May-09-22

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

May 9, 2022

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

Summary

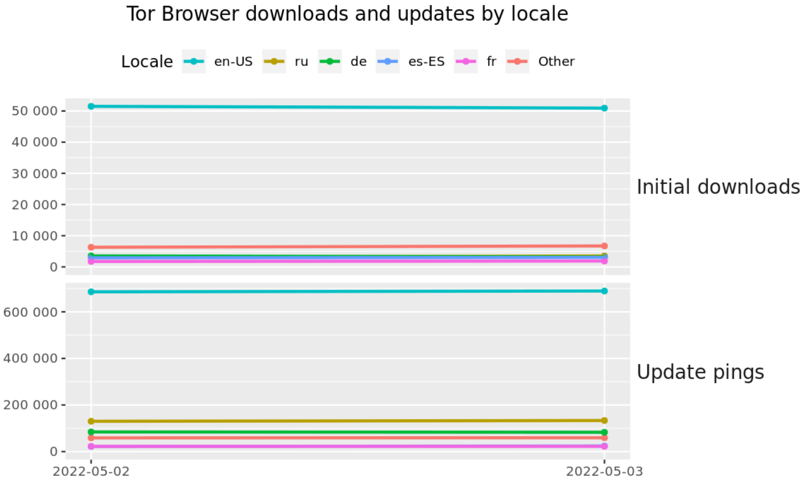
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

LATEST NEWS

Packet Storm Security

* Here's How The Lazarus Hackers Start Their Attacks
* USB-Based Wormable Malware Targets Windows Installer
* Catalans Demand Answers After Spanish Spy Chief Confirms Phone Hacking
* Russia Hammered By Pro-Ukrainian Hackers After Invasion
* Gucci Stores To Accept Crypto Currencies In US
* New Framework Aims To Secure Digital Health Apps Not Covered By HIPAA
* Ridiculous Ransomware Kill Switch
* Stung By 3 Court Losses, ISPs Stop Fighting California's Net Neutrality Law
* VHD Ransomware Linked To North Korea's Lazarus Group
* Avast Patches Decades Old Vulnerabilities In Antivirus Product
* Attackers Use Event Logs To Hide Fileless Malware
* Vulnerabilities Allow Hijacking Of Most Ransomware To Prevent File Encryption
* SEC Nearly Doubles Crypto Currency Cop Roles In Special Cyber Unit
* Unpatched DNS Bug Puts Millions Of Routers, IoT Devices At Risk
* White House Boosting Quantum Technology And Cybersecurity
* This Sneaky Hacking Group Hid Inside Networks For 18 Months Without Being Detected
* Crypto Hackers Have Stolen More Than $370 Million In April Alone
* Aruba, Avaya Network Switches Vulnerable To SSL Flaws
* Spanish Prime Minister's Phone Targeted With Pegasus Spyware
* Botnet That Hid For 18 Months Boasted Some Of The Coolest Tradecraft Ever
* Mozilla Finds Mental Health Apps Fail Spectacularly At User Security, Data Policies
* Data-Wiper Malware Surges As Ukraine Battles Ongoing Invasion
* Wikimedia Foundation Stops Accepting Cryptocurrency As Donations
* Meta, Tracking Code, And The Student Financial Aid Website
* Vulnerable Plugins Plague The CMS Website Security Landscape

Krebs on Security

* Your Phone May Soon Replace Many of Your Passwords
* Russia to Rent Tech-Savvy Prisoners to Corporate IT?
* You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
* Fighting Fake EDRs With 'Credit Ratings' for Police
* Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code
* Conti's Ransomware Toll on the Healthcare Industry
* Microsoft Patch Tuesday, April 2022 Edition
* RaidForums Gets Raided, Alleged Admin Arrested
* Double-Your-Crypto Scams Share Crypto Scam Host
* Actions Target Russian Govt. Botnet, Hydra Dark Market

LATEST NEWS

Dark Reading

* Post-Quantum Cryptography Set to Replace RSA, ECC
* Ikea Canada Breach Exposes 95K Customer Records
* What We've Learned in the 12 Months Since the Colonial Pipeline Attack
* Scammer Infects His Own Machine with Spyware, Reveals True Identity
* White House Moves to Shore Up US Post-Quantum Cryptography Posture
* AT&T Expands Access to Advanced Secure Edge and Remote Workforce Capabilities
* Passwords: Do Actions Speak Louder Than Words?
* Colonial Pipeline 1 Year Later: What Has Yet to Change?
* Microsoft, Apple, and Google Promise to Expand Passwordless Features
* Heroku: Cyberattacker Used Stolen OAuth Tokens to Steal Customer Account Credentials
* NIST Issues Guidance for Addressing Software Supply-Chain Risk
* A Third of Americans Use Easy-to-Guess Pet Passwords
* Critical Cisco VM-Escape Bug Threatens Host Takeover
* FBI: Bank Losses From BEC Attacks Top $43B
* Magnet Forensics Acquires Cybersecurity Software Firm Comae Technologies
* Cisco Announces Cloud Controls Framework Is Now Available to Public
* Multichannel Phishing Concerns Cybersecurity Leaders in 2022
* 1,000+ Attacks in 2 Years: How the SideWinder APT Sheds Its Skin
* Docker Under Siege: Cybercriminals Compromise Honeypots to Ramp Up Attacks
* Why Security Matters Even More in Online Gaming

The Hacker News

* Ukrainian CERT Warns Citizens of a New Wave of Attacks Distributing Jester Malware
* U.S. Offering $10 Million Reward for Information on Conti Ransomware Hackers
* Researchers Develop RCE Exploit for the Latest F5 BIG-IP Vulnerability
* U.S. Sanctions Cryptocurrency Mixer Blender for Helping North Korea Launder Millions
* This New Fileless Malware Hides Shellcode in Windows Event Logs
* QNAP Releases Firmware Patches for 9 New Flaws Affecting NAS Devices
* Researchers Warn of 'Raspberry Robin' Malware Spreading via External Drives
* Hackers Using PrivateLoader PPI Service to Distribute New NetDooka Malware
* Experts Uncover New Espionage Attacks by Chinese 'Mustang Panda' Hackers
* Google Releases Android Update to Patch Actively Exploited Vulnerability
* NIST Releases Updated Cybersecurity Guidance for Managing Supply Chain Risks
* Google to Add Passwordless Authentication Support to Android and Chrome
* The Importance of Defining Secure Code
* Researchers Disclose Years-Old Vulnerabilities in Avast and AVG Antivirus
* Heroku Forces User Password Resets Following GitHub OAuth Token Theft

LATEST NEWS

Security Week

* Zero Trust VPN Company Tailscale Raises $100 Million
* Heroku Shares Details on Recent GitHub Attack
* Tech Giants Unite in Effort to Scrap Passwords
* China Not Happy With South Korea Joining NATO Cyber Defense Center
* Amazon's Shuttering of Alexa Ranking Service Hits Cybersecurity Industry
* US Cyber Command Team Helps Lithuania Protect Its Networks
* Catalan: Spain Spy Chief Admits Legally Hacking Some Phones
* GitHub Announces Mandatory 2FA for Code Contributors
* US Gov Issues Security Memo on Quantum Computing Risks
* Android's May 2022 Security Updates Patch 36 Vulnerabilities
* AutoRABIT Raises $26 Million for Salesforce DevSecOps Platform
* OT Security Firm Network Perception Raises $13 Million
* Flaws in Avast, AVG Antiviruses Could Have Facilitated Attacks on Millions of Devices
* FBI: Losses From BEC Scams Surpass $43 Billion
* Cisco Patches Critical VM Escape in NFV Infrastructure Software
* Idaho Needs to Shore Up Cybersecurity, Task Force Says
* EU Hands Police Agency New Powers Over Personal Data
* Kaspersky Warns of Fileless Malware Hidden in Windows Event Logs
* Google Sees More APTs Using Ukraine War-Related Themes
* Hubble Technology Banks $9 Million for Asset Visibility Platform
* F5 Warns BIG-IP Customers About 18 Serious Vulnerabilities
* China-Linked Winnti APT Group Silently Stole Trade Secrets for Years: Report
* Webinar Today: Blast Radius & Simulated Attack Paths
* Cisco Issues Fresh Warning Over Counterfeit Switches
* Application Security Firm ShiftLeft Raises $29 Million
* Chinese Hackers Abuse Cybersecurity Products for Malware Execution

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* 10 of the Craziest Cyberattacks Seen In the Wild and How You Can Avoid Them
* Your KnowBe4 Fresh Content Updates from April 2022
* Cozy Bear Goes Typosquatting
* Microsoft is Leading the Way to a Password-Less Future
* SMTP Relay Email Spoofing Technique
* 89% of Organizations Experienced One or More Successful Email Breach Types During the Last 12 Months
* FIN12 Threat Group Speeds Up Ransomware Attacks to Just Two Days After Initial Access
* Organizations Have a 76% Likelihood of a Successful Cyberattack in the Next Year
* CyberheistNews Vol 12 #18 [Heads Up] The 4 Major Tactics: How Hackers Steal Your Passwords and How To
* Man Convicted for $23 Million Phishing Scam Against the US DoD

ISC2.org Blog

* Board, (Dash)board and Bored
* CCSP Exam - Many Changes on the Way!
* (ISC)&sup2; Hellenic Chapter Wins Award for Creating Educational Materials
* CLOUD: A SHAKESPEAREAN DRAMA?
* Quantum Cybersecurity: Addressing the Boogeyman in the Room

HackRead

* Anonymous NB65 Claims Hack on Russian Payment Processor Qiwi
* USB-based Wormable Raspberry Robin Malware Targeting Windows Installer
* DDoS Attacks by Hacktivists Disrupted Russian Alcohol Supply Chain
* The Operational Structure of Bitcoin
* What Are Dark Web Search Engines and How to Find Them?
* CIA Wants Russians to Share Secret Info with the Agency via its Darknet Site
* India to Collect User Data from VPNs, Data Centers, and Cloud Service Providers

Koddos

* Anonymous NB65 Claims Hack on Russian Payment Processor Qiwi
* USB-based Wormable Raspberry Robin Malware Targeting Windows Installer
* DDoS Attacks by Hacktivists Disrupted Russian Alcohol Supply Chain
* The Operational Structure of Bitcoin
* What Are Dark Web Search Engines and How to Find Them?
* CIA Wants Russians to Share Secret Info with the Agency via its Darknet Site
* India to Collect User Data from VPNs, Data Centers, and Cloud Service Providers

LATEST NEWS

Naked Security

* You didn't leave enough space between ROSE and AND, and AND and CROWN
* S3 Ep81: Passwords (still with us!), Github, Firefox at 100, and network worms [Podcast]
* World Password Day - the 1960s just called and gave you your passwords back
* Android monthly updates are out - critical bugs found in critical places!
* Firefox hits 100*, fixes bugs&hellip; but no new zero-days this month
* GitHub issues final report on supply-chain source code intrusions
* S3 Ep80: Ransomware news, phishing woes, NAS bugs, and a giant hole in Java [Podcast]
* Ransomware Survey 2022 - like the Curate's Egg, "good in parts"
* Phishing goes KISS: Don't let plain and simple messages catch you out!
* QNAP warns of new bugs in its Network Attached Storage devices

Threat Post

* USB-based Wormable Malware Targets Windows Installer
* CANs Reinvent LANs for an All-Local World
* F5 Warns of Critical Bug Allowing Remote Code Execution in BIG-IP Systems
* VHD Ransomware Linked to North Korea's Lazarus Group
* China-linked APT Caught Pilfering Treasure Trove of IP
* Attackers Use Event Logs to Hide Fileless Malware
* Unpatched DNS Bug Puts Millions of Routers, IoT Devices at Risk
* Mozilla: Lack of Security Protections in Mental-Health Apps Is 'Creepy'
* Bad Actors Are Maximizing Remote Everything
* Deep Dive: Protecting Against Container Threats in the Cloud

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

* shinytest2, Rhino R Shiny framework top news at Appsilon conference
* Leaving cloud scalability to automation
* What is PyTorch? Python machine learning on GPUs
* Will JavaScript containers overtake Linux containers?
* JDK 19: The features targeted for Java 19
* MongoDB CTO: What today's developers need to succeed
* Making AI accountable: Blockchain, governance, and auditability
* GitHub will require two-factor authentication for all coders
* Spotify, startups launch funds to support open source maintainers
* Pulumi extends infrastructure as code support for Java and YAML

C4ISRNET - Media for the Intelligence Age Military

* Defense Innovation Unit chief to resign in September
* Atlantic Council urges Pentagon to utilize commercial space capabilities
* Satellite service provider EchoStar posts Q1 earnings
* Satellite comms firm Telesat unveils first-quarter earnings
* US gave intel before Ukraine sank Russian warship, says official
* Anduril Industries in talks with Australia on autonomous undersea vehicle
* Pentagon denies US intelligence is targeting Russian generals in Ukraine
* US cyber squad boosts Lithuanian defenses amid Russian threat
* DARPA's nuclear space propulsion project advances to next phase
* New Zealand rocket caught but then dropped by helicopter

The Hacker Corner

Conferences

* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021
* Is It Worth Public Speaking?

Google Zero Day Project

* The More You Know, The More You Know You Don't Know
* CVE-2021-1782, an iOS in-the-wild vulnerability in vouchers

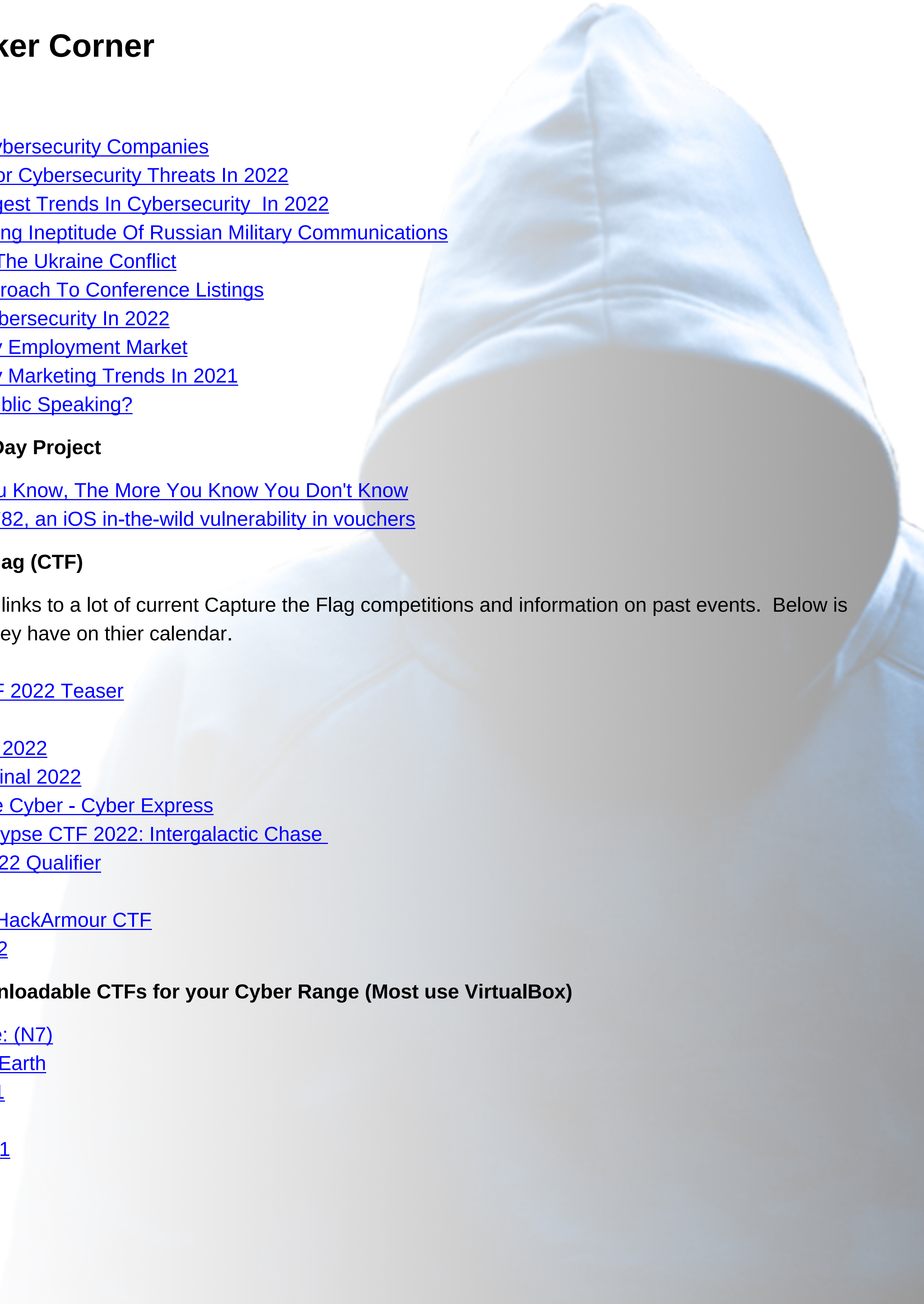
Capture the Flag (CTF)

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.

* m0leCon CTF 2022 Teaser
* TJCTF 2022
* CTF InterIUT 2022
* @HackDay Final 2022
* Challenge the Cyber - Cyber Express
* Cyber Apocalypse CTF 2022: Intergalactic Chase
* VolgaCTF 2022 Qualifier
* 404 CTF
* hackrocks & HackArmour CTF
* saarCTF 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

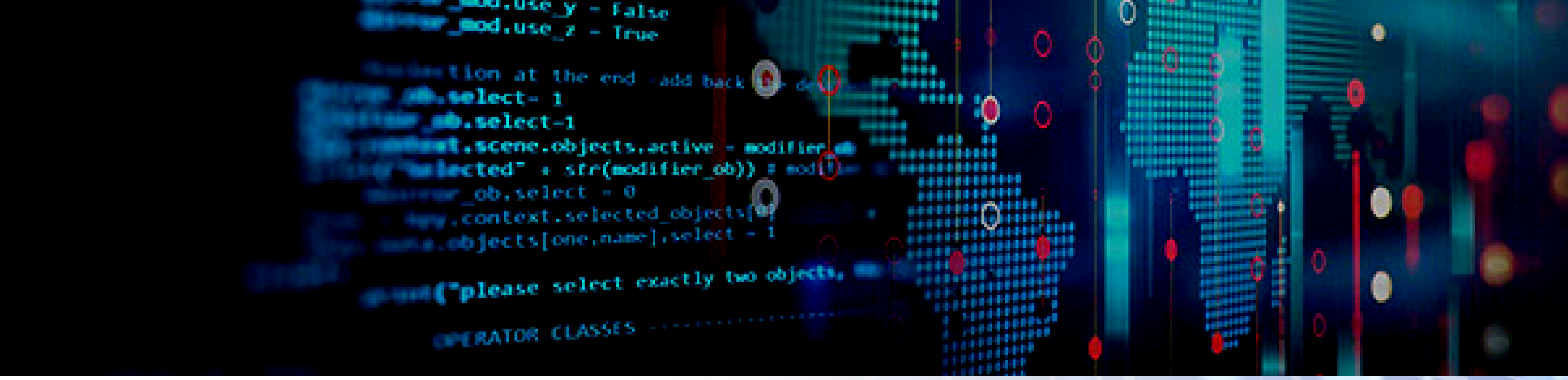
* Adversary3 2.0
* Wireshark Analyzer 3.6.5
* Clam AntiVirus Toolkit 0.105.0
* OpenSSL Toolkit 3.0.3
* OpenSSL Toolkit 1.1.1o
* Samhain File Integrity Checker 4.4.8
* TOR Virtual Network Tunneling Tool 0.4.7.7
* nfstream 6.5.1
* GNU Privacy Guard 2.2.35
* Mandos Encrypted File System Unattended Reboot Utility 1.8.15

Kali Linux Tutorials

* FastFinder : Incident Response - Fast Suspicious File Finder
* Oh365UserFinder : Python3 O365 User Enumeration Tool
* PSRansom : PowerShell Ransomware Simulator With C2 Server
* S3Sec : Check AWS S3 Instances For Read/Write/Delete Access
* Nuclei-Burp-Plugin : Nuclei Plugin For BurpSuite
* Ghostbuster : Eliminate Dangling Elastic IPs By Performing Analysis On Your Resources
* Kali Linux - The Best Tool For Penetration Testing?
* Epagneul : Graph Visualization For Windows Event Logs
* S1EM : This Project Is A SIEM With SIRP And Threat Intel, All In One
* What Makes An Online Poker Platform Stand Out?

GBHackers Analysis

* Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level
* Critical RCE Vulnerability in Google's VirusTotal Platform Let Attackers Scans Capabilities
* Critical Android Bug Let Attackers to Access Users' Media and Audio Conversations
* 15-Year-old Security Vulnerability In The PEAR PHP Repository Permits Supply Chain Attack
* Honda Bug Let Attackers Unlock and Start the Car



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Inside FOR710 Reverse-Engineering Malware: Advanced Code Analysis
* The New GIAC MacOS and iOS Examiner Certification (GIME)
* SANS Threat Analysis Rundown | Katie Nickels
* SANS Threat Analysis Rundown

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

* Use PineAP to Create Rogue WiFi Networks (KARMA on the WiFi Pineapple)
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Live Hacking Q&A with Kody Kinzie & Alex Lynd: WiFi Half Handshake Attacks, WiFi Nugget Development

The PC Security Channel [TPSC]

* How to tell if your Wifi is hacked?
* Avast vs Ransomware | Compared with Windows Defender

Eli the Computer Guy

* NETFLIX BEING SUED for FRAUD
* ELON MUSK FIRING TWITTER EMPOYEES
* NETFLIX is SOOO DEAD - daily blob COVID edition
* COVID SUCKS, but it's getting better - AND DOJO DERBY MEETUP SCHEDULED

Security Now

* Global Privacy Control - DoD DIB-VDP, OpenSSF's Package Analysis Project, Connecticut Privacy
* The 0-Day Explosion - Lenovo EUFI Firmware, Everscale Blockchain Wallet, Major Java Update

Troy Hunt

* Weekly Update 294

Intel Techniques: The Privacy, Security, & OSINT Show

* 260-Google's New Policy Change
* 259-Leaving Kindle

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Trojan-Ransom.Radamant Code Execution
* Trojan.CryptoLocker Code Execution
* Craft CMS 3.7.36 Password Reset Poisoning Attack
* Ransom.CTBLocker Code Execution
* Trojan-Ransom.Cerber Code Execution
* Trojan-Ransom.LockerGoga Code Execution
* ChatBot Application With A Suggestion Feature 1.0 SQL Injection
* Trojan.Ransom.Cryptowall Code Execution
* REvil.Ransom Code Execution
* ZoneMinder Language Settings Remote Code Execution
* PHProjekt PhpSimplyGest / MyProjects 1.3.0 Cross Site Scripting
* SAP Web Dispatcher HTTP Request Smuggling
* Red Planet Laundry Management System 1.0 SQL Injection
* Ransom.WannaCry Code Execution
* REvil.Ransom Code Execution
* Ransom.Conti Code Execution
* Conti.Ransom Code Execution
* RedLine.Stealer Code Execution
* REvil Ransom Code Execution
* Conti Ransom Code Execution
* LokiLocker Ransom Code Execution
* BlackBasta Ransom Code Execution
* Ransom.AvosLocker Code Execution
* VMware Workspace ONE Access Template Injection / Command Execution
* Tenda HG6 3.3.0 Remote Command Injection

CXSecurity

* VMware Workspace ONE Access Template Injection / Command Execution
* Watch Queue Out-Of-Bounds Write
* Easy Appointments 1.4.2 Information Disclosure
* ManageEngine ADSelfService Plus Custom Script Execution
* USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor
* ManageEngine ADSelfService Plus 6.1 User Enumeration
* WordPress Elementor 3.6.2 Shell Upload

Proof of Concept (PoC) & Exploits

Exploit Database

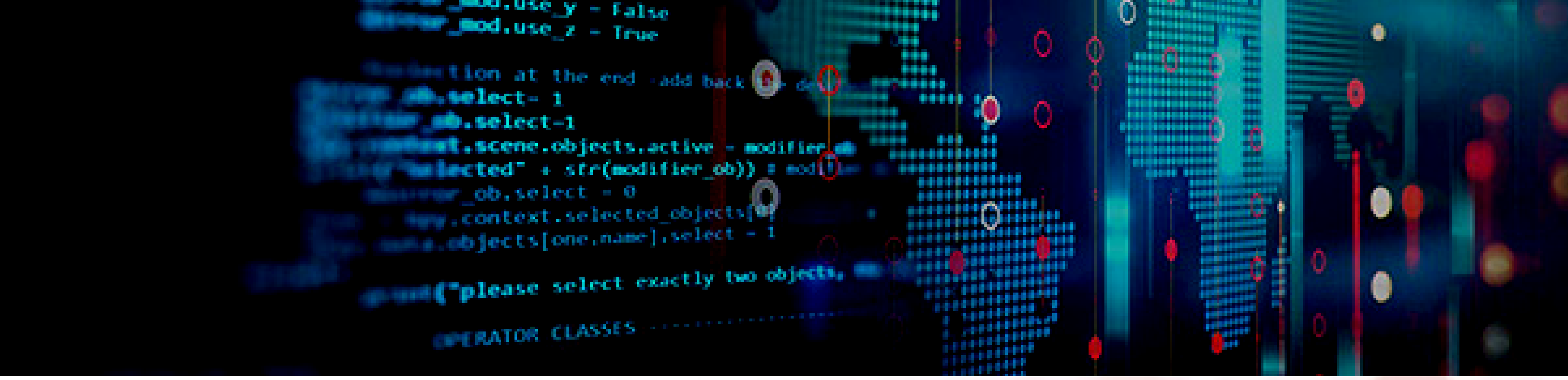
* [webapps] GitLab 14.9 - Stored Cross-Site Scripting (XSS)
* [webapps] Gitlab 14.9 - Authentication Bypass
* [local] EaseUS Data Recovery - 'ensserver.exe' Unquoted Service Path
* [local] PTPublisher v2.3.4 - Unquoted Service Path
* [webapps] Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin Elementor 3.6.2 - Remote Code Execution (RCE) (Authenticated)
* [webapps] PKP Open Journals System 3.3 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cookie User Password Disclosure
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Request Forgery (CSRF)
* [webapps] REDCap 11.3.9 - Stored Cross Site Scripting
* [webapps] WordPress Plugin Popup Maker 1.16.5 - Stored Cross-Site Scripting (Authenticated)
* [remote] Verizon 4G LTE Network Extender - Weak Credentials Algorithm
* [webapps] WordPress Plugin Videos sync PDF 1.7.4 - Stored Cross Site Scripting (XSS)
* [remote] ManageEngine ADSelfService Plus 6.1 - User Enumeration
* [webapps] Scriptcase 9.7 - Remote Code Execution (RCE)
* [webapps] Easy Appointments 1.4.2 - Information Disclosure
* [remote] Zyxel NWA-1100-NH - Command Injection
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - SQL Injection
* [local] Microsoft Exchange Active Directory Topology 15.0.847.40 - 'Service MSExchangeADTopology' Unq
* [local] Microsoft Exchange Mailbox Assistants 15.0.847.40 - 'Service MSExchangeMailboxAssistants' Unq
* [webapps] Razer Sila - Command Injection
* [webapps] Razer Sila - Local File Inclusion (LFI)
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Deletion
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Creation

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
```

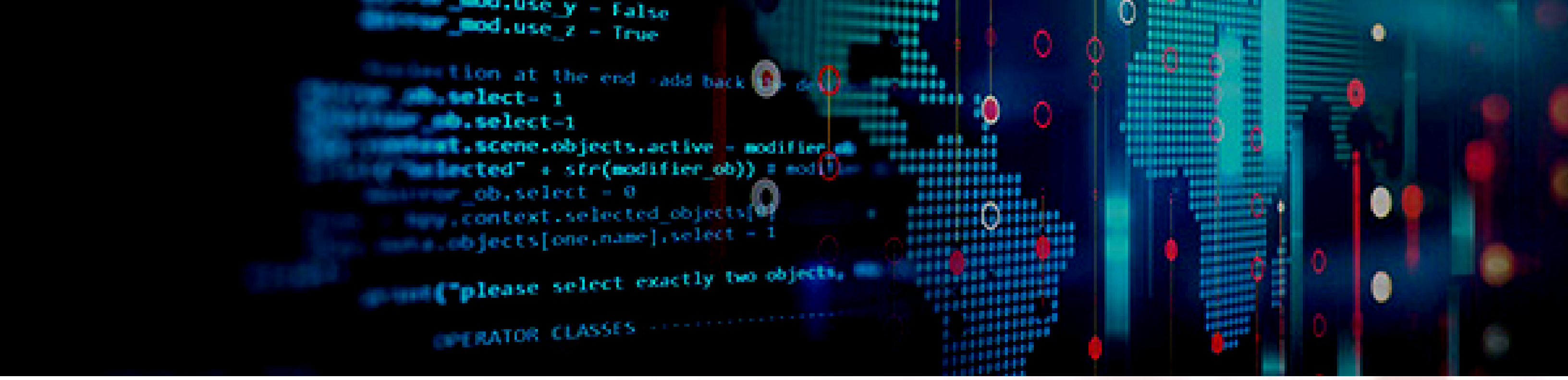
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_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
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Latest Hacked Websites

Published on Zone-h.org

http://esanpt1.go.th/daka.htm
http://esanpt1.go.th/daka.htm notified by telegram@saturaa
https://nptedu.go.th/readmee.htm
https://nptedu.go.th/readmee.htm notified by telegram@saturaa
http://www.nb1.go.th/daka.htm
http://www.nb1.go.th/daka.htm notified by telegram@saturaa
https://www.trang1.go.th/daka.htm
https://www.trang1.go.th/daka.htm notified by telegram@saturaa
https://yagliguresbirligi.gov.tr/mesh.htm
https://yagliguresbirligi.gov.tr/mesh.htm notified by MeshSec
http://pasamankab.go.id/read.html
http://pasamankab.go.id/read.html notified by AnonCoders
https://disporbudpar.baritokualakab.go.id/kz.html
https://disporbudpar.baritokualakab.go.id/kz.html notified by Mr.Kro0oz.305
https://bkpp.baritokualakab.go.id/kz.html
https://bkpp.baritokualakab.go.id/kz.html notified by Mr.Kro0oz.305
https://padangpariamankab.go.id
https://padangpariamankab.go.id notified by AnonSec Team
http://ret2.go.th/readme.htm
http://ret2.go.th/readme.htm notified by AnonCoders
http://camarariodopires.ba.gov.br/robots.txt
http://camarariodopires.ba.gov.br/robots.txt notified by Typical Idiot Security
http://camaramucuge.ba.gov.br/robots.txt
http://camaramucuge.ba.gov.br/robots.txt notified by Typical Idiot Security
http://camaraericocardoso.ba.gov.br/ghost.txt
http://camaraericocardoso.ba.gov.br/ghost.txt notified by Typical Idiot Security
http://camaraantoniocardoso.ba.gov.br/ghost.txt
http://camaraantoniocardoso.ba.gov.br/ghost.txt notified by Typical Idiot Security
http://transparencia.camarasaogoncalodoscampos.ba.gov.br/ghost.txt
http://transparencia.camarasaogoncalodoscampos.ba.gov.br/ghost.txt notified by Typical Idiot Security
https://www.cadreinfo.sg.gov.lk/readme.php
https://www.cadreinfo.sg.gov.lk/readme.php notified by S4NH4X0R
http://cmarea3.go.th/readmee.htm
http://cmarea3.go.th/readmee.htm notified by AnonCoders



Dark Web News

Darknet Live

US Court Orders ISPs to Block Three Pirating Sites

A U.S. court ordered every internet service provider in the United States to block access to three pirate streaming sites. In the Southern District of New York, a judge issued default judgments in three copyright cases against three pirate streaming services. The plaintiffs are three Jewish companies "related&rdquo; to Moshe Edery, the co-founder of Screen iL: United King Film Distribution, DBS Satellite Services, and Hot Communication. The defendants are the Jewish pirate streaming services Israel-tv.com, Israel.tv, and Sdarot.tv. _ Sdarot.tv is apparently a top streaming site in Israel. The lawsuits are typical copyright cases. In short, the operators of the streaming sites violated copyright laws by hosting the plaintiff's content. Plaintiffs transmit their programming in an encrypted form, either as cable television transmission or via satellite transmission, and Defendants' various services and hardware permit end-user consumers to bypass the Plaintiffs' encryption to view Plaintiffs' content. Defendants have gone to great lengths to conceal themselves and their ill-gotten proceeds from Plaintiffs' and this court's detection, including by using multiple false identities and addresses associated with their operations and purposely-deceptive contact information for the infringing Website However, the permanent injunctions in the judgments are the first of their kind in copyright cases. In 2011 and 2012, legislators fought over the Stop Online Piracy Act (SOPA), which included provisions for ordering ISPs to block pirate sites. Large organizations and companies, including Google and Wikipedia, protested SOPA. As a result, the House Judiciary Committee postponed the bill. As TorrentFreak pointed out, the judgment revealed that courts could already force ISPs to block access to pirating sites. Outside of the expansion of criminal law to include prison sentences for the streaming of pirated content, SOPA's significant elements meant very little. IT IS FURTHER ORDERED that all ISPs (including without limitation those set forth in Exhibit B hereto) and any other ISPs providing services in the United States shall block access to the Website at any domain address known today (including but not limited to those set forth in Exhibit A hereto) or to be used in the future by the Defendants ("Newly-Detected Websites&rdquo;) by any technological means available on the ISPs' systems. The domain addresses and any Newly Detected Websites shall be channeled in such a way that users will be unable to connect and/or use the Website, and will be diverted by the ISPs' DNS servers to a landing page operated and controlled by Plaintiffs (the "Landing Page&rdquo;) which can be reached as follows: _ The landing page already exists. IT IS FURTHER ORDERED, that third parties providing services used in connection with Defendants' operations - including, without limitation, ISPs, web hosting providers, CDN service providers, DNS service providers, VPN service providers, domain name purchasing service, domain names privacy service, back-end service providers, affiliate program providers, web designers, shippers, search-based online advertising services (such as through-paid inclusion, paid search results, sponsored search results, sponsored links, and Internet keyword advertising), any banks, savings and loan associations, merchant account providers, payment processors and providers, credit card associations, or other financial institutions, including without limitation, PayPal, and any other service provider which has provided services or in the future provides services to Defendants and/or the infringing Website (including without limitation those set forth in the list annexed and made Exhibit C annexed hereto) (each, a "Third Party Service Provider&rdquo;) - having knowledge of this Order by service, actual notice or otherwise be and are hereby permanently enjoined from providing services to the Website (through any of the domain names set forth in Exhibit A hereto or at any Newly-Detected Websites) or to any Defendant in conjunction with any of the acts set forth in subparagraphs (A)(1) to (A)(6) above;   That all domain names associated with the infringing Website, including without limitation those set forth in Exhibit A hereto, as well as any Newly-Detected Websites, be transferred to Plaintiffs' ownership and control; and   That in accordance with this court's inherent equitable powers and its power to coerce compliance with its lawful orders, and due to Defendants' on-going operation of their counterfeiting activities, in the event Plaintiffs identifies any Newly-Detected Website registered or operated by any Defendant and used in conjunction with the streaming any of Plaintiffs' Works, including such Websites utilizing domain names containing any of Plaintiffs' service mark or marks confusingly similar thereto, Plaintiffs shall have the ongoing authority to serve this Order on the domain name registries and/or the individual registrars holding and/or listing one or more of such the domain names associated with the Newly-Detected Websites; and   That the domain name registries and/or the individual registrars holding and/or listing one or more of the domain names associated with the Newly-Detected Websites, within seven (7) days of service of a copy of this Order, shall temporarily disable any domain names associated with the Newly-Detected Websites, make them inactive, and channel them in such a way that users will be unable to connect and/or use the Website, and will be diverted to the Landing Page; and   That after thirty (30) business days following the service of this Order, the registries and/or the individual registrars shall provide Plaintiffs with all contact information for the Newly-Detected Websites; shall transfer any domain names associated with the Newly-Detected Websites to the ownership and control of Plaintiffs, through the registrar of Plaintiffs' choosing, unless the Defendant has filed with the court and served upon Plaintiffs' counsel a request that such Newly-Detected Websites be exempted from this Order or unless Plaintiffs requests that such domain names associated with the NewlyDetected Websites be released rather than transferred; and   That any Defendant may upon two (2) business days' written notice to the Court and Plaintiffs' counsel, upon proper showing, appear and move for the dissolution or modification of the provisions of this Order concerning the restriction upon transfer of such domain names associated with the Newly-Detected Websites belonging to or controlled by any Defendant _ Shut it down! - the landing page for the pirate streaming sites   A Jew-vs-Jew copyright battle is undoubtedly the least of an average person's concerns. The ruling by the court, which is unprecedented, introduces a new form of control over internet infrastructure, including ISPs, by the U.S. government. TorrentFreak concluded: "Whether every (or any) ISP in the United States will contest the injunction is currently unknown, but we can be fairly confident that if they choose not to, these three site-blocking injunctions won't be the last in the United States.&rdquo;   I have included the judgement against Israel-TV. The other judgement are not materially different. DEFAULT JUDGMENT AND PERMANENT INJUNCTION ORDER pdf US Court Orders Every ISP in the United States to Block Illegal Streaming Sites archive.is archive.org torrentfreak.com

_ Somebody will claim that I am lionizing streaming sites or care about copyright laws. I do not care about either of those things.   (via darknetlive.com at https://darknetlive.com/post/shoah-v2-court-orders-isps-to-block-three-pirating-sites/)

"Guilty Plea Imminent" in "GoodDopeUSA" Case

A once-convicted darkweb vendor will soon be pleading guilty to selling methamphetamine through another darkweb vendor account, according to the defendant's attorney. Christopher Harris, also known as Christopher Harris-Edmundson, faces one count of narcotics conspiracy in the Southern District of New York. At a status conference held before United States District Court Judge Analisa Torres, Harris' attorney said that "the guilty plea is imminent.&rdquo; In August 2019, Harris was convicted in Virginia of selling Schedule I or II narcotics in connection with the operation of the darkweb vendor account "GoodDopeUSA.&rdquo; Through the account, Harris sold methamphetamine and heroin. A judge sentenced Harris to five years' probation.

_ The Recon Profile for GoodDopeUSA   According to a criminal complaint accusing Harris of narcotics conspiracy in the Southern District of New York, Harris has been selling methamphetamine on the darkweb from November 2020 through November 2021. This time, the complaint alleges, Harris created a vendor account with the username "KeepTheDopeAlive.&rdquo; An investigation into darkweb vendors led by Homeland Security Investigations resulted in the identification of Harris as the party responsible for the operation of the KeepTheDopeAlive account. _ The Recon Profile for KeepTheDopeAlive On August 12, 2021, an undercover law enforcement officer (LEO) placed an online order for 28 grams of methamphetamine from KeepTheDopeAlive on an undisclosed darkweb marketplace. The undercover LEO paid $462.50 and provided the vendor with an address in New York, New York. On August 20, law enforcement officers received and opened the package sent by KeepTheDopeAlive. They identified a bubble envelope, inside of which was a mylar bag. The mylar bag contained 32.7 grams of 98% pure methamphetamine. Law enforcement personnel at the Homeland Security Investigations Forensic Laboratory processed the received package for fingerprints. They recovered a fingerprint from the adhesive side of the tape on the box. The fingerprint matched the fingerprint on file for Harris in a law enforcement database of fingerprint records. In November 2021, an undercover LEO conducted a controlled delivery from KeepTheDopeAlive for two ounces of methamphetamine. When the package arrived at the LEO-controlled address in New York, investigators noted the sender of the package was listed as "Starboy Collectables&rdquo; in Commerce, California. The package contained 58 grams of methamphetamine. Later in November, law enforcement officers conducted physical surveillance of Harris at his apartment and business in Los Angeles, California. Harris lived in an apartment building above an undisclosed smoke shop where Harris worked. According to the California Secretary of State, the smoke shop's mailing address is Harris' apartment address. Investigators observed Harris leaving the smoke shop carrying a bag of USPS Flat Rate Priority boxes. Law enforcement officers followed Harris to a UPS store where they observed him "applying clear tape, with bare hands, to the seams of numerous small flat rate priority boxes.&rdquo; Harris then placed the packages on a cart designated for USPS mail drop-offs. _ tape-gate After Harris left the UPS store, law enforcement officers examined the packages Harris had left on the cart. The sender address listed on each of the sixteen packages was "Starboy Collectables&rdquo; at the same address in Commerce, California, as a package from one of the undercover purchases. Police arrested Harris in December 2021. An indictment accused Harris of narcotics conspiracy and possession of a weapon in furtherance of the narcotics conspiracy. complaint pdf indictment pdf (via darknetlive.com at https://darknetlive.com/post/guilty-plea-imminent-in-gooddopeusa-case/)

NYDFS Issues Blockchain Analytics Guidance for Companies

New guidance from the New York State Department of Financial Services mandates the use of blockchain analytics services for cryptocurrency businesses licensed in New York. The New York State Department of Financial Services (NYDFS), which is the government body responsible for regulating the banking and finance sector of entities subject to New York's laws, recently issued the "Guidance on Use of Blockchain Analytics ,&rdquo; clarifying some of the requirements for "all virtual currency business entities&rdquo; licensed under the state's "BitLicense&rdquo; or chartered under New York Banking Law. As the first guidance from a state regulatory body covering blockchain analytics, some legal commentators believe it will be the model for future regulations in different states. "Other regulators and law enforcement will likely start looking to this guidance to inform their own best practices for crypto monitoring going forward, and those in the industry would be well served by internalizing and implementing these guidelines, regardless of their jurisdiction,&rdquo; an author at the National Law Review wrote. The purpose of this guidance from the New York State Department of Financial Services ("Department&rdquo;) is to emphasize to all virtual currency business entities that are either licensed under 23 NYCRR Part 200 or chartered as a limited purpose trust company under the New York Banking Law (collectively, "VC Entities&rdquo;) the importance of blockchain analytics to effective policies, processes, and procedures, including, for example, those relating to customer due diligence, transaction monitoring, and sanctions screening. Compliance in a Virtual Currency Context _ Financial activity involving virtual currency can involve, among other things, different sources, destinations, and types of funds flows than are found in more traditional, fiat-currency contexts. For example, virtual currencies such as Bitcoin and Ether can be transferred peer-to-peer directly from one individual or entity to another pseudonymously, absent the use of a regulated third party (e.g., between non-custodial wallets, or self-hosted wallets that allow users to maintain control of their private keys). Thus, to effectively address compliance requirements under the New York Banking Law and the New York Financial Services Law, as well as federal Bank Secrecy Act/anti-money laundering ("BSA/AML&rdquo;) and Office of Foreign Assets Control ("OFAC&rdquo;) requirements, VC Entities must be sure that their compliance programs fully take into account the unique characteristics of virtual currencies.   While such characteristics present compliance challenges, they also present new possibilities for control measures that leverage these new technologies. For example, virtual currencies, by their nature, typically enable provenance tracing (i.e., review of previous transfers or "hops&rdquo; along the public blockchain ledger, or "on-chain&rdquo;). Put differently, the blockchain ledger's immutability typically allows a historical view of a virtual currency transmission between wallet addresses, providing the opportunity for greater visibility into transaction lineage than is typically found with traditional, fiat funds transfers.   A VC Entity's risk mitigation strategies must take account of the VC Entity's business profile to assess risk across types of virtual currencies and effectively address the specific characteristics of any particular virtual currency involved. For most virtual currencies, information stored on-chain includes certain identifying information, such as sending and receiving wallet addresses, time and date, and value of the transaction. However, as suggested above, these wallet addresses are typically pseudonymous, with nothing on the face of the transfer tying back to the originator, beneficiary, or underlying beneficial owners. In addition, the effectiveness of existing blockchain analytics tools can vary depending on the particular virtual currency in question. Control Measures that May Leverage Blockchain Analytics _ Given the above-noted characteristics of virtual currencies, the Department emphasizes the importance of blockchain analytics to VC Entities in addressing, for example, anti-money laundering requirements under 23 NYCRR &sect; 200.15, and across a range of BSA/AML and OFAC-related compliance controls,1 including but not limited to: Augmenting Know Your Customer (or "KYC&rdquo;)-related controls Conducting transaction monitoring of on-chain activity; and Conducting sanctions screening of on-chain activity.   VC Entities can use third-party service providers or internally developed blockchain analytics products and services for additional control measures, whether separately or in combination. To the degree that VC Entities outsource such control functions, the VC Entities must have clearly documented policies, processes, and procedures with regard to how the blockchain analytics activity integrates into the VC Entity's overall control framework consistent with the VC Entity's risk profile. Augmenting Know Your Customer-related controls _ As part of their KYC responsibilities, VC Entities must obtain and maintain information regarding, and understand and effectively address the risks presented by, their customers and potential customers.   Potentially useful in this regard are products and services that allow their users to obtain identifying information (e.g., location of a wallet address on a specific exchange for custodial transactions) that ties directly to the pseudonymous on-chain data, particularly in combination with customer-provided information. These products and services typically can identify wallet addresses associated with an institution (e.g., a VC Entity) as well as known high-risk wallet addresses such as darknet marketplaces, but such tools may not be able to identify underlying owners, including ultimate beneficial owners, and may have limited attribution capability, absent further "off-chain&rdquo; verification methods integrating customer-provided data. For example, VC Entities must have policies, processes, and procedures to assess counterparty exposure for virtual currency funds transfers (e.g., beneficiary institutions for outbound transfers). For example, certain vendor products or internally developed tools provide numerical scores or tiered rankings to represent the risk of the counterparty institution, typically based on on-chain transaction data supplemented with other factors such as strength of the institution's BSA/AML Program. Conducting transaction monitoring of on-chain activity _ VC Entities must also have in place appropriate control measures to monitor and identify unusual activity tailored to the VC Entity's risk profile. Accordingly, it is important for VC Entities to have policies, processes, and procedures for the tracing of transaction activity for each type of virtual currency the entity supports and the flow of funds through the blockchain for any inbound or outgoing activity (often described as "provenance tracing&rdquo; or "transaction tracing&rdquo;). For example, FinCEN recently noted: "It is critical that all financial institutions, including those with visibility into CVC [convertible virtual currency] flows, &hellip; identify and quickly report suspicious activity associated with potential sanctions evasion, and conduct appropriate risk-based customer due diligence or, where required, enhanced due diligence.&rdquo; For instance, it is important that VC Entities evidence appropriately tailored transaction monitoring coverage against applicable typologies and red flags, identify deviations from the profile of a customer's intended purposes, and address other risk considerations as applicable. Relevant typologies related to virtual currency business activity include but are not limited to: assessing whether a virtual currency (1) has substantial exposure to a high-risk or sanctioned jurisdiction; (2) is processed through a mixer or tumbler; (3) is sent to or from darknet markets; (4) is associated with scams/ransomware; and (5) is associated with other illicit activity relevant to the VC Entity's business model. Documentation must describe case management and escalation processes, with clearly delineated roles and responsibilities across the business and compliance functions, including the VC entity's approach where there are any doubts (e.g., related to source of funds). Conducting sanctions screening of on-chain activity _ The Department also emphasizes the importance of risk-based policies, processes, and procedures to identify transaction activity involving virtual currency addresses or other identifying information associated with sanctioned individuals and entities listed on the SDN List, or located in sanctioned jurisdictions; and, OFAC notes: "Transaction monitoring and investigation software can be used to identify transactions involving virtual currency addresses or other identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities listed on the SDN List or other sanctions lists, or located in sanctioned jurisdictions.&rdquo; CipherTrace and Chainalysis must be making a killing. The New York State Department of Financial Services alleges that the state's regulations for cryptocurrency businesses "ensure that New Yorkers have a well-regulated way to access the virtual currency marketplace and that New York remains at the center of technological innovation and forward-looking regulation.&rdquo; Of course, after the introduction of New York's "BitLicense&rdquo; in 2015, Kraken, BitFinex, ShapeShift, Paxful, and many others left the state. __ Very well regulated The New York State Assembly just passed bill that places a two-year ban on PoW mining operations that rely on "a carbon-based fuel&rdquo; (Assembly Bill A7389C) as part of an "Earth Day&rdquo; package (supporters allege that people are getting too sweaty in New York). The State Senate has not yet voted on the bill, though. __ Assemblywoman Anna Kelles sponsored the bill banning PoW mining operations | @annakelles In March, the European Parliament - Committee on Economic and Monetary Affairs voted against a draft of the Markets in Crypto Assets regulatory framework that would have banned PoW mining. Guidance on Use of Blockchain Analytics - archive.is, archive.org, dfs.ny.gov FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts pdf Advisory on Illicit Activity Involving Convertible Virtual Currency pdf (via darknetlive.com at https://darknetlive.com/post/nydfs-published-blockchain-analytics-guidance-for-crypto-companies/)

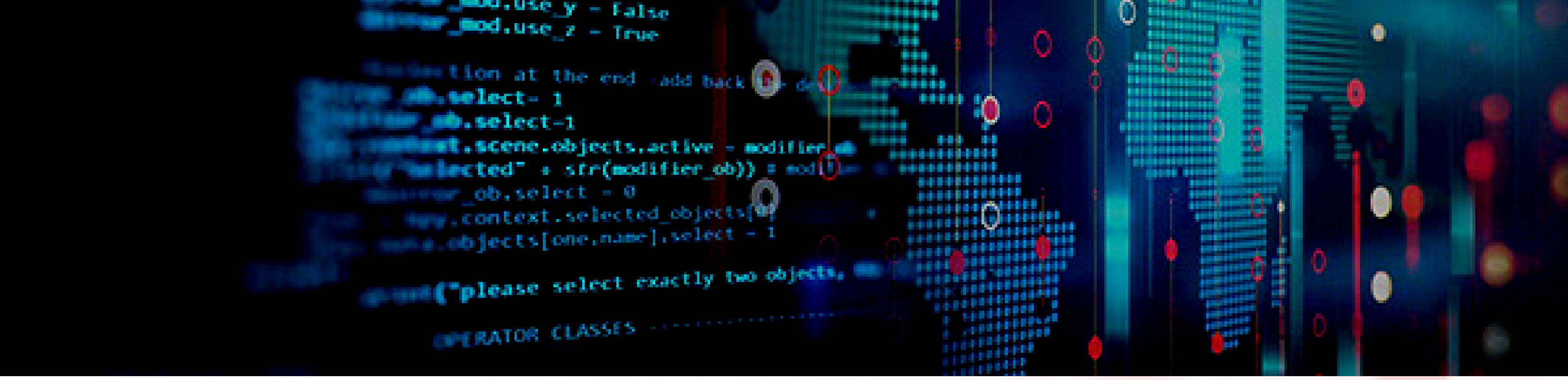
"Adderall123" Bust: iCloud Records, USPS Profiling, Surveillance

Under the username "Adderall123&rdquo; on darkweb markets, two Bay Area men allegedly shipped counterfeit Adderall pills to customers throughout the United States. An investigation led by the Drug Enforcement Administration (DEA) and the United States Postal Inspection Service (USPIS) resulted in the arrest of Andrew and Tony Tan for allegedly selling methamphetamine on darkweb markets. According to DEA Special Agent Colin Hart, Andrew, Tony, and one other co-conspirator operated the vendor account "Adderall123&rdquo; on several darkweb marketplaces, including White House Market (WHM), Torrez Market, ASAP Market, and Empire Market. __ Adderall123 sold counterfeit Adderall pills on several marketplaces. The investigation into Adderall123 began in April 2021. Investigators examined the vendor's profile on White House Market, where Adderall123 had been selling 30 milligram Adderall pills for sale in quantities of 30, 50, and 100 pills. White House Market, which shut down in October 2021, allowed vendors to import feedback from vendor profiles on different marketplaces. Adderall123 had imported feedback from Empire Market, indicating that the vendor had a presence on the darkweb as early as August 2020. In September 2021, Special Agent Hart conducted an undercover purchase ("UC Purchase #4&rdquo;) of 200 30mg Adderall pills from Adderall123 on White House Market. Agents had the package shipped to an "Arlo Krauser&rdquo; at an address in Elverta, California, controlled by law enforcement. Before UC Purchase #4 had occurred, a USPIS General Analyst had identified the Westlake Post Office in Daly City, California, as a post office used by Adderall123. A mailing at the Westlake Post Office on September 17, 2021, had been flagged as a package shipped by Adderall123. "[The] mailing had been identified as part of a set of mailings flagged by a USPIS General Analyst (GA) as suspected ADDERALL123 mailings. The packages in these mailings were identified based on similarities they shared with previous suspected ADDERALL123 mailings and prior undercover purchases from ADDERALL123. These similarities included over-the-counter mailing transactions of large volumes of Priority Mail Flat Rate envelopes, mailed out of 940 and 941 zip codes, mailed to addresses all over the U.S., with handwritten labels (often with fake names or fake return addresses), and postage-paid for in cash.&rdquo;   __   Purported users had conflicting conclusions about the active ingredient of Adderall123's products.   Agents reviewed the post office surveillance footage from September 17, 2021. They observed an Asian male with glasses, a black face mask, and a grey hoodie mailing a stack of Priority Mail Flat Rate Envelopes. The suspect, later identified as Andrew Tan, left the post office and entered a white Subaru SUV with honeycomb-shaped rims. On September 30, 2021, agents set up surveillance at multiple post offices in South San Francisco, Daly City, San Bruno, and San Francisco. A Postal Inspector at the Daly City Main Post Office observed Andrew Tan conducting an over-the-counter transaction. The Postal Inspector walked to the parking lot and recorded the license plate during the transaction. After the suspect had left, the Postal Inspector returned to the post office and recovered nine Priority Mail Flat Rate Envelopes. The suspect had paid for them with cash, and all of the packages had a handwritten return address ("Jimmy Leung, 191 Whittier St, Daly City, CA 94014&rdquo;). One of the packages was addressed to the name and address provided during UC Purchase #4.   __   ASAP is the only remaining market where Adderall123 had an account.   The package contained 207 orange, circular pills pressed with "dp&rdquo; and "30.&rdquo; The pills tested positive for methamphetamine. Three controlled purchases are described in the criminal complaint. After receiving similar counterfeit Adderall pills from a different order, agents sent the pills to a lab to have them tested for fingerprints. One of the pills tested positive for a fingerprint that matched a fingerprint card for Andrew Tan. According to the California DMV, the license plate was registered to Andrew Tan or one of his relatives at an address investigators believe belongs to his parents. Apple gave agents access to the data stored in Tan's iCloud account. "Agents observed a video, dated June 16, 2020, which shows Tony TAN sitting in an indoor location, taking orange circular pills from a large clear zip-lock bag and sliding the pills onto a white piece of paper. The pills in the video match the appearance of the counterfeit Adderall pills pressed with methamphetamine that agents have purchased and seized throughout this investigation, including those contained within UC Purchase #4 and Parcel Intercept #2. GPS location data for this video is [Lat], [Long], which shows to be on the street outside of [Address], the suspected residence of Andrew TAN and Tony TAN's parents. I know the individual handling the pills in the video to be Tony TAN because his appearance matches that of Tony TAN in his DMV photo, a family photo of Tony TAN found on Andrew TAN's iCloud account, bank photos and video of Tony TAN making cash deposits into his bank account, and Tony TAN as observed on surveillance and pole camera footage during this investigation.&rdquo; Agents also obtained a copy of Tan's iMessages. The records contained incriminating messages sent to and from Tan's girlfriend. A message sent to Tan from his girlfriend: "I am trying to be open-minded at least about weed. You smoking with my brother multiple times. That time where you were so high you couldn't drive after you smoked with Matt. You smoking with Nathan. I even smoked with you. Eating them with you. But at least you were upfront with me. You said it would only be with me, but you don't follow through with anything that you say. I didn't like it but I tolerated you having this job. We are waiting for you to pick up your career and you claim it got fcked bc of this job. Now you're moving onto pills. the first time you told me about the pills I said to get rid of them. You didn't and I let it go. You offered them to me and at one point I even considered it despite my values bc I should be more open minded and at least give it a try. But that's against what I believe in and yet you still suggest them to me every now and then. You're offering them to my brother and now you want to sell this shit?! That's too much for me to try to understand.&rdquo; In another message, Tan sent a message to his girlfriend: "I don't supply. It's like Matt supplies me. Its like Natalie buys them. And shares with your brother. She's not supplying. It's called sharing what we hav.&rdquo;   __   Tan's girlfriend thought he sold actual Adderall aparently.   Police arrested Andrew and Tony Tan in April 2022. Both men face one count of possession with intent to distribute 5 grams or more of

methamphetamine and 50 grams or more of a mixture or substance containing detectable amounts of methamphetamine. Tony Tan's court documents are sealed, and the third co-conspirator's court documents are unavailable. If convicted, Andrew and Tony face a minimum of five years imprisonment. Complaint pdf
Vendors with "adderall&rdquo; in their username have a thing about selling methamphetamine apparently. (via darknetlive.com at https://darknetlive.com/post/adderall123-bust-imessage-records-usps-profiling-surveillance/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, in this article [...] The post Top Darknet Markets 2022: The Outstanding Performances To Consider Now appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Breaking Bad Forum On The Darknet Is Revolutionary
The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

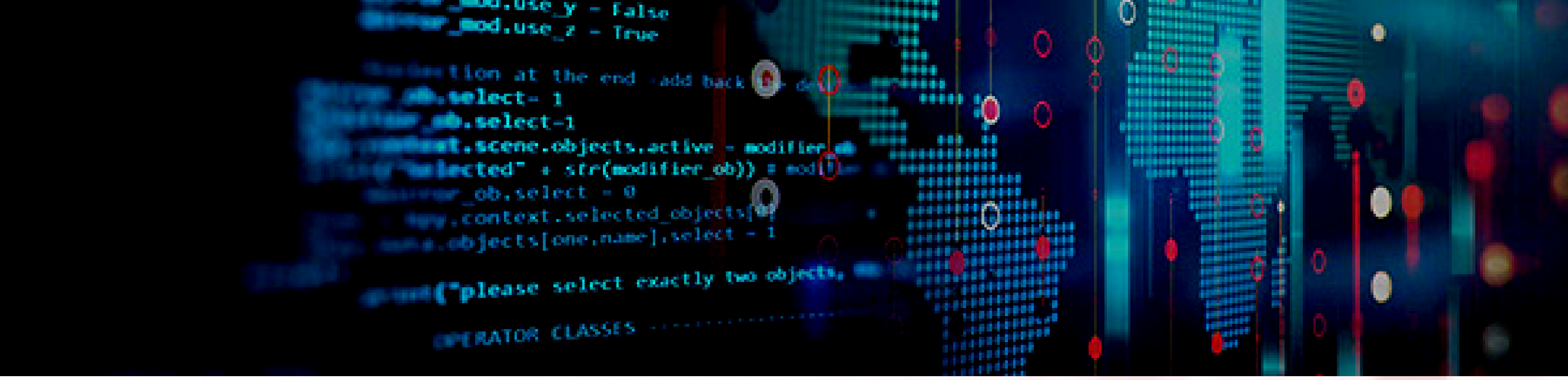
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: 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
* Retailers Using WooCommerce are at Risk of Magecart Attacks

FireEye

* Metasploit Wrap-Up
* Unsung Security Superheroes: You're Now Sung
* XSS in JSON: Old-School Attacks for Modern Applications
* Is Your Kubernetes Cluster Ready for Version 1.24?
* MDR, MEDR, SOCaaS: Which Is Right for You?
* Cloud-Native Application Protection (CNAPP): What's Behind the Hype?
* Metasploit Wrap-Up
* Widespread Exploitation of VMware Workspace ONE Access CVE-2022-22954
* [Security Nation] Whitney Merrill on the Crypto & Privacy Village (and the Latest in Data Privacy)
* How to Strategically Scale Vendor Management and Supply Chain Security



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for Enterprise NFV Infrastructure Software
* F5 Releases Security Advisories Addressing Multiple Vulnerabilities
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* CISA Adds Five Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Updates for Multiple Products
* Google Releases Security Updates for Chrome
* CISA and FBI Update Advisory on Destructive Malware Targeting Organizations in Ukraine
* 2021 Top Routinely Exploited Vulnerabilities
* AA22-117A: 2021 Top Routinely Exploited Vulnerabilities
* AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
* Vulnerability Summary for the Week of April 25, 2022
* Vulnerability Summary for the Week of April 18, 2022

Zero Day Initiative Advisories

Ubuntu Security Notice USN-5405-1
Ubuntu Security Notice 5405-1 - It was discovered that jbig2dec incorrectly handled memory when parsing invalid files. An attacker could use this issue to cause jbig2dec to crash, leading to a denial of service. It was discovered that jbig2dec incorrectly handled memory when processing untrusted input. An attacker could use this issue to cause a denial of service, or possibly execute arbitrary code.
Ubuntu Security Notice USN-5259-2
Ubuntu Security Notice 5259-2 - USN-5259-1 fixed several vulnerabilities in Cron. This update provides the corresponding update for Ubuntu 18.04 LTS. It was discovered that the postinst maintainer script in Cron unsafely handled file permissions during package install or update operations. An attacker could possibly use this issue to perform a privilege escalation attack.
Red Hat Security Advisory 2022-1739-01
Red Hat Security Advisory 2022-1739-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. This advisory covers the containers for the release.
Red Hat Security Advisory 2022-1730-01
Red Hat Security Advisory 2022-1730-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-1726-01
Red Hat Security Advisory 2022-1726-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-1734-01
Red Hat Security Advisory 2022-1734-01 - The Migration Toolkit for Containers enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API.
Red Hat Security Advisory 2022-1727-01
Red Hat Security Advisory 2022-1727-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-1724-01
Red Hat Security Advisory 2022-1724-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-1725-01
Red Hat Security Advisory 2022-1725-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.
Ubuntu Security Notice USN-5403-1
Ubuntu Security Notice 5403-1 - It was discovered that SQLite command-line component incorrectly handled certain queries. An attacker could possibly use this issue to cause a crash or possibly execute arbitrary code.
Red Hat Security Advisory 2022-1716-01
Red Hat Security Advisory 2022-1716-01 - Red Hat Ceph Storage is a scalable, open, software-defined storage platform that combines the most stable version of the Ceph storage system with a Ceph management platform, deployment utilities, and support services. Issues addressed include bypass, crlf injection, and memory leak vulnerabilities.
Red Hat Security Advisory 2022-1715-01
Red Hat Security Advisory 2022-1715-01 - Red Hat Advanced Cluster Management for Kubernetes 2.3.10 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console&mdash;with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs. Issues addressed include bypass and traversal

vulnerabilities.

Ubuntu Security Notice USN-5354-2

Ubuntu Security Notice 5354-2 - USN-5354-1 fixed vulnerabilities in Twisted. This update provides the corresponding updates for Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 22.04 LTS. It was discovered that Twisted incorrectly processed SSH handshake data on connection establishments. A remote attacker could use this issue to cause Twisted to crash, resulting in a denial of service.

Red Hat Security Advisory 2022-1620-01

Red Hat Security Advisory 2022-1620-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.6.57. Issues addressed include bypass and denial of service vulnerabilities.

Red Hat Security Advisory 2022-1713-01

Red Hat Security Advisory 2022-1713-01 - The rh-sso-7/sso75-openshift-rhel8 container image has been updated for RHEL-8 based Middleware Containers. Issues addressed include a privilege escalation vulnerability.

SAP NetWeaver Java Denial Of Service

SAP NetWeaver JAVA suffers from a denial of service vulnerability.

Ubuntu Security Notice USN-5395-2

Ubuntu Security Notice 5395-2 - USN-5395-1 fixed vulnerabilities in networkd-dispatcher. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem. It was discovered that networkd-dispatcher incorrectly handled internal scripts. A local attacker could possibly use this issue to cause a race condition, escalate privileges and execute arbitrary code.

Red Hat Security Advisory 2022-1703-01

Red Hat Security Advisory 2022-1703-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.9.0 ESR. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-5401-1

Ubuntu Security Notice 5401-1 - Wenxiang Qian discovered that DPDK incorrectly checked certain payloads. An attacker could use this issue to cause DPDK to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that DPDK incorrectly handled inflight type messages. An attacker could possibly use this issue to cause DPDK to consume resources, leading to a denial of service.

Ubuntu Security Notice USN-5402-1

Ubuntu Security Notice 5402-1 - Elison Niven discovered that OpenSSL incorrectly handled the c_rehash script. A local attacker could possibly use this issue to execute arbitrary commands when c_rehash is run. Raul Metsma discovered that OpenSSL incorrectly verified certain response signing certificates. A remote attacker could possibly use this issue to spoof certain response signing certificates. This issue only affected Ubuntu 22.04 LTS.

Red Hat Security Advisory 2022-1701-01

Red Hat Security Advisory 2022-1701-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.9.0 ESR. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-1708-01

Red Hat Security Advisory 2022-1708-01 - Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments.

Red Hat Security Advisory 2022-1705-01

Red Hat Security Advisory 2022-1705-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.9.0 ESR.

Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-1709-01

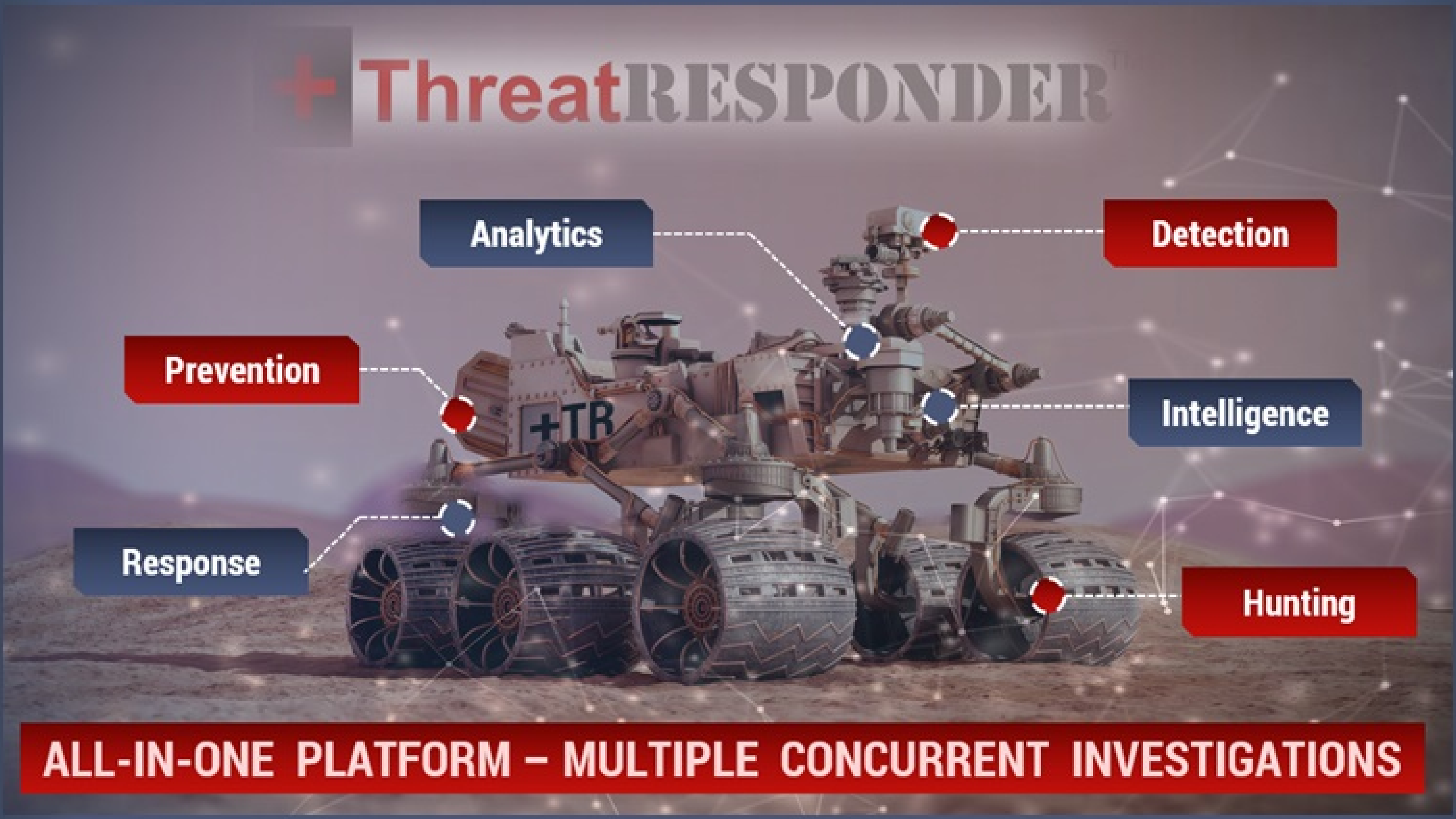
Red Hat Security Advisory 2022-1709-01 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.5.2 serves as a replacement for Red Hat Single Sign-On 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. 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



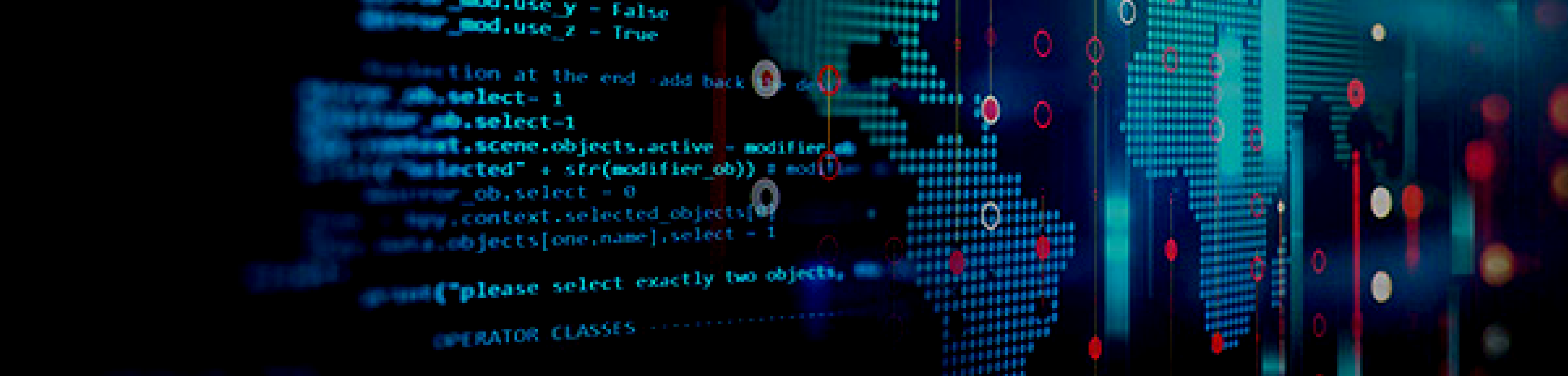
The Solution – ThreatResponder® Platform

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



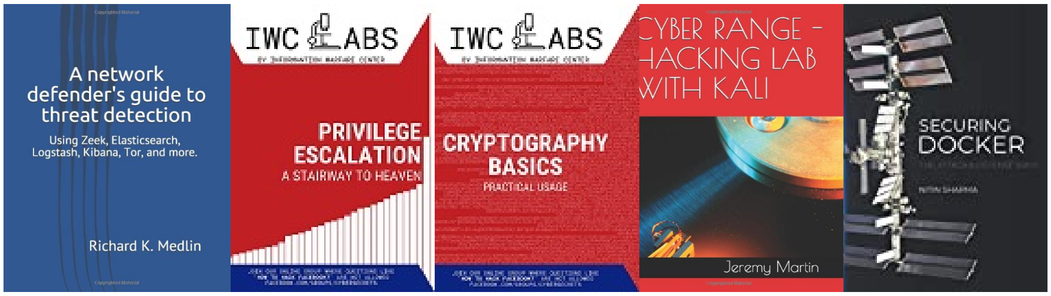
The Cyber Secrets publications on Amazon

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?
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
THE 8 LAYERS OF THE OSI CAKE
LAUNCHING EXPLOITS
INCIDENT RESPONSE

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