Sells Most Of Its Bitcoin Holdings
* Jan. 6 Committee Lays Out How Trump Let Capitol Riot Rage For Three Hours While He Watched Fox
* US Spots Another 20 Malware Strains Targeting Ukraine

Krebs on Security

* 911 Proxy Service Implodes After Disclosing Breach
* Breach Exposes Users of Microleaves Proxy Service
* A Retrospective on the 2015 Ashley Madison Breach
* Massive Losses Define Epidemic of 'Pig Butchering'
* A Deep Dive Into the Residential Proxy Service '911'
* Why 8kun Went Offline During the January 6 Hearings
* Microsoft Patch Tuesday, July 2022 Edition
* Experian, You Have Some Explaining to Do
* The Link Between AWM Proxy & the Glupteba Botnet
* Meet the Administrators of the RSOCKS Proxy Botnet

LATEST NEWS

Dark Reading

* AWS Focuses on Identity Access Management at re:Inforce
* Attackers Have 'Favorite' Vulnerabilities to Exploit
* ICYMI: Dark Web Happenings Edition With Evil Corp., MSP Targeting & More
* Why Bug-Bounty Programs Are Failing Everyone
* Security Teams Overwhelmed With Bugs, Bitten by Patch Prioritization
* Amazon Adds Malware Detection to GuardDuty TDR Service
* Big Questions Remain Around Massive Shanghai Police Data Breach
* Malicious npm Packages Scarf Up Discord Tokens, Credit Card Info
* 3 Tips for Creating a Security Culture
* Patch Now: Atlassian Confluence Bug Under Active Exploit
* What the White House's Cybersecurity Workforce Plan Should Look Like
* APT-Like Phishing Threat Mirrors Landing Pages
* What Women Should Know Before Joining the Cybersecurity Industry
* 1,000s of Phishing Attacks Blast Off From InterPlanetary File System
* In a Post-Macro World, Container Files Emerge as Malware-Delivery Replacement
* When Human Security Meets PerimeterX
* OneTouchPoint, Inc. Provides Notice of Data Privacy Event
* Overcoming the Fail-to-Challenge Vulnerability With a Friendly Face
* Multiple Windows, Adobe Zero-Days Anchor Knotweed Commercial Spyware
* US Offers $10M Double-Reward for North Korea Cyberattacker Info

The Hacker News

* Australian Hacker Charged with Creating, Selling Spyware to Cyber Criminals
* Gootkit Loader Resurfaces with Updated Tactic to Compromise Targeted Computers
* Stop Putting Your Accounts At Risk, and Start Using a Password Manager
* Microsoft Links Raspberry Robin USB Worm to Russian Evil Corp Hackers
* North Korean Hackers Using Malicious Browser Extension to Spy on Email Accounts
* CISA Warns of Atlassian Confluence Hard-Coded Credential Bug Exploited in Attacks
* Over a Dozen Android Apps on Google Play Store Caught Dropping Banking Malware
* Dahua IP Camera Vulnerability Could Let Attackers Take Full Control Over Devices
* Researchers Warns of Increase in Phishing Attacks Using Decentralized IPFS Network
* How to Combat the Biggest Security Risks Posed by Machine Identities
* Spanish Police Arrest 2 Nuclear Power Workers for Cyberattacking the Radiation Alert System
* Latest Critical Atlassian Confluence Vulnerability Under Active Exploitation
* Google Delays Blocking 3rd-Party Cookies in Chrome Browser Until 2024
* Hackers Opting New Attack Methods After Microsoft Blocked Macros by Default
* Microsoft Uncovers Austrian Company Exploiting Windows and Adobe Zero-Day Exploits

LATEST NEWS

Security Week

* Microsoft Connects USB Worm Attacks to 'EvilCorp' Ransomware Gang
* Malicious Macro-Enabled Docs Delivered via Container Files to Bypass Microsoft Protections
* Governments Ramp Up Demands for User Info, Twitter Warns
* N Korean APT Uses Browser Extension to Steal Emails From Foreign Policy, Nuclear Targets
* OneTouchPoint Discloses Data Breach Impacting Over 30 Healthcare Firms
* Major Cybersecurity Breach of US Court System Comes to Light
* GitHub Improves npm Account Security as Incidents Rise
* Calls Mount for US Gov Clampdown on Mercenary Spyware Merchants
* Cybersecurity Growth Investment Flat, M&A Activity Strong for 2022
* Crackdown on BEC Schemes: 100 Arrested in Europe, Man Charged in US
* House Passes Cybersecurity Bills Focusing on Energy Sector, Information Sharing
* Securing Smart Cities from the Ground Up
* Exploitation of Recent Confluence Vulnerability Underway
* Moxa NPort Device Flaws Can Expose Critical Infrastructure to Disruptive Attacks
* France Closes 'Cookies' Case Against Facebook
* Microsoft: Attackers Increasingly Using IIS Extensions as Server Backdoors
* Victim of Private Spyware Warns It Can be Used Against US
* Nuki Smart Lock Vulnerabilities Allow Hackers to Open Doors
* Microsoft Catches Austrian Company Exploiting Windows, Adobe Zero-Days
* HUMAN Security and PerimeterX Merge on Mission to Combat Bots
* Mailing List Provider WordFly Scrambling to Recover Following Ransomware Attack
* IBM Security: Cost of Data Breach Hitting All-Time Highs
* What the Titanic Can Teach Us About Fraud?
* US Offers $10 Million for Information on North Korean Hackers
* Dozens of 'Luca Stealer' Malware Samples Emerge After Source Code Made Public
* AWS Announces Enhancements to Cloud Security, Privacy, Compliance

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Happy 23rd Annual SysAdmin Day from KnowBe4!
* Your KnowBe4 Fresh Content Updates from July 2022
* Phishing-Based Data Breaches Take 295 Days to Contain and Breach Costs Soar to $4.91 Million
* Beware of Sophisticated Malicious USB Keys
* Microsoft 365 Users are Once Again the Target of Phishing Scams using Fake Voice Mail Messages
* Hackers Use Free Email Accounts from QuickBooks to Launch Spoofed Phishing Attacks
* Spear Phishing Campaign Targets Facebook Business Accounts
* IBM: Phishing is the Most Common Way to Gain Access to Victim Networks
* KnowBe4 Top-Clicked Phishing Email Subjects for Q2 2022 [INFOGRAPHIC]
* Nearly Half of Organizations Have Experienced Vishing

ISC2.org Blog

* Latest Cyberthreats and Advisories - July 29, 2022
* (ISC)&sup2; and Others Commit to Closing the Cybersecurity Workforce Gap While at the White House
* Latest Cyberthreats and Advisories - July 21, 2022
* APAC Security Leaders Come Together at SECURE Singapore
* #ISC2Congress: Piloting Teams While Under Pressure - Carey Lohrenz Will Speak as an (ISC)&sup2; Keyno

HackRead

* Alleged ShinyHunters Hacker Group Member Arrested
* 911 (911.re) Proxy Service Shuts Down After Confirming Security Breach
* LofyLife: Malicious npm Packages Used in Siphoning Off Discord Tokens, Card Data
* Telegram and Discord Bots Delivering Infostealing Malware
* Microsoft: Hackers are Using Malicious IIS Extensions to Backdoor Exchange Servers
* With $11.5M In Funding, Naoris Protocol Will Use Blockchain & Decentralization To Plug Web3 Security
* Ways Hackers Can Steal Information from Your Device

Koddos

* Alleged ShinyHunters Hacker Group Member Arrested
* 911 (911.re) Proxy Service Shuts Down After Confirming Security Breach
* LofyLife: Malicious npm Packages Used in Siphoning Off Discord Tokens, Card Data
* Telegram and Discord Bots Delivering Infostealing Malware
* Microsoft: Hackers are Using Malicious IIS Extensions to Backdoor Exchange Servers
* With $11.5M In Funding, Naoris Protocol Will Use Blockchain & Decentralization To Plug Web3 Security
* Ways Hackers Can Steal Information from Your Device

LATEST NEWS

Naked Security

* How to celebrate SysAdmin Day!
* S3 Ep93: Office security, breach costs, and leisurely patches [Audio + Text]
* Critical Samba bug could let anyone become Domain Admin - patch now!
* Mild monthly security update from Firefox - but update anyway
* T-Mobile to cough up $500 million over 2021 data breach
* Office macro security: on-again-off-again feature now BACK ON AGAIN!
* Apple patches "0-day" browser bug fixed 2 weeks ago in Chrome, Edge
* S3 Ep92: Log4Shell4Ever, travel tips, and scamminess [Audio + Text]
* Last member of Gozi malware troika arrives in US for criminal trial
* 8 months on, US says Log4Shell will be around for "a decade or longer"

Threat Post

* Malicious Npm Packages Tapped Again to Target Discord Users
* Threat Actors Pivot Around Microsoft's Macro-Blocking in Office
* Messaging Apps Tapped as Platform for Cybercriminal Activity
* Novel Malware Hijacks Facebook Business Accounts
* Phishing Attacks Skyrocket with Microsoft and Facebook as Most Abused Brands
* IoT Botnets Fuels DDoS Attacks - Are You Prepared?
* Why Physical Security Maintenance Should Never Be an Afterthought
* Hackers for Hire: Adversaries Employ 'Cyber Mercenaries'
* Conti's Reign of Chaos: Costa Rica in the Crosshairs
* Magecart Serves Up Card Skimmers on Restaurant-Ordering Systems

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

* Microsoft's .NET Core 3.1 nears the end
* AWS revenue jumps 33%, but growth slows
* BrandPost: Initial Results of the Intel and Aible Benchmark and Case Studies Report Released
* BrandPost: Cloud Migration Accelerates as Confidence Grows
* It's past time to figure out cross-cloud security
* What is TOML? An easier way to configure Python apps and more
* Jetpack Compose 1.2 packs text improvements
* What is Quarto? RStudio rolls out next-generation R Markdown
* Carbon language aims to be a better C++
* How to test minimal APIs in ASP.NET Core 6

C4ISRNET - Media for the Intelligence Age Military

* Army pursues shared software among uncrewed vehicles
* Meet Britain's new ship that will test autonomous and lethal technologies
* Biden pick for Pentagon acquisitions role vows to cut weapons system costs
* Saltzman nominated to lead Space Force
* They're 'all different': Air Force adviser says services diverge on JADC2
* The hypersonic race: A case for guarded optimism
* US Army sets timeline for demo of new, hard-to-detect mobile command post
* Battle from the skies: How aviation advances empower the Corps' new combat plan
* Biden presses for chips legislation in meeting with Pentagon's No. 2 and Lockheed
* Leonardo DRS chief talks taking out drone swarms and what integrated sensing has in common with Tesla

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

* 2022 0-day In-the-Wild Exploitation&hellip;so far
* The curious tale of a fake Carrier.app

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.

* Arab Security Cyber Wargames 2022 Qualifications
* corCTF 2022
* T3N4CI0US CTF - Escape
* DEF CON CTF 2022
* SHELLCTF 2022
* WMCTF2022
* Midnight Sun CTF 2022 Finals
* Hacker's Playground 2022
* CTFZone 2022
* HITB SECCONF CTF 2022

VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1
* Napping: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

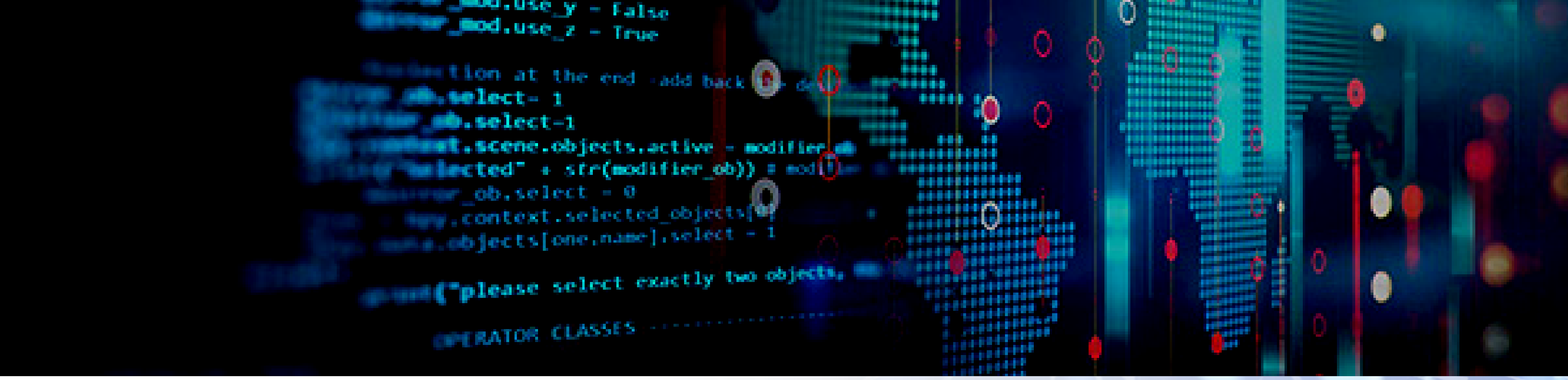
* Faraday 4.0.4
* Wireshark Analyzer 3.6.7
* Clam AntiVirus Toolkit 0.105.1
* Logwatch 7.7
* AIEngine 2.2.0
* Global Socket 1.4.38
* Suricata IDPE 6.0.6
* GNU Privacy Guard 2.3.7
* GNU Privacy Guard 2.2.36
* Falco 0.32.1

Kali Linux Tutorials

* Trufflehog : Find Credentials All Over The Place
* Bypass-Url-Parser : Tool That Tests Many URL Bypasses To Reach A 40X Protected Page
* WebView2-Cookie-Stealer : Attacking With WebView2 Applications
* Tofu : Windows Offline Filesystem Hacking Tool For Linux
* Frostbyte : FrostByte Is A POC Project That Combines Different Defense Evasion Techniques
* Admin-Panel_Finder : A Burp Suite Extension That Enumerates Infrastructure And Application Admin Inte
* Gshell : A Flexible And Scalable Cross-Plaform Shell Generator Tool
* DOMDig : DOM XSS Scanner For Single Page Applications
* ConfluencePot : Simple Honeypot For Atlassian Confluence (CVE-2022-26134)
* SharpEventPersist : Persistence By Writing/Reading Shellcode From Event Log

GBHackers Analysis

* Critical SonicWall Vulnerability Allows SQL Injection - Patch Now!
* Security Giant Entrust Hacked - Attackers Stole Data From Internal Systems
* Cisco Nexus Dashboard Flaw Let Remote Attacker Execute Arbitrary Commands
* VMware vCenter Server Flaw Let Attacker Exploit to Perform Elevate Privileges Attack
* Critical Fortinet Flaws Patched - Following Products Affected


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

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Introducing the Enterprise Cloud Forensics & Incident Response Poster
* FOR585 Course Animation: Potential Crime Scene iPhone and Android
* FOR585 Course Animation: IMEI vs GSM
* FOR585 Course Animation: How WAL Gets Populated Initial State

Defcon Conference

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

Hak5

* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Hacking Air-Gapped Machines Over SATA; New Trend In Ransomware - ThreatWire
* Installing and Configuring Kismet Pineapple Mk7

The PC Security Channel [TPSC]

* How to know if your PC is hacked? Suspicious Network Activity 101
* Windows Defender: Test vs Ransomware 2022

Eli the Computer Guy

* eBeggar Wednesday - MARVEL PHASE 5 SUCKS
* What is a Router?
* SILICON DERBY - Life in the fast lane...
* eBeggar Wednesday - NETFLIX KEEPS FAILING

Security Now

* The MV720 - MS Office VBA macros, Win 11 security changes, start button failure
* RetBleed - Facebook encrypted URLs, cracking Lockdown Mode, ClearView AI resistance, Roskomnadzor

Troy Hunt

* Weekly Update 306

Intel Techniques: The Privacy, Security, & OSINT Show

* 272-Processor Attacks Explained
* 271-OSINT Tool Updates II

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Transposh WordPress Translation 1.0.8.1 Remote Code Execution
* Transposh WordPress Translation 1.0.8.1 SQL Injection
* Transposh WordPress Translation 1.0.8.1 Improper Authorization
* Geonetwork 4.2.0 XML Injection
* Transposh WordPress Translation 1.0.8.1 Information Disclosure
* Crime Reporting System 1.0 Cross Site Scripting
* Transposh WordPress Translation 1.0.8.1 Cross Site Request Forgery
* rpc.py 0.6.0 Remote Code Execution
* Transposh WordPress Translation 1.0.7 Incorrect Authorization
* Dingtian-DT-R002 3.1.276A Authentication Bypass
* Transposh WordPress Translation 1.0.7 Cross Site Scripting
* Transposh WordPress Translation 1.0.7 Cross Site Scripting
* WordPress WP-UserOnline 2.87.6 Cross Site Scripting
* Loan Management System 1.0 Cross Site Scripting
* Loan Management System 1.0 SQL Injection
* Roxy-WI Remote Command Execution
* Hospital Information System 1.0 SQL Injection
* Garage Management System 1.0 Shell Upload
* Expert X Jobs Portal And Resume Builder 1.0 SQL Injection
* PCProtect Endpoint 5.17.470 Tampering / Privilege Escalation
* Patlite 1.46 Buffer Overflow
* Marty Marketplace Multi Vendor Ecommerce Script 1.2 SQL Injection
* Backdoor.Win32.Eclipse.h MVID-2022-0625 Hardcoded Credential
* Chrome Scope Break
* Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) Remote Root

CXSecurity

* Roxy-WI Remote Command Execution
* Sourcegraph gitserver sshCommand Remote Command Execution
* JBOSS EAP/AS 6.x Remote Code Execution
* Exploit mktba 4.2 Arbitrary File Upload
* WiFi Mouse 1.7.8.5 Remote Code Execution
* Kitty 0.76.0.8 Stack Buffer Overflow
* phpIPAM 1.4.5 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

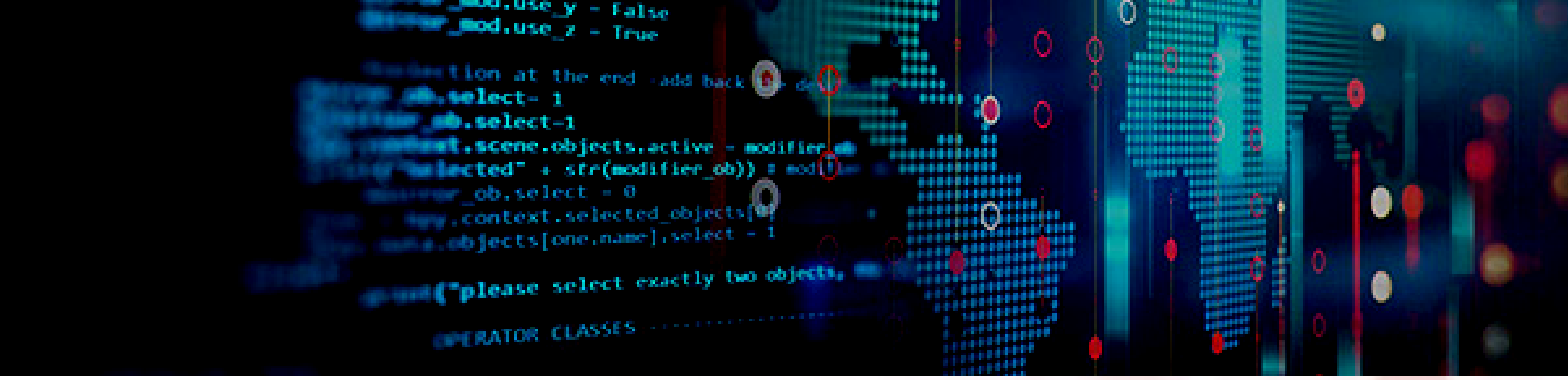
* [webapps] WordPress Plugin WP-UserOnline 2.87.6 - Stored Cross-Site Scripting (XSS)
* [remote] Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) - Remote Code Execution
* [webapps] Carel pCOWeb HVAC BACnet Gateway 2.1.0 - Directory Traversal
* [local] Asus GameSDK v1.0.0.4 - 'GameSDK.exe' Unquoted Service Path
* [webapps] Dingtian-DT-R002 3.1.276A - Authentication Bypass
* [remote] rpc.py 0.6.0 - Remote Code Execution (RCE)
* [webapps] Geonetwork 4.2.0 - XML External Entity (XXE)
* [webapps] WordPress Plugin Visual Slide Box Builder 3.2.9 - SQLi
* [webapps] OctoBot WebInterface 0.4.3 - Remote Code Execution (RCE)
* [webapps] CodoForum v5.1 - Remote Code Execution (RCE)
* [local] Dr. Fone 4.0.8 - 'net_updater32.exe' Unquoted Service Path
* [webapps] Magnolia CMS 6.2.19 - Stored Cross-Site Scripting (XSS)
* [local] Kite 1.2021.610.0 - Unquoted Service Path
* [remote] IOTransfer 4.0 - Remote Code Execution (RCE)
* [remote] Nginx 1.20.0 - Denial of Service (DOS)
* [remote] WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)
* [webapps] Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)
* [webapps] WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scriptin
* [webapps] WordPress Plugin Weblizar 8.9 - Backdoor
* [webapps] SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)
* [webapps] SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)
* [webapps] Old Age Home Management System 1.0 - SQLi Authentication Bypass
* [webapps] ChurchCRM 4.4.5 - SQLi
* [remote] Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)
* [webapps] phpIPAM 1.4.5 - Remote Code Execution (RCE) (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
```

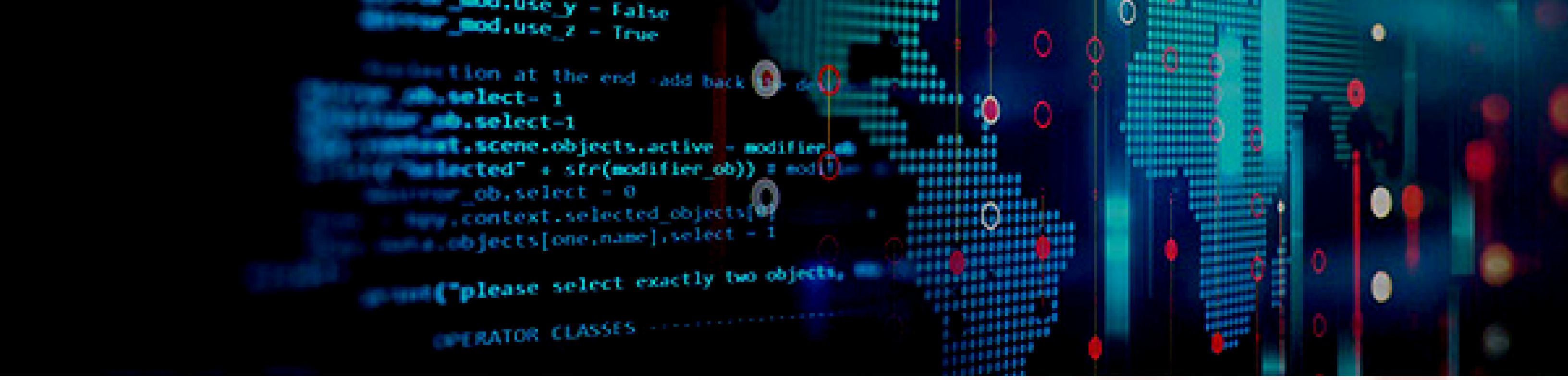
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://owwa.gov.ph/0x.html
https://owwa.gov.ph/0x.html notified by 0xJoshua
http://www.pasanghospital.go.th/404.php
http://www.pasanghospital.go.th/404.php notified by 0x1998
http://sipendi.pta-palangkaraya.go.id/readme.html
http://sipendi.pta-palangkaraya.go.id/readme.html notified by WE WILL BE BACK SOON WITH THE BIGGEST CYBER ATTACK OF ALL TIME
http://aplikasi.pta-palangkaraya.go.id/readme.html
http://aplikasi.pta-palangkaraya.go.id/readme.html notified by WE WILL BE BACK SOON WITH THE BIGGEST CYBER ATTACK OF ALL TIME
http://utostore.moph.go.th/srrt/kurd.html
http://utostore.moph.go.th/srrt/kurd.html notified by 0x1998
http://dns1.sedesore.gob.mx/sidesore/fotos/20_8402index.html
http://dns1.sedesore.gob.mx/sidesore/fotos/20_8402index.html notified by rooterror
http://www.sedesore.gob.mx/sidesore/fotos/20_8402index.html
http://www.sedesore.gob.mx/sidesore/fotos/20_8402index.html notified by rooterror
https://eketapang.dkp.balangankab.go.id/read.txt
https://eketapang.dkp.balangankab.go.id/read.txt notified by Mr.L3RB1
http://nanuan.go.th/nanuan/module_eservice1/
http://nanuan.go.th/nanuan/module_eservice1/ notified by ./Niz4r
http://srinarong.go.th/srinarong/mainfile/hai.html
http://srinarong.go.th/srinarong/mainfile/hai.html notified by ./Niz4r
http://www.krabuang.go.th/krabuang/file_editor/hai.html
http://www.krabuang.go.th/krabuang/file_editor/hai.html notified by ./Niz4r
http://www.arpon.go.th/arpon/mainfile/hai.html
http://www.arpon.go.th/arpon/mainfile/hai.html notified by ./Niz4r
http://www.tago.go.th/tago/gallery/hai.html
http://www.tago.go.th/tago/gallery/hai.html notified by ./Niz4r
https://esehospicaldas.gov.co/1975.html
https://esehospicaldas.gov.co/1975.html notified by 1975 Team
https://www.corpoguavio.gov.co/dz.php
https://www.corpoguavio.gov.co/dz.php notified by djebbaranon
https://uab.cubatao.sp.gov.br/moodle/CONTRIBUTING.txt
https://uab.cubatao.sp.gov.br/moodle/CONTRIBUTING.txt notified by Typical Idiot Security
https://baritotimurkab.go.id/1.txt
https://baritotimurkab.go.id/1.txt notified by chinafans



Dark Web News

Darknet Live

Tor Browser 11.5.1 Released

Nothing interesting since 11.5, it seems. Tor Browser 11.5 _ Tor Browser 11.5 is now available from the Tor Browser download page and also from our distribution directory. This new release builds upon features introduced in Tor Browser 10.5 to transform the user experience of connecting to Tor from heavily censored regions. Update (2022-07-19): We're tracking two known issues affecting certain language versions of Tor Browser, and users who attempt to visit IP addresses that do not support HTTPS. Please see Known issues below for details. What's new? _ Automatic censorship detection and circumvention _ We began reshaping the experience of connecting to Tor with the release of Tor Browser 10.5 last year, including the retirement of the Tor Launcher and the integration of the connection flow into the browser window. However, circumventing censorship of the Tor Network itself remained a manual and confusing process - requiring users to dive into Tor Network settings and figure out for themselves how to apply a bridge to unblock Tor. What's more, censorship of Tor isn't uniform - and while a certain pluggable transport or bridge configuration may work in one country, that doesn't mean it'll work elsewhere. This placed the burden on censored users (who are already under significant pressure) to figure out what option to pick, resulting in a lot of trial, error and frustration in the process. In collaboration with the Anti-Censorship team at the Tor Project, we've sought to reduce this burden with the introduction of Connection Assist: a new feature that when required will offer to automatically apply the bridge configuration we think will work best in your location for you. __ Connection assist Connection Assist works by looking up and downloading an up-to-date list of country-specific options to try using your location (with your consent). It manages to do so without needing to connect to the Tor Network first by utilizing moat - the same domain-fronting tool that Tor Browser uses to request a bridge from torproject.org. While Connection Assist has reached the milestone of its first stable release, this is only version 1.0, and your feedback will be invaluable to help us improve its user experience in future releases. Users from countries where the Tor Network may be blocked (such as Belarus, China, Russia and Turkmenistan) can test the most recent iteration of this feature by volunteering as an alpha tester, and reporting your findings on the Tor forum. Redesigned Tor Network settings _ __ Connection settings We hope that the majority of our users living under extreme censorship will be able to connect to Tor at the press of a button, thanks to Connection Assist. However we know there will always be exceptions to that, and there are many users who prefer to configure their connection manually as well. That's why we've invested time redesigning Tor Network settings too - featuring: A brand new name: Tor Network settings is now called Connection settings. This change is intended to clarify exactly what settings you can find within this tab. Connection statuses: Your last known connection status can now be found at the top of the tab, including the option to test your Internet connection without Tor, using moat, to help you untangle the source of your connection woes. Streamlined bridge options: Gone is the long list of fields and options. Each method to add a new bridge has been tidied away into individual dialog menus, which will help support further improvements to come. Connection Assist: When Tor Browser's connection to the Tor Network isn't reachable due to suspected censorship, an additional option to select a bridge automatically becomes available. Brand-new bridge cards:

Bridges used to be almost invisible, even when configured. Now, your saved bridges appear in a handy stack of bridge cards - including new options for sharing bridges too. __ Bridge card diagram This is the anatomy of a bridge card when expanded. In addition to copying and sharing the bridge line, each bridge also comes with a unique QR code that will be readable by Tor Browser for Android (and hopefully other Tor-powered apps too) in a future release - helping facilitate the transfer of a working bridge from desktop to mobile. When you have multiple bridges configured the cards will collapse into a stack - each of which can be expanded again with a click. And when connected, Tor Browser will let you know which bridge it's currently using with the purple "&#10004; Connected&rdquo; pill. To help differentiate between your bridges without needing to compare long, unfriendly bridge lines, we've introduced bridge-moji: a short, four emoji visualization you can use to identify the right bridge at a glance. Lastly, help links within Connection settings now work offline. To recap - there are two types of help links in Tor Browser's settings: those that point to support.mozilla.org, and those that point to tb-manual.torproject.org (i.e. the Tor Browser Manual). However, since web-based links aren't very useful when you're troubleshooting connection issues with Tor Browser, the manual is now bundled in Tor Browser 11.5 and is available offline. In addition to the help links within Tor Browser's settings, the manual can be accessed via the Application Menu > Help > Tor Browser Manual, and by entering "about:manual&rdquo; into your browser's address bar too. HTTPS-Only Mode, by default _ __ HTTPS-Only Mode HTTPS-Everywhere is one of two extensions that previously came bundled in Tor Browser, and has led a long and distinguished career protecting our users by automatically upgrading their connections to HTTPS wherever possible. Now, HTTPS is actually everywhere, and all major web browsers include native support to automatically upgrade to HTTPS. Firefox - the underlying browser on which Tor Browser is based - calls this feature HTTPS-Only Mode. Starting in Tor Browser 11.5, HTTPS-Only Mode is enabled by default for desktop, and HTTPS-Everywhere will no longer be bundled with Tor Browser. Why now? Research by Mozilla indicates that the fraction of insecure pages visited by the average users is very low - limiting the disruption caused to the user experience. Additionally, this change will help protect our users from SSL stripping attacks by malicious exit relays, and strongly reduces the incentive to spin up exit relays for Man-in-the-Middle attacks in the first place. You may or may not know that HTTPS-Everywhere also served a second purpose in Tor Browser, and was partly responsible for making SecureDrop's human-readable onion names work. Well, SecureDrop users can rest assured that we've patched Tor Browser to ensure that human-readable onion names still work in HTTPS-Everywhere's absence. Note: Unlike desktop, Tor Browser for Android will continue to use HTTPS-Everywhere in the short term. Please see our separate update about Android below. Improved font support _ __ More fonts One of Tor Browser's many fingerprinting defenses includes protection against font enumeration - whereby an adversary can fingerprint you using the fonts installed on your system. To counter this, Tor Browser ships with a standardized bundle of fonts to use in place of those installed on your system. However some writing scripts did not render correctly, while others had no font available in Tor Browser at all. To solve this issue and expand the number of writing systems supported by Tor Browser, we've bundled many more fonts from the Noto family in this release. Naturally, we have to find a balance between the number of fonts Tor Browser supports without increasing the size of the installer too much, which is something we're very conscious of. So if you spot a language whose characters don't render correctly in Tor Browser, please let us know! Tor Browser for Android _ You have no doubt noticed that the features announced above are all for desktop. So, we wanted to share a little update about where we're at with Android: We know that Tor Browser for Android is quite behind desktop in terms of feature parity. The Tor Project has hit a few bumps in the road over the last couple of years that have delayed our releases, and led us to reassess our roadmap for Android. Since the beginning of the year our priorities for Android have been three-fold: Start releasing regular updates for Android again Fix the crashes that many Android users have experienced Begin catching up with Fenix (Firefox for Android) releases Since then, Android has averaged one stable update per month, crash reports are down significantly thanks to the patch issued in fenix#40212, and downloads are working again due to the fixes in fenix#40192 and android-components#40075. However we still have work to do to catch up with Fenix, and upgrading Tor Browser to Fenix v102 will be our priority for the next few months. We've also taken steps to expand the team's capacity in order to dedicate more resources to Android, keep the application stable, and help us bring some of these features described above to Android in the future too. Thank you for your patience and support! Known issues _ Tor Browser 11.5 comes with a number of known issues: Bug torbrowser#40159: Bridge cards aren't displaying, and toggle themselves off _ We're aware of an issue affecting certain language-versions of Tor Browser that's preventing bridge cards from rendering within Connection settings, even if a bridge has been configured. Furthermore, bridges can appear to toggle themselves on and off too. Our initial testing indicates that this bug is limited to the UI only, and Tor Browser will remain connected to the bridge you have input regardless. We're working on a fix for this issue as a priority. Bug torbrowser#41050: "Continue to HTTP Site&rdquo; button doesn't work on IP addresses _ HTTPS-Only Mode will alert you whenever a HTTP connection cannot be upgraded. Normally this alert can by bypassed using the "Continue to HTTP Site&rdquo; button, which grants an exception for the site in question. However this button does not work when visiting an IP address directly, and an exception cannot be granted by other means. A fix for this issue will be coming soon. Should you need to visit an IP address over HTTP in the meantime, we recommend against turning HTTPS-Only Mode off. Instead, consider downgrading temporarily to Tor Browser 11.0.15 until fixed. Changelog _ Changelog The full changelog since Tor Browser 11.0.15 is: All Platforms Update OpenSSL to 1.1.1q Windows + OS X + Linux Update Firefox to 91.11.0esr Update Tor-Launcher to 0.2.37 Update Translations Bug tor-browser#11698: Incorporate Tor Browser Manual pages into Tor Browser Bug tor-browser#19850: Disable Plaintext HTTP Clearnet Connections Bug tor-browser#30589: Allowed fonts to render a bunch of missing scripts Bug tor-browser#40458: Implement about:rulesets https-everywhere replacement Bug tor-browser-build#40527: Remove https-everywhere from tor-browser alpha desktop Bug tor-browser#40562: Reorganize patchset Bug tor-browser#40598: Remove legacy settings read from TorSettings module Bug tor-browser#40645: Migrate Moat APIs to Moat.jsm module Bug tor-browser#40684: Misc UI bug fixes Bug tor-browser#40773: Update the about:torconnect frontend page to match additional UI flows Bug tor-browser#40774: Update about:preferences page to match new UI designs Bug tor-browser#40775: about:ion should not be labeled as a Tor Browser page Bug tor-browser#40793: moved Tor configuration options from old-configure.in to moz.configure Bug tor-browser#40825: Redirect HTTPS-Only error page when not connected Bug tor-browser#40912: Hide screenshots menu since we don't support it Bug tor-browser#40916: Remove the browser.download.panel.shown preference Bug tor-browser#40923: Consume country code to improve error report Bug tor-browser#40966: Render emojis in bridgemoji with SVG files, and added emojii descriptions Bug tor-browser#41011: Make sure the Tor Connection status is shown only in about:preferences#connection Bug tor-browser#41023: Update manual URLs Bug tor-browser#41035: OnionAliasService should use threadsafe ISupports Bug tor-browser#41036: Add a preference to disable Onion Aliases Bug tor-browser#41037: Fixed the connection preferences on the onboarding Bug tor-browser#41039: Set 'startHidden' flag on tor process in tor-launcher OS X Bug tor-browser#40797: font-family: monospace renders incorrectly on macOS Bug tor-browser#41004: Bundled fonts are not picked up on macOS Linux Bug tor-browser#41015: Add -name parameter to correctly setup WM_CLASS when running as native Wayland client Bug tor-browser#41043: Hardcode the UI font on Linux Android Update Fenix to 99.0.0b3 Build System All Platforms Bug tor-browser-build#40288: Bump mmdebstrap version to 0.8.6 Bug tor-browser-build#40426: Update Ubuntu base image to 22.04 Bug tor-browser-build#40519: Add Alexis' latest PGP key to https-everywhere key ring Android Update Go to 1.18.3 Bug tor-browser-build#40433: Bump LLVM to 13.0.1 for android builds Bug tor-browser-build#40470: Fix zlib build issue for android Bug tor-browser-build#40485: Resolve Android reproducibility issues Windows + OS X + Linux Bug tor-browser-build#34451: Include Tor Browser Manual in packages during build Bug tor-browser-build#40525: Update the mozconfig for tor-browser-91.9-11.5-2 Tor Browser 11.5.1 _ Tor Browser 11.5.1 is now available from the Tor Browser download page and also from our distribution directory. Tor Browser 11.5.1 updates Firefox on Windows, macOS, and Linux to 91.12.0esr. We would like to thank WofWca for sending us some patches for the preferences page. ChangeLog _ Tor Browser 11.5.1 - July 26 2022 The full changelog since Tor Browser 11.5 is: Windows + OS X + Linux Update Firefox to 91.12.0esr Bug tor-browser#41049: QR codes in connection settings aren't recognized by some readers in dark theme Bug tor-browser#41050: "Continue to HTTP Site&rdquo; button doesn't work on IP addresses Bug tor-browser#41053: remove HTTPS-Everywhere entry from browser.uiCustomization.state pref Bug tor-browser#41054: Improve color contrast of purple elements in connection settings in dark theme Bug tor-browser#41055: Icon fix from #40834 is missing in 11.5 stable Bug tor-browser#41058: Hide currentBridges description when the section itself is hidden Bug tor-browser#41059: Bridge cards aren't displaying, and toggle themselves off Build System Windows + OS X + Linux Update Go to 1.17.12 Bug tor-browser-build#40547: Remove container/remote_* from rbm.conf Bug tor-browser-build#40584: Update tor-browser manual to latest (via darknetlive.com at https://darknetlive.com/post/tor-browser-11.5.1-released/)

SEROCU Arrested Two for Selling Heroin on the Darkweb

Police in the United Kingdom arrested two people for allegedly conspiring to supply heroin on the darkweb. Officers with the Cyber and Dark Web Unit of the South East Regional Organised Crime Unit arrested a 34-year-old from Isle of Wight and a 41-year-old man from London for allegedly supplying heroin on the darkweb. __ The hero image displayed on the homepage of the SEROCU website | serocu.police.uk SEROCU officers, officers from the Metropolitan Police Service, and Hampshire Constabulary executed five search warrants at addresses in Portsmouth, Isle of Wight, Hackney, and Walthamstow during the investigation. Both suspects have been released pending further investigation. Detective Inspector Rob Bryant of SEROCU's Regional Cyber Crime Unit said: "This is an ongoing investigation and our action sends out a clear message to organised criminal groups who are using the Dark Web to commit such offences, that crime really doesn't pay. We continue to work in partnership with the National Crime Agency, US Law Enforcement and our regional and force colleagues to identify and investigate those using the Dark Web. Anyone who is selling drugs on the Dark Web should realise that we will find them and we will look to prosecute them. The wider impact of drug dealing causes untold damage to people's lives and we will take every opportunity to disrupt this criminal activity to protect the communities of the South East from harm.&rdquo; __ Detective Inspector Rob Bryant's Linkedin The National Police Chiefs Council (NPCC) lead for the Dark Web, detective chief inspector Phil Donnelly, said: "The regional Dark Web Teams, which form part of the UK Dark Web Intelligence Collaboration and Exploitation, are having a real impact on disrupting organised criminal activity on the Dark Web. Criminals should not see the Dark Web as a safe place where police cannot touch them. Our highly trained and capable officers and staff are actively taking down Dark Web operations on a daily basis and the South East team have played an integral role in this ongoing investigation.&rdquo; Two arrested on suspicion of drug offences on the Dark Web | archive.is, archive.org, serocu.police.uk (via darknetlive.com at https://darknetlive.com/post/serocu-arrested-two-suspected-heroin-vendors/)

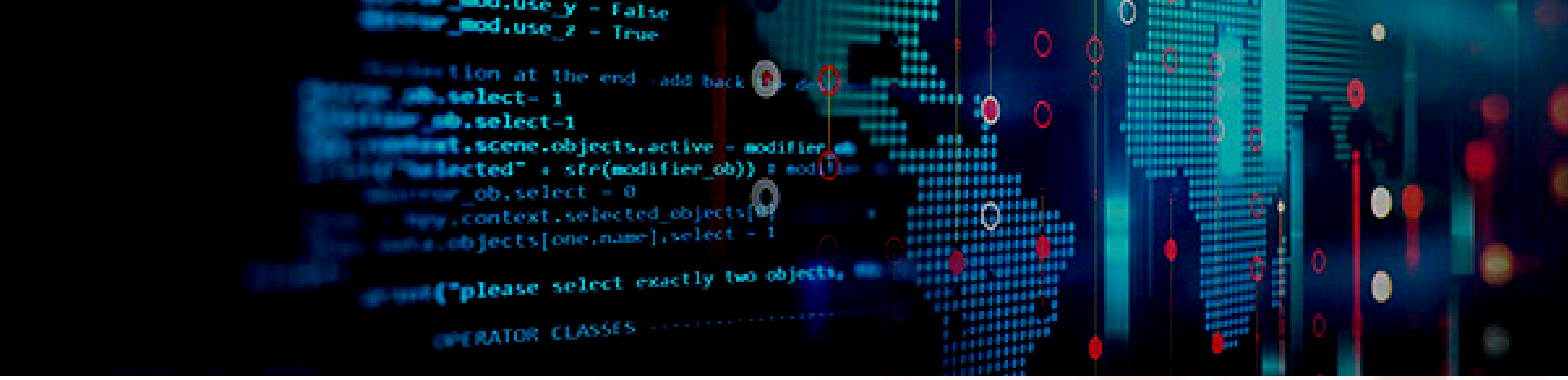
Chicago Police and USPS Seized $2.4 Million Worth of Drugs

A collaboration between Chicago police and the United States Postal Service (USPS) resulted in the seizure of $2.4 million of illegal drugs. __ Bill Hendricks wants to "defend the community&rdquo; Chicago police, USPS, and the United States Postal Inspection Service (USPIS) launched a joint task force in February 2021 to prevent packages of drugs and illegal guns from entering Chicago. __ Package tracking status showing "seized by law enforcement&rdquo; "We want to play our part in helping defend our communities from the illegal things that come into those communities,&rdquo; USPIS employee Bill Hendricks said. According to a press release published by CBS, the task force intercepted 42 guns and $2.4 million worth of illicit substances, including cocaine, fentanyl, and meth. __ $2.4 million worth of drugs seems low. Did the Postal Service need to team up with Chicago police for that? Chicago police, U.S. Postal Service team up to search for drugs, guns in mail | archive.is, archive.org, cbsnews.com (via darknetlive.com at https://darknetlive.com/post/chicago-police-and-usps-seized-two-million-worth-of-drugs/)

Sports Direct Employee Convicted of Soliciting Murder

After deliberating for four hours at Reading Crown Court, a jury convicted a 26-year-old of soliciting murder via the darkweb. A jury of 10 men and two women unanimously convicted Whitney Franks, 26, of soliciting murder. During the trial, the court heard that Franks had posted an advertisement on a dark web site on the darkweb, offering Â£1,000 or more to kill her colleague. Whitney Franks, 26 "I'm looking for the murder of a woman. I have Â£1,000, and I am willing to pay more. This woman has caused a lot of problems for myself and others. Please can you help sort this out,&rdquo; part of the advertisement read. From the previous Darknetlive article about the case: "The advertisement also included the address and Facebook profile of Ruut Ruutna, one of Franks' colleagues at Sports Direct. According to the prosecutor, Franks had started "an affair&rdquo; with her store manager, James Prest, in 2016. Ruutna joined the team in 2017 and also started having "an affair&rdquo; with Prest.&rdquo; "Prest, who had a "partner&rdquo; of his own and two children, would sneak out to see the women. "By 2020, James Prest would, while his partner and children were in bed, frequently leave his house and go to Ruut Ruutna's house,&rdquo; the prosecutor said.&rdquo; Franks almost certainly followed her lover after work. "One encounter with Franks concerned Prest, the court heard. On August 17, 2020, Franks confronted Prest about his relationship with Ruutna at the Milton Keynes Sports Direct. During the conversation, Franks brought up Prest's "sneaking around at night.&rdquo; In court, the prosecutor asked, "how did she know about James Prest going around Ruut Ruutna's at night?&rdquo; The women did not speak with or about each other.&rdquo; A journalist working with the BBC found Franks' advertisement. The journalist notified the police, who identified Ruutna as the intended victim. Ruutna pointed the police toward Franks as a possible suspect. Franks had an affair with James Prest, another Sports Direct employee. Franks denied the charge in court but admitted that she had posted the advertisement. She said she had developed an interest in darkweb murder-for-hire sites after watching true crime documentaries. She told the court that she had suspected the site was a scam but wanted to "prove it&rdquo; to satisfy her curiosity. Judge Dugdale scheduled a sentencing hearing for September 9, 2022. "You have been unanimously convicted of soliciting murder, it is a very serious offence. It is an offence for which I will have to pass a fairly lengthy sentence. I will need to find out more about you, which will take time. There is no option other than to take away your bail,&rdquo; Judge Dugdale told Franks. (via darknetlive.com at https://darknetlive.com/post/crazy-lady-convicted-of-soliciting-murder/)

Dark Web Link



Trend Micro Anti-Malware Blog

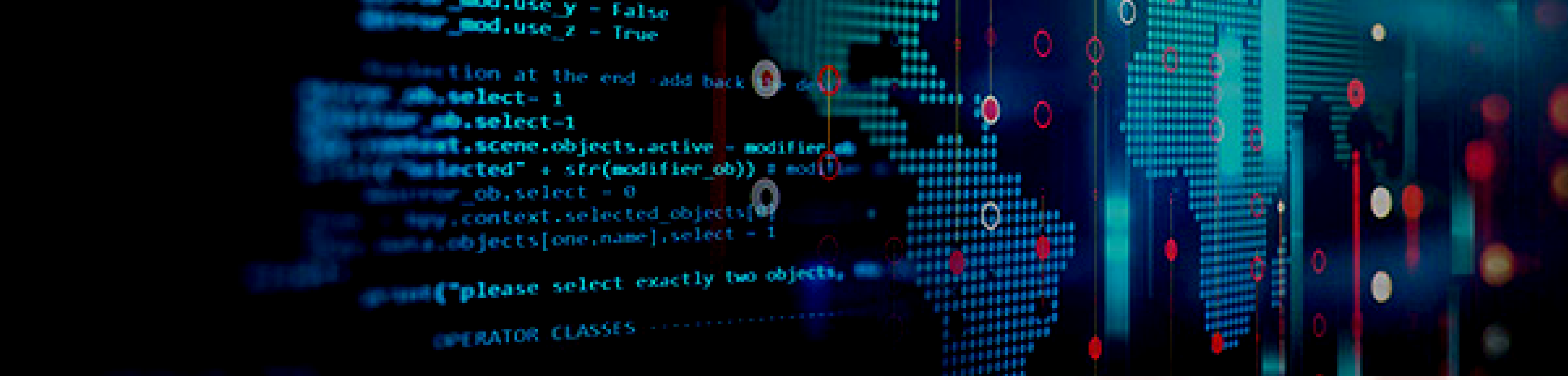
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* 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&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-Up
* [VIDEO] An Inside Look at AWS re:Inforce 2022 From the Rapid7 Team
* [The Lost Bots] Season 2, Episode 2: The Worst and Best Hollywood Cybersecurity Depictions
* What's New in InsightVM and Nexpose: Q2 2022 in Review
* Active Exploitation of Atlassian's Questions for Confluence App CVE-2022-26138
* To Maze and Beyond: How the Ransomware Double Extortion Space Has Evolved
* 5 SOAR Myths Debunked
* Rapid7 at AWS re:Inforce: 2 Big Announcements
* CVE-2022-35629..35632 Velociraptor Multiple Vulnerabilities (FIXED)
* ISO 27002 Emphasizes Need For Threat Intelligence


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

Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* CISA Releases Log4Shell-Related MAR
* Samba Releases Security Updates
* Apple Releases Security Updates for Multiple Products
* Cisco Releases Security Updates for Multiple Products
* Atlassian Releases Security Advisory for Questions for Confluence App, CVE-2022-26138
* Google Releases Security Updates for Chrome
* Drupal Releases Security Update&#8239;
* AA22-187A: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and
* AA22-181A: #StopRansomware: MedusaLocker
* Vulnerability Summary for the Week of July 18, 2022
* Vulnerability Summary for the Week of July 11, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5540-1

Ubuntu Security Notice 5540-1 - Liu Jian discovered that the IGMP protocol implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the USB gadget subsystem in the Linux kernel did not properly validate interface descriptor requests. An attacker could possibly use this to cause a denial of service.

Red Hat Security Advisory 2022-5753-01

Red Hat Security Advisory 2022-5753-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Ubuntu Security Notice USN-5539-1

Ubuntu Security Notice 5539-1 - It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service. Duoming Zhou discovered that the AX.25 amateur radio protocol implementation in the Linux kernel did not handle detach events properly in some situations. A local attacker could possibly use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5536-1

Ubuntu Security Notice 5536-1 - Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the mouse pointer position, bypass Subresource Integrity protections, obtain sensitive information, or execute arbitrary code.

Ubuntu Security Notice USN-5537-2

Ubuntu Security Notice 5537-2 - USN-5537-1 fixed a vulnerability in MySQL. This update provides the corresponding update for Ubuntu 16.04 ESM. Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues. MySQL has been updated to 5.7.39 in Ubuntu 16.04 ESM.

Ubuntu Security Notice USN-5538-1

Ubuntu Security Notice 5538-1 - It was discovered that libtirpc incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2022-5754-01

Red Hat Security Advisory 2022-5754-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for Red Hat build of OpenJDK 8 and includes security and bug fixes as well as enhancements. For further information, refer to the release notes linked to in the References section.

Ubuntu Security Notice USN-5537-1

Ubuntu Security Notice 5537-1 - Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues. MySQL has been updated to 8.0.30 in Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. Ubuntu 18.04 LTS has been updated to MySQL 5.7.39. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Ubuntu Security Notice USN-5535-1

Ubuntu Security Notice 5535-1 - Joseph Nuzman discovered that some Intel processors did not properly initialise shared resources. A local attacker could use this to obtain sensitive information. Mark Ermolov, Dmitry Sklyarov and Maxim Goryachy discovered that some Intel processors did not prevent test and debug logic from being activated at runtime. A local attacker could use this to escalate privileges.

Red Hat Security Advisory 2022-5640-01
Red Hat Security Advisory 2022-5640-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-5718-01
Red Hat Security Advisory 2022-5718-01 - Grafana is an open source, feature rich metrics dashboard and graph editor for Graphite, InfluxDB & OpenTSDB.
Red Hat Security Advisory 2022-5664-01
Red Hat Security Advisory 2022-5664-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.10.24.
Red Hat Security Advisory 2022-5703-01
Red Hat Security Advisory 2022-5703-01 - An update is now available for Red Hat Ansible Automation Platform 1.2. Issues addressed include a remote SQL injection vulnerability.
Red Hat Security Advisory 2022-5641-01
Red Hat Security Advisory 2022-5641-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-5531-01
Red Hat Security Advisory 2022-5531-01 - Red Hat Advanced Cluster Management for Kubernetes 2.5.1 General Availability release images, which fix security issues and bugs.
Red Hat Security Advisory 2022-5626-01
Red Hat Security Advisory 2022-5626-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include information leakage, memory leak, privilege escalation, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-5622-01
Red Hat Security Advisory 2022-5622-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc. Issues addressed include a privilege escalation vulnerability.
Red Hat Security Advisory 2022-5004-01
Red Hat Security Advisory 2022-5004-01 - Red Hat OpenShift Service Mesh is a Red Hat distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. This advisory covers the RPM packages for the release. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-5719-01
Red Hat Security Advisory 2022-5719-01 - Grafana is an open source, feature rich metrics dashboard and graph editor for Graphite, InfluxDB & OpenTSDB.
Red Hat Security Advisory 2022-5597-01
Red Hat Security Advisory 2022-5597-01 - An update for pandoc is now available for Red Hat Enterprise Linux 8. Issues addressed include an integer overflow vulnerability.
Red Hat Security Advisory 2022-4931-01
Red Hat Security Advisory 2022-4931-01 - The RHV-M Appliance automates the process of installing and configuring the Red Hat Virtualization Manager. The appliance is available to download as an OVA file from the Customer Portal.
Red Hat Security Advisory 2022-5620-01
Red Hat Security Advisory 2022-5620-01 - 389 Directory Server is an LDAP version 3 compliant server. The base packages include the Lightweight Directory Access Protocol server and command-line utilities for server administration. Issues addressed include a denial of service vulnerability.
Red Hat Security Advisory 2022-5556-01
Red Hat Security Advisory 2022-5556-01 - Logging Subsystem 5.4.3 has security updates. Issues addressed include denial of service and out of bounds read vulnerabilities.

Red Hat Security Advisory 2022-5564-01

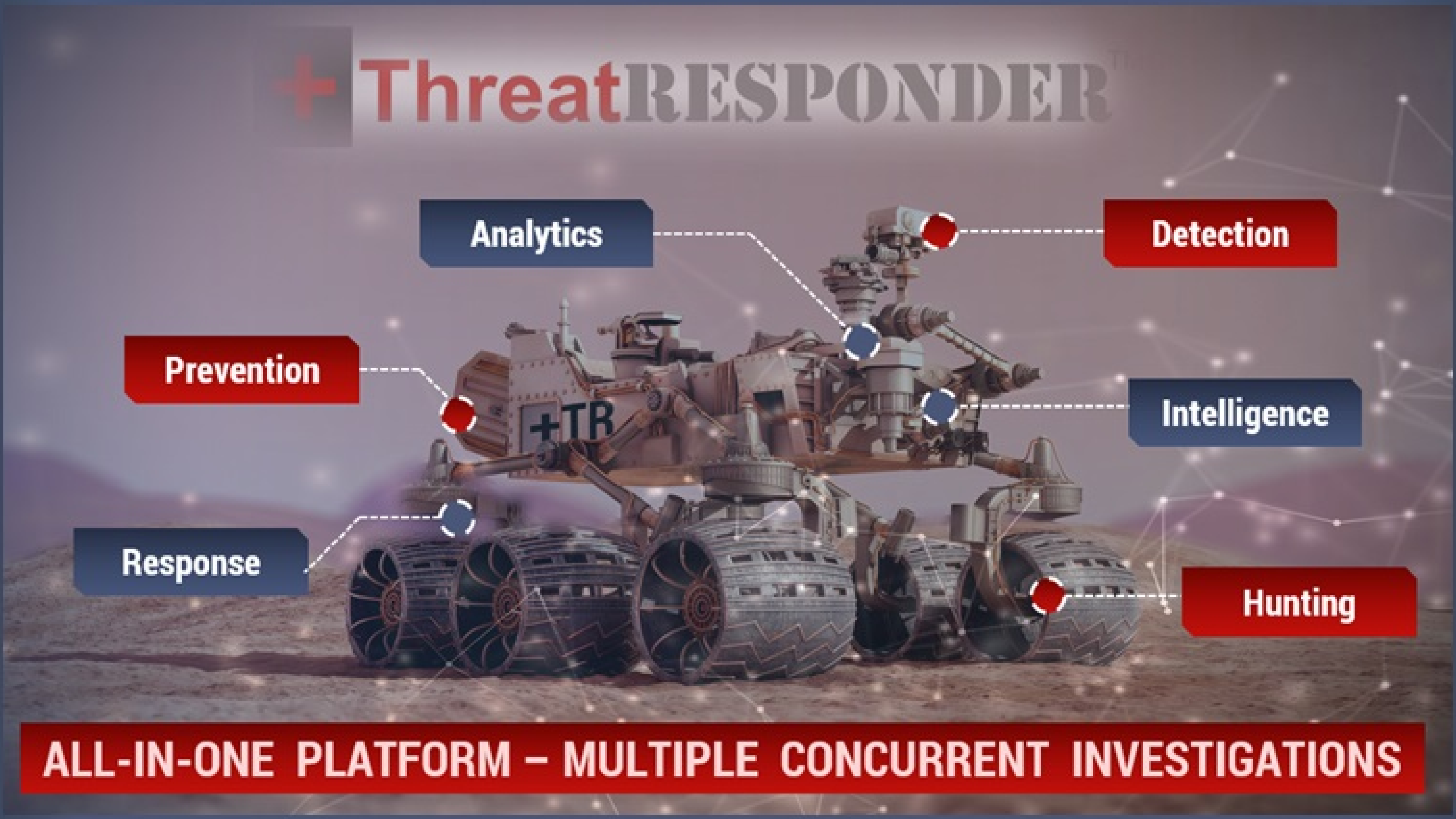
Red Hat Security Advisory 2022-5564-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a privilege escalation vulnerability.

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



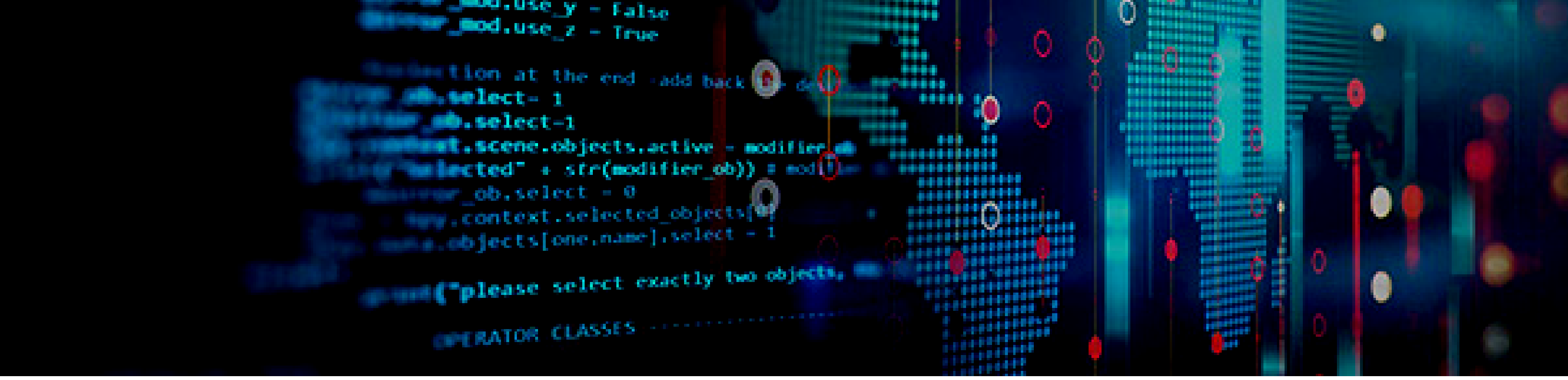
The Solution – ThreatResponder® Platform

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



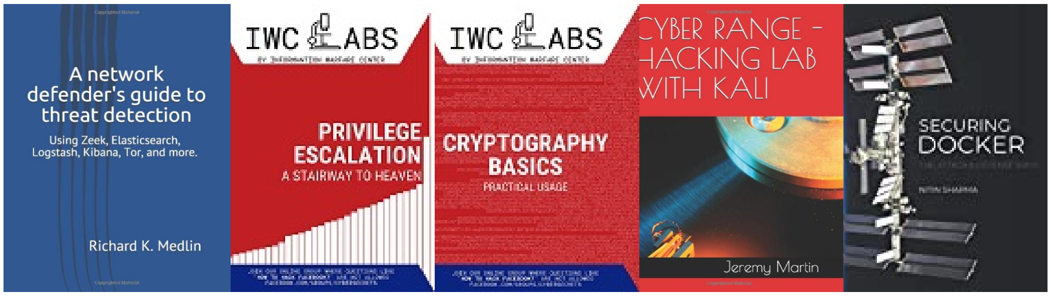
The Cyber Secrets publications on Amazon

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
EVIDENCE PRESERVATION AND COLLECTION

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP