Jul-25-22

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

July 25, 2022

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

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

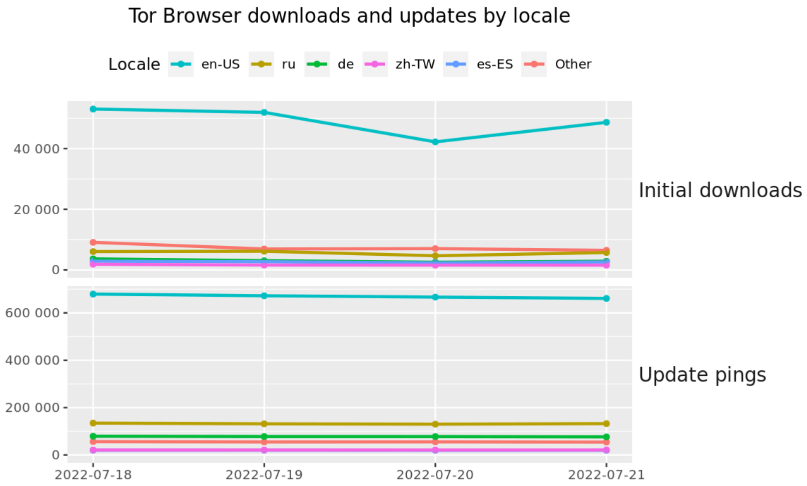
Internet Storm Center Infocon Status

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

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* 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
* Atlassian Reveals Critical Flaws In Almost Everything It Makes And Touches
* Authentication Weakness Responsible For 80% Of Financial Breaches
* National Data Privacy Law Draws Mixed Reactions
* Hackers For Hire: Adversaries Employ Cyber Mercenaries
* A Hacker Is Trying To Sell Data On 69 Million Neopots Users
* Belgium Says Chinese APT Gangs Attacked Its Government And Military
* Singapore Distances Itself From Local Crypto Companies
* Critical Flaws In GPS Tracker Enable Life Threatening Hacks
* US Seizes Stolen Funds From Suspected North Korean Hackers
* Russia Released A Ukrainian App For Hacking Russia That Was Really Malware
* Magecart Serves Up Card Skimmers On Restaurant Ordering Systems
* Inside Ukraine's Decentralized Cyber Army
* Industrial Control System Password Cracker May Be Bad, Actually
* Walmart-Controllled Flight Booking Service Suffers Data Leak
* Servers Running Digium Phones VoIP Software Are Getting Backdoored
* White House To Hold Summit On Addressing The Thousands Of Unfilled Cybersecurity Jobs
* Google Boots Multiple Malware-Laced Android Apps From Store
* Albanian Government Websites Go Dark After Cyberattack
* Microsoft's Latest Security Patch Troubles Windows 11 Users
* Nephew Of Jailed Hotel Rwanda Dissident Hacked By NSO Spyware
* Windows Network File System Flaw Results In Arbitrary Code Execution As SYSTEM

Krebs on Security

* 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
* Why Paper Receipts are Money at the Drive-Thru
* Microsoft Patch Tuesday, June 2022 Edition
* Ransomware Group Debuts Searchable Victim Data

LATEST NEWS

Dark Reading

* Understanding Proposed SEC Rules Through an ESG Lens
* ICYMI: Neopets & the Gaming Problem; SolarWinds Hackers Are Back; Google Ads Abused
* Critical Bugs Threaten to Crack Atlassian Confluence Workspaces Wide Open
* Google Chrome Zero-Day Weaponized to Spy on Journalists
* Snowballing Ransomware Variants Highlight Growing Threat to VMware ESXi Environments
* Phishing Bonanza: Social-Engineering Savvy Skyrockets as Malicious Actors Cash In
* Thales Expands Cybersecurity Portfolio With OneWelcome Acquisition
* What Firewalls Can - and Can't - Accomplish
* Mysterious, Cloud-Enabled macOS Spyware Blows Onto the Scene
* Equitable Digital Identity Verification Requires Moving Past Flawed Legacy Systems
* Google Becomes First Cloud Operator to Join Healthcare ISAC
* The Market Is Teeming: Bargains on Dark Web Give Novice Cybercriminals a Quick Start
* The Kronos Ransomware Attack: What You Need to Know So Your Business Isn't Next
* Cybercrime Group TA4563 Targets DeFi Market With Evolving Evilnum Backdoor
* Cybersecurity Professionals Push Their Organizations Toward Vendor Consolidation and Product Integrat
* Lax Security Fuels Massive 8220 Gang Botnet Army Surge
* 'AIG' Threat Group Launches With Unique Business Model
* Feds Recoup $500K From Maui Ransomware Gang
* Data-Centric Security Market Worth $12.3B by 2027 - Exclusive Report by MarketsandMarketsâ„¢
* Mutare Voice Network Threat Survey Shows Nearly Half of Organizations Experienced Vishing or Social E

The Hacker News

* Racoon Stealer is Back - How to Protect Your Organization
* Roaming Mantis Financial Hackers Targeting Android and iPhone Users in France
* SonicWall Issues Patch for Critical Bug Affecting its Analytics and GMS Products
* Microsoft Resumes Blocking Office VBA Macros by Default After 'Temporary Pause'
* Google Bringing the Android App Permissions Section Back to the Play Store
* An Easier Way to Keep Old Python Code Healthy and Secure
* Ukrainian Radio Stations Hacked to Broadcast Fake News About Zelenskyy's Health
* Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists
* New Linux Malware Framework Lets Attackers Install Rootkit on Targeted Systems
* Hackers Target Ukrainian Software Company Using GoMet Backdoor
* Hackers Use Evilnum Malware to Target Cryptocurrency and Commodities Platforms
* The New Weak Link in SaaS Security: Devices
* Atlassian Rolls Out Security Patch for Critical Confluence Vulnerability
* FBI Seizes $500,000 Ransomware Payments and Crypto from North Korean Hackers
* Cynomi Automated Virtual CISO (vCISO) Platform for Service Providers

LATEST NEWS

Security Week

* T-Mobile Settles to Pay $350M to Customers in Data Breach
* SonicWall Warns of Critical GMS SQL Injection Vulnerability
* Chrome Flaw Exploited by Israeli Spyware Firm Also Impacts Edge, Safari
* Intezer Documents Powerful 'Lightning Framework' Linux Malware
* New Default Account Lockout Policy in Windows 11 Blocks Brute Force Attacks
* Edge Management and Orchestration Firm Zededa Raises $26 Million
* New Cross-Platform 'Luna' Ransomware Only Offered to Russian Affiliates
* Code Execution and Other Vulnerabilities Patched in Drupal
* Microsoft Resumes Rollout of Macro Blocking Feature
* Understanding the Evolution of Cybercrime to Predict its Future
* Romanian Operator of Bulletproof Hosting Service Extradited to the US
* Anvilogic Scores $25 Million Series B to Tackle SOC Modernization
* USCYBERCOM Releases IoCs for Malware Targeting Ukraine
* Atlassian Patches Servlet Filter Vulnerabilities Impacting Multiple Products
* Exploitation of Recent Chrome Zero-Day Linked to Israeli Spyware Company
* Hundreds of ICS Vulnerabilities Disclosed in First Half of 2022
* Cisco Patches Severe Vulnerabilities in Nexus Dashboard
* Machine Identity Management Firm AppViewX Raises $20 Million
* Apple Ships Urgent Security Patches for macOS, iOS
* Netwrix Auditor Vulnerability Can Facilitate Attacks on Enterprises
* Google Introduces DNS-over-HTTP/3 in Android
* Google, EU Warn of Malicious Russian Cyber Activity
* Can Encryption Key Intercepts Solve The Ransomware Epidemic?
* Chrome 103 Update Patches High-Severity Vulnerabilities
* Oracle Releases 349 New Security Patches With July 2022 CPU
* German Consumer Group Sues Tesla Over Privacy, Climate

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Striving for 100% Completion Rates: Getting Compliance on Your Compliance Training
* [Heads Up] Huge Losses Caused By Epidemic of 'Pig Butchering' Scams
* [Eye Opener] Both Job Seekers and Employers Should Be Aware Of New Sophisticated Scams
* FBI Warns of Phony Cryptocurrency Investment Apps
* Cybersecurity Should be an Issue for Every Board of Directors
* CyberheistNews Vol 12 #29 [Heads Up] New Phishing Attacks Shame, Scare Victims into Surrendering Twit
* New Multi-Factor Authentication Prompt "Bombing" Attacks Give Access to Laptops, VPNs, and More
* Copyright Claim Email is a LockBit Ransomware Phishing Attack in Disguise
* Phishing Kit Imitates PayPal
* New Phishing Attacks Shame, Scare Victims into Surrendering Twitter, Discord Credentials

ISC2.org Blog

* 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
* (ISC)&sup2; Pledges 1 Million Certified in Cybersecurity
* How Long Does it Take to Train Entry-Level Cybersecurity Team Members?

HackRead

Koddos

LATEST NEWS

Naked Security

* 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"
* 7 cybersecurity tips for your summer vacation!
* S3 Ep91: CodeRed, OpenSSL, Java bugs, Office macros [Audio + Text]
* Facebook 2FA scammers return - this time in just 21 minutes
* Paying ransomware crooks won't reduce your legal risk, warns regulator
* That didn't last! Microsoft turns off the Office security it just turned on

Threat Post

* 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
* Authentication Risks Discovered in Okta Platform
* FBI Warns Fake Crypto Apps are Bilking Investors of Millions
* Google Boots Multiple Malware-laced Android Apps from Marketplace
* CISA Urges Patch of Exploited Windows 11 Bug by Aug. 2
* Emerging H0lyGh0st Ransomware Tied to North Korea
* Journalists Emerge as Favored Attack Target for APTs
* Large-Scale Phishing Campaign Bypasses MFA

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.

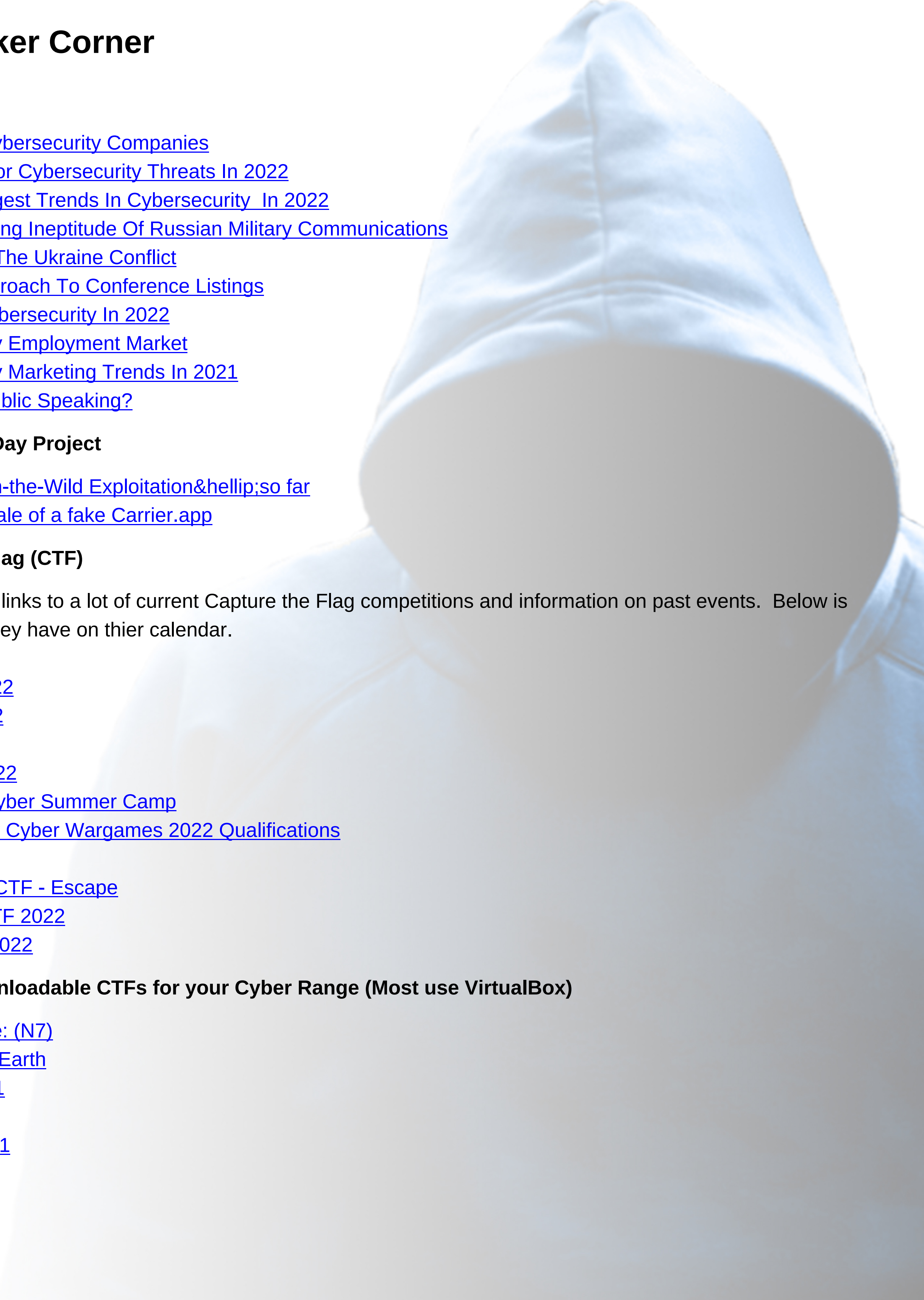
InfoWorld

* Majority of open source developers eyeing job change: EDB survey
* How to attend RStudio Conference 2022 remotely for free
* Why do businesses suck at using data?
* What is PaaS (platform-as-a-service)? A simpler way to build software applications
* What is IaaS? A data center in the cloud packed with services
* What is cloud computing? Everything you need to know now
* R tutorials: Learn R programming for data science
* The best new features in ASP.NET Core 6
* 12 ggplot extensions for snazzier R graphics
* Intro to Ethereum smart contracts

C4ISRNET - Media for the Intelligence Age Military

* Up, up and away: Airbus' Zephyr drone breaks flight record high above Arizona
* Future of autonomous flight comes into focus at Farnborough Airshow
* Why Isn't Russia jamming GPS harder in Ukraine?
* Mission Possible: Securing remote access for classified networks
* US seeking to understand Russia's failure to project cyber power in Ukraine
* Contractors look to lasers for unmanned systems
* Pentagon renames UFO office, expands mission to include 'transmedium' objects
* As US struggles to fill cyber defense jobs, Australia works to keep talent at home
* Norway to buy Raytheon's Stormbreaker smart bomb for F-35 fleet
* UK aviation sustainability mandates could bolster US defense sector

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.

* TFC CTF 2022
* UIUCTF 2022
* UACTF 2022
* Aero CTF 2022
* hackrocks Cyber Summer Camp
* Arab Security Cyber Wargames 2022 Qualifications
* corCTF 2022
* T3N4CI0US CTF - Escape
* DEF CON CTF 2022
* SHELLCTF 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

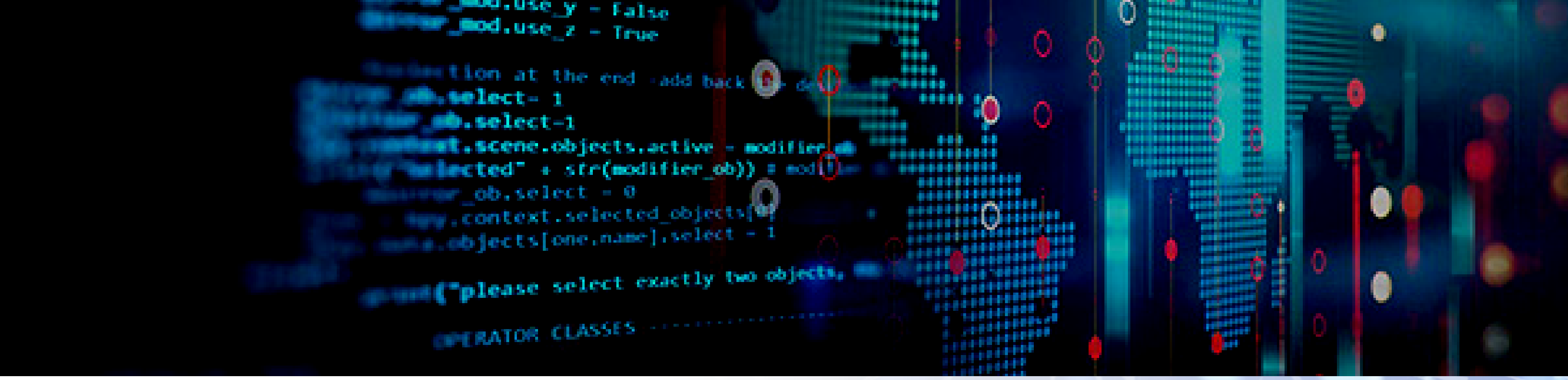
* AIEngine 2.2.0
* Global Socket 1.4.38
* Suricata IDPE 6.0.6
* GNU Privacy Guard 2.3.7
* GNU Privacy Guard 2.2.36
* Falco 0.32.1
* Zeek 5.0.0
* OpenSSL Toolkit 3.0.5
* OpenSSL Toolkit 1.1.1q
* TripleCross Linux eBPF Rootkit

Kali Linux Tutorials

* PacketStreamer : Distributed Tcpdump For Cloud Native Environments
* Blackbird : An OSINT Tool To Search For Accounts By Username In 101 Social Networks
* AutoPWN Suite : Project For Scanning Vulnerabilities And Exploiting Systems Automatically
* Offensive-Azure : Collection Of Offensive Tools Targeting Microsoft Azure
* Socialhunter : Crawls The Website And Finds Broken Social Media Links That Can Be Hijacked
* Nipe : An Engine To Make Tor Network Your Default Gateway
* Sentinel-Attack : Tools To Rapidly Deploy A Threat Hunting Capability On Azure Sentinel
* AzureRT : A Powershell Module Implementing Various Azure Red Team Tactics
* AWS-Threat-Simulation-and-Detection : Playing Around With Stratus Red Team And SumoLogic
* Lockc : Making Containers More Secure With eBPF And Linux Security Modules (LSM)

GBHackers Analysis

* 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
* Kids and Teens Forming Hacking Groups Online to Exchange Malware



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

* Adding GPS to Tactical WiFi Pineapple Mk7
* 5 Reasons Hackers Want Your Accounts
* Live Hacking Q&A with Kody Kinzie and Alex Lynd

The PC Security Channel [TPSC]

* Windows Defender: Test vs Ransomware 2022
* YouTube Stealer: Hackers target gaming YouTubers

Eli the Computer Guy

* SILICON DERBY - Life in the fast lane...
* eBeggar Wednesday - NETFLIX KEEPS FAILING
* What is a Network Switch
* eBeggar Wednesday - TWITTER SUES ELON MUSK for BEING AN ASS

Security Now

* RetBleed - Facebook encrypted URLs, cracking Lockdown Mode, ClearView AI resistance, Roskomnadzor
* The Rolling Pwn - OpenSSL patch, iOS Lockdown Mode, Yubikey's to Ukraine, Office Macros re-enabled

Troy Hunt

* Weekly Update 305

Intel Techniques: The Privacy, Security, & OSINT Show

* 271-OSINT Tool Updates II
* 270-OSINT Tool Updates I

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Backdoor.Win32.Eclipse.h MVID-2022-0625 Hardcoded Credential
* Chrome Scope Break
* Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) Remote Root
* CodoForum 5.1 Remote Code Execution
* OctoBot WebInterface 0.4.3 Remote Code Execution
* Kite 1.2021.610.0 Unquoted Service Path
* Dr. Fone 4.0.8 Unquoted Service Path
* IOTransfer 4.0 Remote Code Execution
* DASDEC Cross Site Scripting / HTML Injection
* Emporium eCommerce Online Shopping CMS 1.2 SQL Injection
* Spryker Commerce OS Remote Command Execution
* Asus GameSDK 1.0.0.4 Unquoted Service Path
* Builder XtremeRAT 3.7 MVID-2022-0624 Insecure Crypto Bypass
* Builder XtremeRAT 3.7 MVID-2022-0623 Insecure Permissions
* Backdoor.Win32.HoneyPot.a MVID-2022-0622 Weak Hardcoded Password
* Orange Station 1.0 SQL Injection
* Property Listing Script 3.1 SQL Injection
* Travel Tours Script 1.0 SQL Injection
* Windows Kernel nt!MiRelocateImage Invalid Read
* Windows LSA Service LsapGetClientInfo Impersonation Level Check Privilege Escalation
* PrestaShop 1.7.6.7 Cross Site Scripting
* Sourcegraph gitserver sshCommand Remote Command Execution
* JBOSS EAP/AS 6.x Remote Code Execution
* WordPress Visual Slide Box Builder 3.2.9 SQL Injection
* Sashimi Evil OctoBot Tentacle

CXSecurity

* 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
* Pandora FMS 7.0NG.742 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

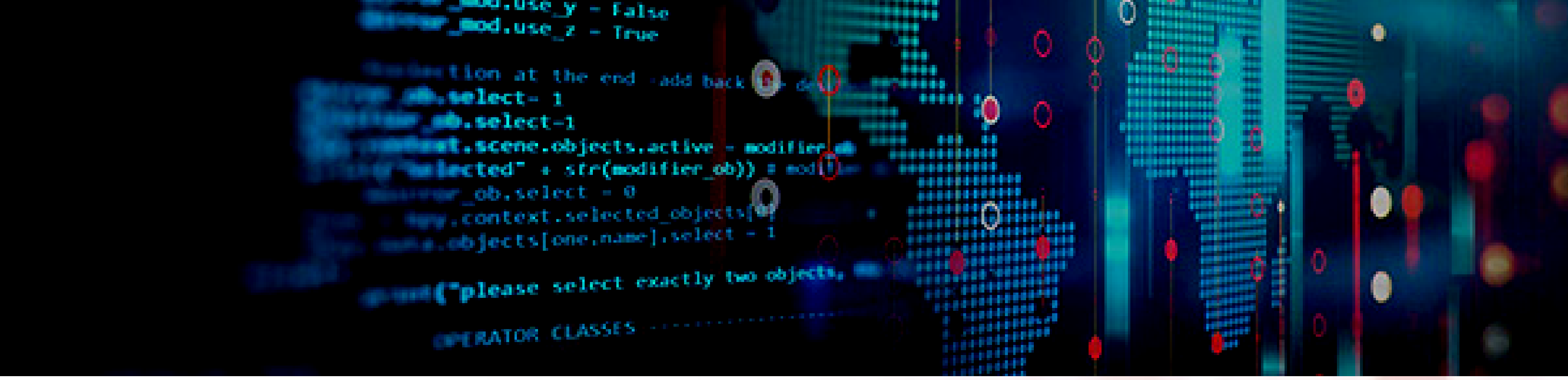
* [webapps] OctoBot WebInterface 0.4.3 - Remote Code Execution (RCE)
* [webapps] CodoForum v5.1 - Remote Code Execution (RCE)
* [local] Dr. Fone 4.0.8 - 'net_updater32.exe' Unquoted Service Path
* [webapps] Magnolia CMS 6.2.19 - Stored Cross-Site Scripting (XSS)
* [local] Kite 1.2021.610.0 - Unquoted 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)
* [remote] TP-Link Router AX50 firmware 210730 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Pandora FMS v7.0NG.742 - Remote Code Execution (RCE) (Authenticated)
* [remote] Algo 8028 Control Panel - Remote Code Execution (RCE) (Authenticated)
* [local] HP LaserJet Professional M1210 MFP Series Receive Fax Service - Unquoted Service Path
* [remote] Virtua Software Cobranca 12S - SQLi
* [remote] Marval MSM v14.19.0.12476 - Cross-Site Request Forgery (CSRF)
* [remote] Marval MSM v14.19.0.12476 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Avantune Genialcloud ProJ 10 - Cross-Site Scripting (XSS)

Exploit Database for offline use

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

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

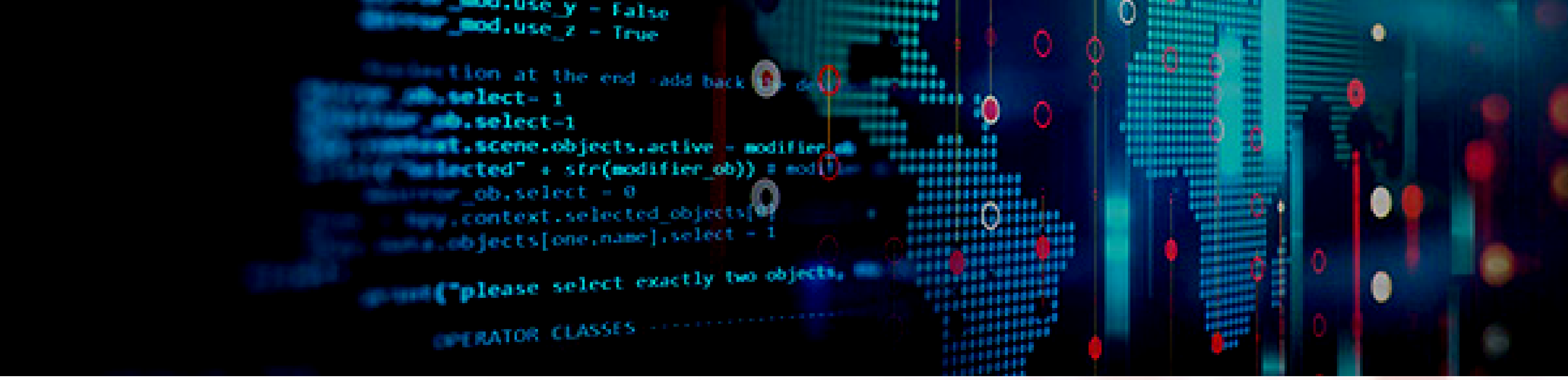
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.dec.gov.sy
http://www.dec.gov.sy notified by cyber mafia team
https://ar.gov.mn/vz.txt
https://ar.gov.mn/vz.txt notified by aDriv4
https://www.caces.gob.ec/vz.txt
https://www.caces.gob.ec/vz.txt notified by aDriv4
https://kpu-sumbawakab.go.id/readme.htm
https://kpu-sumbawakab.go.id/readme.htm notified by Mr.L3RB1
http://www.kokkrabuang.go.th/index.php
http://www.kokkrabuang.go.th/index.php notified by ./Niz4r
https://tavapy.gov.py/su.htm
https://tavapy.gov.py/su.htm notified by MR.T1T4N
https://dpmptsp1.pesisirbaratkab.go.id/read.txt
https://dpmptsp1.pesisirbaratkab.go.id/read.txt notified by Mr.L3RB1
http://setwan.pesisirbaratkab.go.id/read.txt
http://setwan.pesisirbaratkab.go.id/read.txt notified by Mr.L3RB1
http://setwan1.pesisirbaratkab.go.id/read.txt
http://setwan1.pesisirbaratkab.go.id/read.txt notified by Mr.L3RB1
https://pedrogomes.ms.gov.br/vz.txt
https://pedrogomes.ms.gov.br/vz.txt notified by aDriv4
https://dwh.ciptakarya.pu.go.id/redme.htm
https://dwh.ciptakarya.pu.go.id/redme.htm notified by Mr.L3RB1
http://sipp.pn-kasongan.go.id/read.txt
http://sipp.pn-kasongan.go.id/read.txt notified by Mr.L3RB1
http://www.cheewuek.go.th/index.php
http://www.cheewuek.go.th/index.php notified by ./Niz4r
http://www.naleng.go.th/index.php
http://www.naleng.go.th/index.php notified by ./Niz4r
https://pdk.batangharikab.go.id/upload
https://pdk.batangharikab.go.id/upload notified by Mr.L3RB1
https://lad-bsbr.batangharikab.go.id/upload
https://lad-bsbr.batangharikab.go.id/upload notified by Mr.L3RB1
https://kesbangpol.batangharikab.go.id/upload
https://kesbangpol.batangharikab.go.id/upload notified by Mr.L3RB1



Dark Web News

Darknet Live

DOJ Seized Almost $500k in Cryptocurrency from Hackers

The Department of Justice seized "approximately half a million dollars&rdquo; in cryptocurrency from accounts owned by alleged hackers. On July 19, the Justice Department announced a complaint filed in the District of Kansas to forfeit approximately half a million dollars worth of cryptocurrency from "cryptocurrency accounts&rdquo; owned by purported hackers from the Democratic People's Republic of Korea (DPRK). "Thanks to rapid reporting and cooperation from a victim, the FBI and Justice Department prosecutors have disrupted the activities of a North Korean state-sponsored group deploying ransomware known as 'Maui,'&rdquo; Deputy Attorney General Lisa O. Monaco said at the International Conference on Cyber Security. "Not only did this allow us to recover their ransom payment as well as a ransom paid by previously unknown victims, but we were also able to identify a previously unidentified ransomware strain. The approach used in this case exemplifies how the Department of Justice is attacking malicious cyber activity from all angles to disrupt bad actors and prevent the next victim.&rdquo; Deputy Attorney General Lisa O. Monaco at the International Conference on Cyber Security According to an announcement from the Department of Justice (DOJ), North Korean hackers used a ransomware strain called Maui to encrypt the files and servers of a hospital in Kansas in May 2021. After a week without access to their infrastructure and data, the hospital paid the hackers approximately $100,000 in Bitcoin to decrypt their files. After being infected by the ransomware, the hospital cooperated with law enforcement agencies, including the Federal Burea of Investigation (FBI). Because of their cooperation, the FBI identified "never-before-seen North Korean ransomware&rdquo; and traced the Bitcoin payment to a money-launderer in China. Maui ransomware encrypting files | BleepingComputer In April 2022, the FBI learned that the hackers had received another payment of approximately $120,000 worth of Bitcoin. An investigation into the payment revealed that a medical provider in Colorado had paid a ransom to the same hacking group. In May 2022, the FBI seized two cryptocurrency accounts the hackers had used to receive ransom payments. After the seizure, the District of Kansas moved to forfeit the Bitcoin and return it to the healthcare providers. "cryptocurrency accounts&rdquo; = custodial wallets Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators | archive.org, archive.is, justice.gov (via darknetlive.com at https://darknetlive.com/post/doj-seized-cryptocurrency-from-alleged-hackers/)

Woman Allegedly Tried to Hire a Hitman to Kill Her Coworker

A 26-year-old allegedly tried to hire a hitman on the darkweb to kill a colleague "when she discovered they were both having an affair&rdquo; with the same man. Whitney Franks, 26, allegedly posted an advertisement offering to pay a hitman Â£1,000 to kill a "woman has caused a lot of problems.&rdquo; A BBC journalist spotted the ad and forwarded it to the police, resulting in Franks' arrest. A family man with two children had an affair with Whitney Franks. In court, Prosecutor Andrew Copeland read part of the advertisement: '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.' 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. 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. 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. __ James Prest Later, Franks emailed Prest, asking for another chance with him. "I can give you the entire world James, if you can give me a chance I think you could be the happiest you have ever been in your life. I truly mean it. I hope you're doing well inside and out. I have been trying to sort out my anxiety. I have found some things that could help, so I'm going to give them a go.&rdquo; One day after Franks had emailed Prest for another chance, a BBC journalist found the advertisement on the darkweb. The police brought Ruutna to a safe house and questioned her about the potential hit. She told investigators that she "had a hunch&rdquo; about who was responsible for the darkweb ad. Police arrested Franks on September 10, 2020, for soliciting murder. The court heard that Franks had created an account at a cryptocurrency exchange and purchased Bitcoin, only to resell it the next day. Franks admitted accessing the darkweb but claimed she never tried to hire a hitman. (via darknetlive.com at https://darknetlive.com/post/woman-arrested-for-trying-to-hire-hitman/)

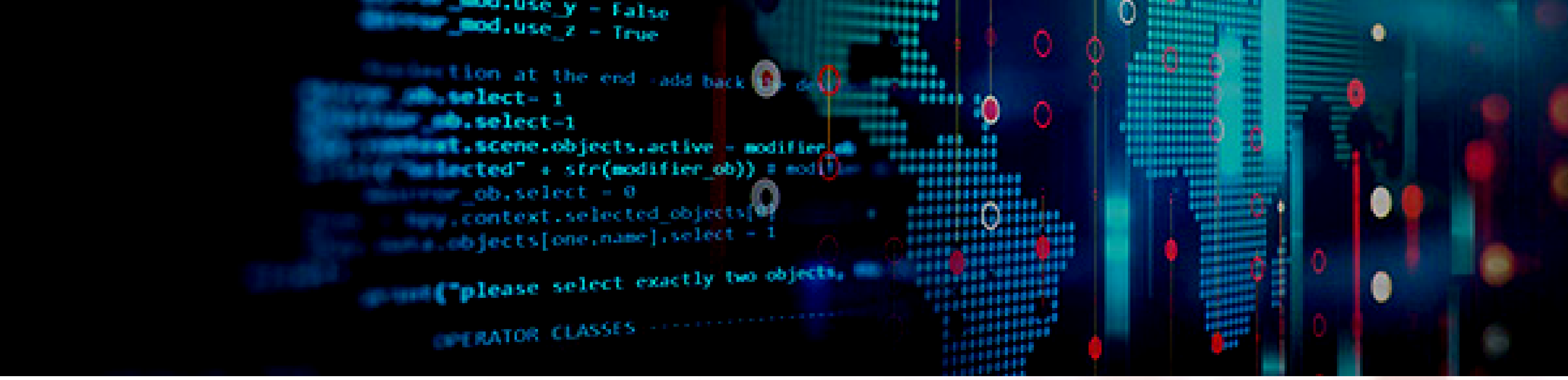
Darkweb Vendor "Dragoncove" Indicted in New York

A three-count indictment accuses a man living in New York of selling heroin and cocaine through vendor accounts on darkweb markets. An indictment was unsealed in the United States District Court for the Eastern District of New York accuses Edison Hernandez of selling drugs on Silk Road, AlphaBay, Dream Market, and Wall Street Market. According to the indictment, Hernandez: Operated a vendor account on Silk Road under the username "dragoncove&rdquo; from January 2013 to September 2013; Operated a vendor account on AlphaBay under the username "theoriginaldragoncove&rdquo; from September 2016 to June 2017; Operated a vendor account on Dream Market under the username "originaldragoncove&rdquo; from January 2019 and February 2019; and Operated a vendor account on Wall Street Market under the username "dragoncove&rdquo; in April 2019 All of Hernandez's accounts used the same PGP key. The defendant and others sold heroin and cocaine through the vendor accounts listed in the indictment. Hernandez had more than 1,000 completed transactions across his vendor accounts and "regularly received high ratings and positive reviews from buyers.&rdquo; According to dragoncove's profile on Recon, the vendor 3,774 transactions and had 1,000 transactions on Agora alone (/vendor/0xE06596B66B98549B). Count one of the indictment is Distribution and Possession with Intent to Distribute Heroin and Cocaine. Count two is the Delivery and Distribution of Heroin and Cocaine by Means of the Internet. __ Dragoncove had nearly 4,000 completed transactions on Recon. "Hernandez is alleged to have used complex technology such as the dark web, cryptocurrency, and encrypted messaging applications to conceal his actions. Today's enforcement actions are examples to high-tech criminals that no matter how well-hidden you believe you are, you are not beyond the reach of the law,&rdquo; said Homeland Security Investigations (HSI) New York Acting Special Agent in Charge Patel. "HSI and our partners will continue to work tirelessly to keep deadly narcotics out of our communities, no matter where they are sold - on the street corner or from the virtual corners of the dark web.&rdquo; A third count of the indictment accuses Edison Hernandez, Irvin Hernandez, Michael Caruso, and Raymer Ynoa of operating a so-called "a Door-to-Door Drug Delivery Service.&rdquo; The charge is one count of Conspiracy to Distribute and Possess with Intent to Distribute Cocaine, Methamphetamine, Ketamine, and MDMA. Per the indictment, the defendants operated their door-to-door drug distribution operation between February 2019 and January 2022. They named their business Nino & Viktor's Pastry Shoppe and distributed cocaine, methamphetamine, ketamine, and 3,4 Methylenedioxymethamphetamine, also known as MDMA or ecstasy, to others through the delivery service. __ Most of the vendor's feedback was positive. Customers ordered from the shop by messaging a "particular phone number over an encrypted communication platform.&rdquo; The defendants had a menu of coded products that customers could order. The announcement from the U.S. Attorney's Office for the Eastern District of New York provided some examples: the defendants referred to cocaine as "grapes&rdquo; and methamphetamine as "tic tacs.&rdquo; In addition, customers ordered drugs not by weight but by "unit,&rdquo; with each unit costing $100, regardless of the drug. Hence, a customer who ordered "two grapes&rdquo; and "two tic tacs&rdquo; would pay a total of $400 for two "units&rdquo; of cocaine and two "units&rdquo; of methamphetamine. "As alleged, Edison Hernandez went to great lengths to conceal his identity so he could send thousands of packages containing dangerous drugs throughout the country and team up with his co-conspirators to deliver them door-to-door in New York City,&rdquo; stated United States Attorney Peace. "Hiding behind the dark web, encryption services, or BitCoin will not stop this Office from rooting out those who flood our communities with illegal and hazardous narcotics.&rdquo; Dark Web Vendor of Illegal Narcotics Indicted for Distributing Heroin and Cocaine in Exchange for Bitcoin | archive.is, archive.org, justice.gov Indictment pdf (via darknetlive.com at https://darknetlive.com/post/new-york-man-in-quotation-marks-arrested-for-selling-drugs/)

Italian Man Allegedly Hired a Hitman on the Darkweb

According to Italian law enforcement, a man from the Province of Treviso attempted to hire a hitman on the darkweb to kill his romantic rival. __ This image was part of the police's media release The Federal Bureau of Investigation in the United States notified law enforcement agencies in Italy that someone had targeted a 45-year-old man from Conegliano through a murder-for-hire site on the darkweb. Local authorities discretely alerted the intended victim of the hit. By tracing the payment, investigators with the Postal and Communications Police identified the person responsible for paying for the hit. They "tracked the movemenent of cryptocurrencies from the virtual wallet of the suspect to the administrator of the site.&rdquo; The investigation resulted in the identification of a 34-year-old man from the province of Treviso as the suspect. __ What is the blurred website? The suspect allegedly wanted to "freely court&rdquo; the intended victim's girlfriend, with whom the suspect was "secretly in love.&rdquo; By eliminating the competition, the suspect believed he would have a chance with the woman. __ Dread? Police referred the information to prosecutors. According to the police, the case is an example of Italian law enforcement's "modern investigative techniques.&rdquo; "The whole judicial affair is characterized by some novel aspects that deserve to be highlighted. The successful identification of a user operating on the darkweb testifies that the non-indexed part of the internet, where illicit goods and services are freely offered, hitherto considered impenetrable by the Police, is no longer so. Indeed, modern investigative techniques used by the Postal and Communications Police, particularly those for tracking cryptocurrency payments, make it possible, as in this case, to trace cryptocurrency wallet holders.&rdquo;   LA POLIZIA DI STATO IDENTIFICA IL MANDANTE DI UN OMICIDIO SUL DARKWEB | archive.is, archive.org, commissariatodips.it (via darknetlive.com at https://darknetlive.com/post/italian-man-cited-for-hiring-hitman-on-the-darkweb/)

Dark Web Link



Trend Micro Anti-Malware Blog

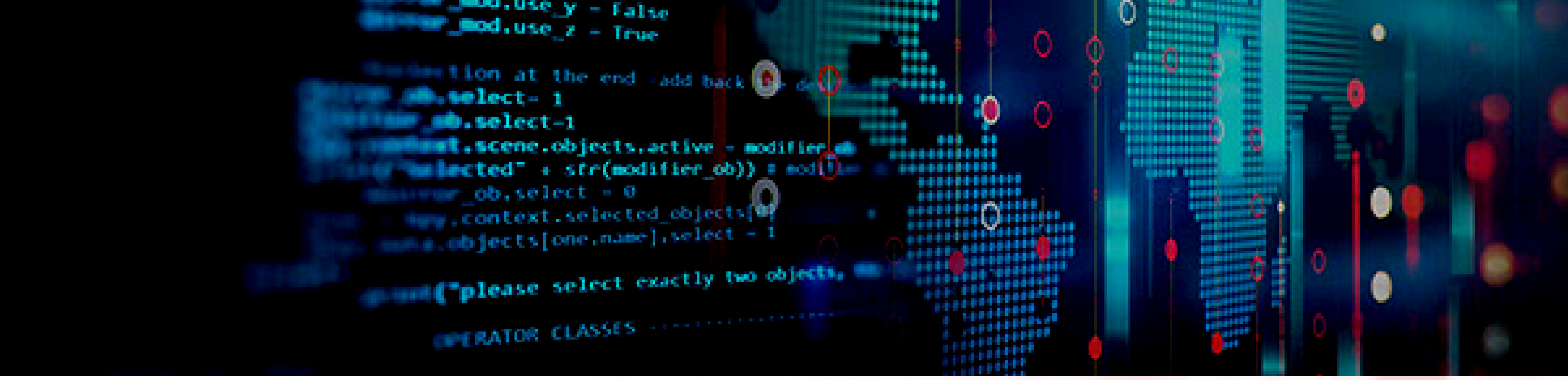
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Cloud Threat Detection: To Agent or Not to Agent?
* Simplify SIEM Optimization With InsightIDR
* 4 key statistics to build a business case for an MDR partner
* Deploying a SOAR Tool Doesn't Have to Be Hard: I've Done It Twice
* [Security Nation] Jacques Chester of Shopify Talks CVSS Scores
* 4 Strategies for Achieving Greater Visibility in the Cloud
* Gimme! Gimme! Gimme! (More Data): What Security Pros Are Saying
* CVE-2022-30526 (Fixed): Zyxel Firewall Local Privilege Escalation
* Deploy tCell More Easily With the New AWS AMI Agent



Advisories

US-Cert Alerts & bulletins

* 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;
* CNMF Discloses Malware in Ukraine
* Oracle Releases July 2022 Critical Patch Update
* CISA released Security Advisory on MiCODUS MV720 Global Positioning System (GPS) Tracker
* 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 11, 2022
* Vulnerability Summary for the Week of July 4, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Apple Security Advisory 2022-07-20-7

Apple Security Advisory Safari - Safari 15.6 addresses code execution and out of bounds write vulnerabilities.

Apple Security Advisory 2022-07-20-6

Apple Security Advisory 2022-07-20-6 - watchOS 8.7 addresses buffer overflow, bypass, code execution, out of bounds read, out of bounds write, and spoofing vulnerabilities.

Apple Security Advisory 2022-07-20-5

Apple Security Advisory 2022-07-20-5 - tvOS 15.6 addresses buffer overflow, bypass, code execution, information leakage, out of bounds read, out of bounds write, and spoofing vulnerabilities.

Apple Security Advisory 2022-07-20-4

Apple Security Advisory 2022-07-20-4 - Security Update 2022-005 Catalina addresses code execution, information leakage, null pointer, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2022-07-20-3

Apple Security Advisory 2022-07-20-3 - macOS Big Sur 11.6.8 addresses code execution, information leakage, null pointer, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2022-07-20-2

Apple Security Advisory 2022-07-20-2 - macOS Monterey 12.5 addresses bypass, code execution, information leakage, null pointer, out of bounds read, out of bounds write, and spoofing vulnerabilities.

Apple Security Advisory 2022-07-20-1

Apple Security Advisory 2022-07-20-1 - iOS 15.6 and iPadOS 15.6 addresses buffer overflow, bypass, code execution, information leakage, null pointer, out of bounds read, out of bounds write, and spoofing vulnerabilities.

Ubuntu Security Notice USN-5529-1

Ubuntu Security Notice 5529-1 - It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Yongkang Jia discovered that the KVM hypervisor implementation in the Linux kernel did not properly handle guest TLB mapping invalidation requests in some situations. An attacker in a guest VM could use this to cause a denial of service in the host OS.

Red Hat Security Advisory 2022-5673-01

Red Hat Security Advisory 2022-5673-01 - Red Hat OpenStack Platform 16.2 (Train) director operator containers, with several Important security fixes, are available for technology preview. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5528-1

Ubuntu Security Notice 5528-1 - It was discovered that FreeType did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5525-1

Ubuntu Security Notice 5525-1 - It was discovered that Apache XML Security for Java incorrectly passed a configuration property when creating specific key elements. This allows an attacker to abuse an XPath Transform to extract sensitive information.

Ubuntu Security Notice USN-5527-1

Ubuntu Security Notice 5527-1 - It was discovered that Checkmk incorrectly handled authentication. An attacker could possibly use this issue to cause a race condition leading to information disclosure. It was discovered that Checkmk incorrectly handled certain inputs. An attacker could use these cross-site scripting issues to inject arbitrary html or javascript code to obtain sensitive information including user information, session cookies and valid credentials.

Ubuntu Security Notice USN-5526-1

Ubuntu Security Notice 5526-1 - Aapo Oksman discovered that PyJWT incorrectly handled signatures constructed from SSH public keys. A remote attacker could use this to forge a JWT signature.

Ubuntu Security Notice USN-5524-1

Ubuntu Security Notice 5524-1 - It was discovered that HarfBuzz incorrectly handled certain glyph sizes. A remote attacker could use this issue to cause HarfBuzz to crash, resulting in a denial of service.

Ubuntu Security Notice USN-5523-1

Ubuntu Security Notice 5523-1 - It was discovered that LibTIFF was not properly performing checks to guarantee that allocated memory space existed, which could lead to a NULL pointer dereference via a specially crafted file. An attacker could possibly use this issue to cause a denial of service. It was discovered that LibTIFF was not properly performing checks to avoid division calculations where the denominator value was zero, which could lead to an undefined behavior situation via a specially crafted file. An attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5520-2

Ubuntu Security Notice 5520-2 - USN-5520-1 fixed a vulnerability in HTTP-Daemon. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that HTTP-Daemon incorrectly handled certain crafted requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Ubuntu Security Notice USN-5522-1

Ubuntu Security Notice 5522-1 - Several security issues were discovered in WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Ubuntu Security Notice USN-5519-1

Ubuntu Security Notice 5519-1 - It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5520-1

Ubuntu Security Notice 5520-1 - It was discovered that HTTP-Daemon incorrectly handled certain crafted requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Ubuntu Security Notice USN-5518-1

Ubuntu Security Notice 5518-1 - It was discovered that the eBPF implementation in the Linux kernel did not properly prevent writes to kernel objects in BPF_BTF_LOAD commands. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the Marvell NFC device driver implementation in the Linux kernel did not properly perform memory cleanup operations in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5517-1

Ubuntu Security Notice 5517-1 - It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, 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 virtio RPMSG bus driver in the Linux kernel contained a double-free vulnerability in certain error conditions. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-5516-1

Ubuntu Security Notice 5516-1 - It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution.

Ubuntu Security Notice USN-5515-1

Ubuntu Security Notice 5515-1 - Eric Biederman discovered that the cgroup process migration implementation in the Linux kernel did not perform permission checks correctly in some situations. A local attacker could possibly use this to gain administrative privileges. Jann Horn discovered that the FUSE file system in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5514-1

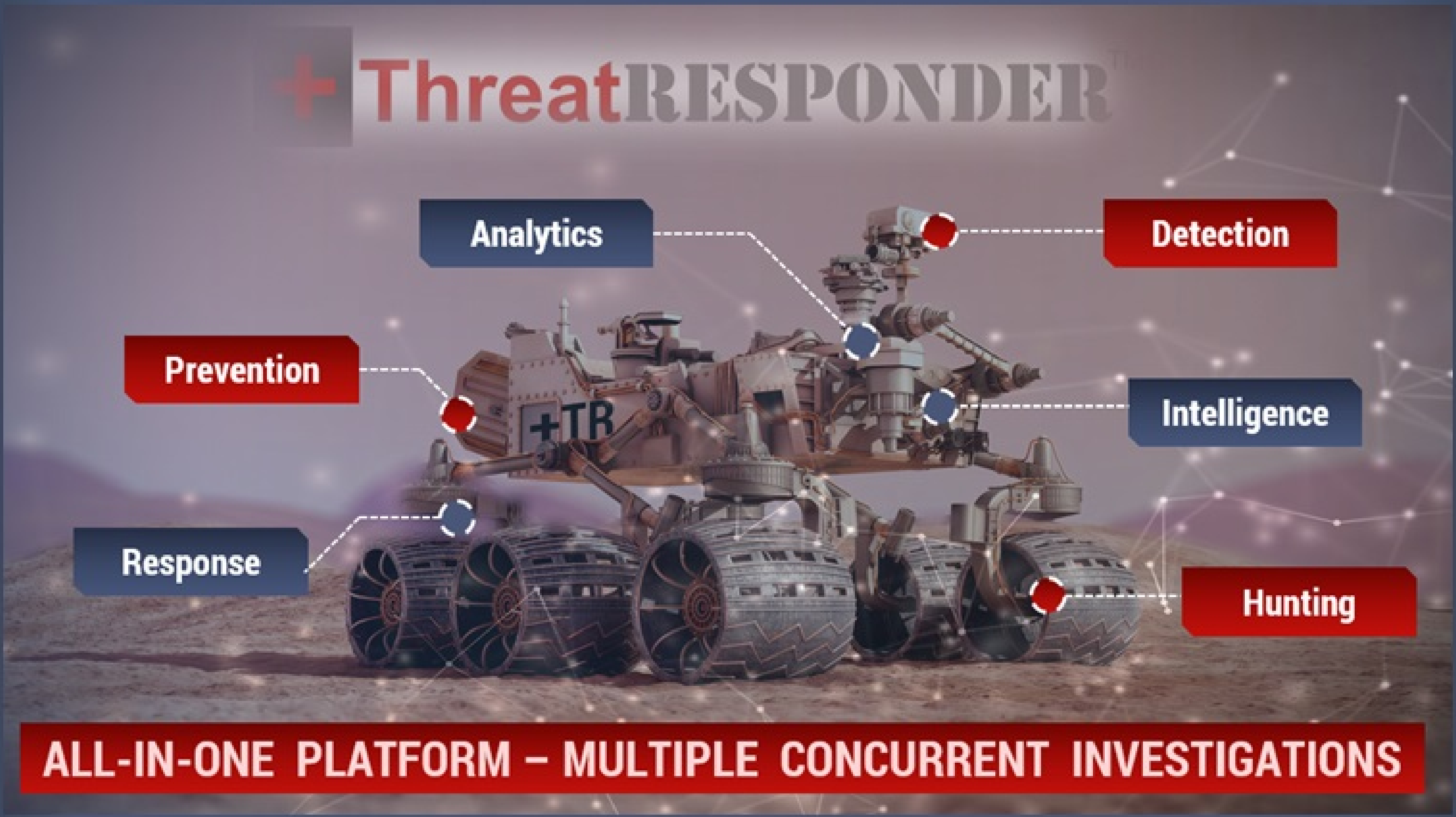
Ubuntu Security Notice 5514-1 - It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service. Duoming 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.

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



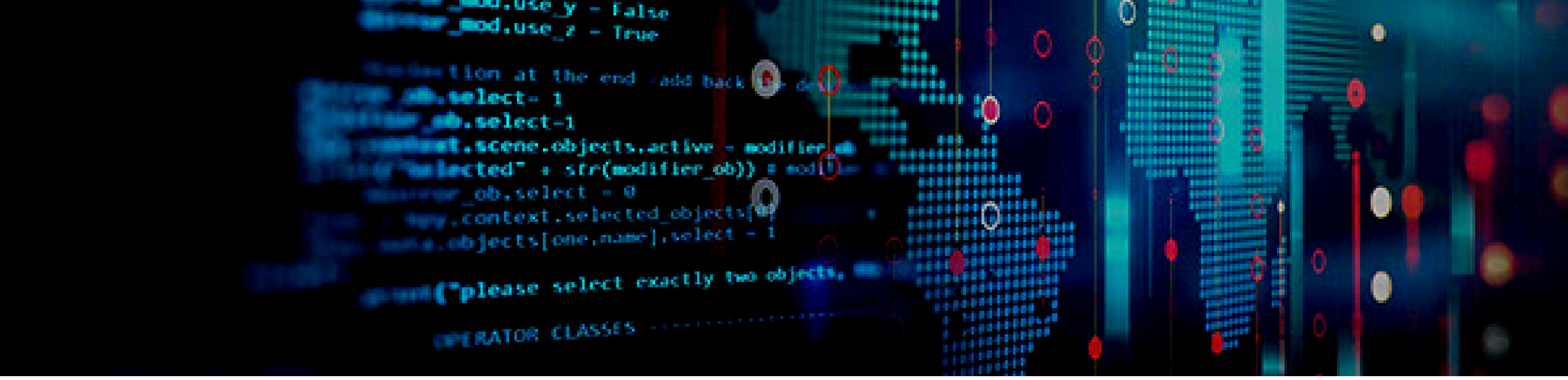
The Solution – ThreatResponder® Platform

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



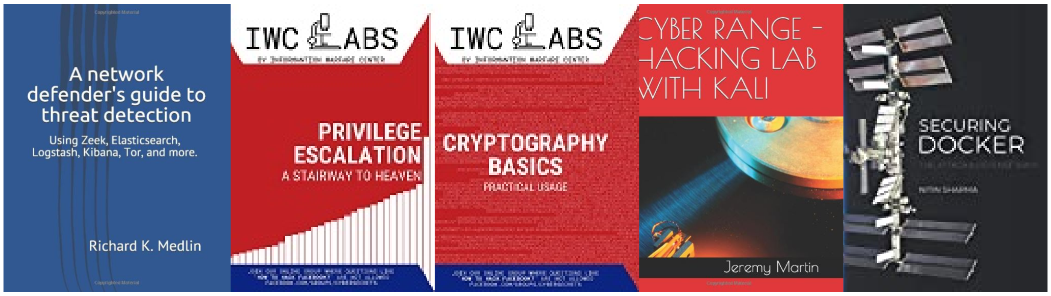
The Cyber Secrets publications on Amazon

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
Information Warfare Center
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
CYBER SECRETS
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
SOCRANGE
LINUX
CYBER SECRETS
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
CYBER SECRETS
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
CYBER SECRETS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

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