Jul-11-22

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 11, 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

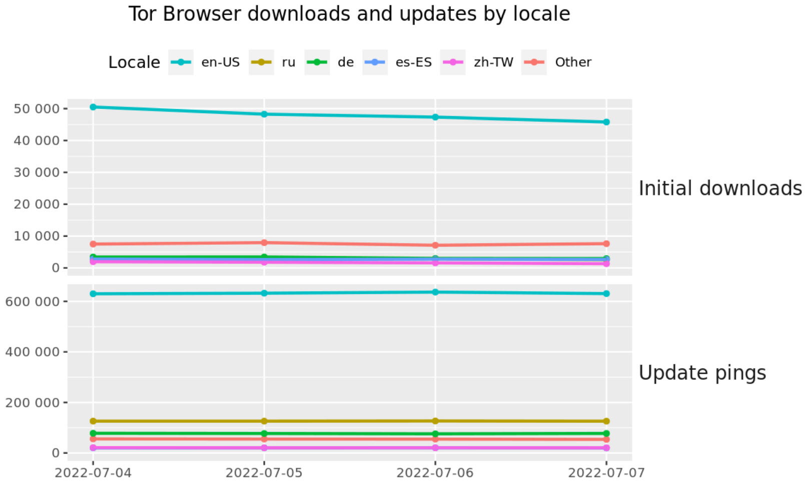
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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

* End-To-End Encryption's Central Role In Modern Self Defense
* Hack Allows Drone Takeover Via ExpressLRS Protocol
* Apple Launches Lockdown To Block Spyware
* FBI And MI5 Leaders Give Unprecedented Joint Warning On Chinese Spying
* NIST Rolls Out New Encryption Standards To Prepare For Quantum Computing
* Marriott Hotels Suffers Third Data Breach In Four Years
* Cryptocurrency Broker Voyager Digital Files For Bankruptcy Protection
* Bug Bounty Platform's Employee Abused Internal Access To Steal Bounties
* China Tries To Censor What Could Be Biggest Data Hack In History
* Germany Unveils Plan To Tackle Cyberattacks On Satellites
* Google Patches Actively Exploited Chrome Bug
* Google: Half Of Zero-Day Exploits Linked To Poor Software Fixes
* MPs Call For UK Ban On Two Chinese CCTV Firms
* Hacker Claims To Have Stolen 1 Billion Records Of Chinese Citizens From Police
* British Army's YouTube And Twitter Accounts Hacked
* Google Location Tracking To Forget You Were Ever At That Medical Clinic
* What To Do About Inherent Security Flaws In Critical Infrastructure?
* ZuoRAT Can Take Over Widely Used SOHO Routers
* Flagstar Bank Breach Another Example Of Hacker Threat To Financial Sector
* FBI Adds Missing Cryptoqueen To Top Ten Most Wanted List
* Microsoft Exchange Servers Worldwide Hit By Stealthy New Backdoor
* Jenkins Warns Of Security Holes In These 25 Plugins
* China Lured Graduate Jobseekers Into Digital Espionage
* Leaky Access Tokens Exposed Amazon Photos Of Users
* The Supreme Court Just Fucked The Planet

Krebs on Security

* 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
* "Downthem" DDoS-for-Hire Boss Gets 2 Years in Prison
* Adconion Execs Plead Guilty in Federal Anti-Spam Case
* KrebsOnSecurity in New Netflix Series on Cybercrime
* What Counts as "Good Faith Security Research?"

LATEST NEWS

Dark Reading

* Microsoft Reverses Course on Blocking Office Macros by Default
* DoJ Charges CEO for Dealing $1B in Fake Cisco Gear
* SOAR Market Worth $2.3 Billion by 2027, According to Exclusive Report by MarketsandMarkets
* Welcome-Back-to-the-Future Shock
* Swimlane Secures $70M Growth Round to Fuel Global Expansion of Next Generation Low-Code Security Auto
* Worldwide Enterprise Endpoint Security Industry to 2027: Focus on Antivirus, Firewall, Endpoint Devic
* Coalition Closes $250 Million in Series F Funding, Valuing the Cyber Insurance Provider at $5 Billion
* Zero Trust Bolsters Our National Defense Against Rising Cyber Threats
* In Switch, Trickbot Group Now Attacking Ukrainian Targets
* What Do All of Those Cloud Cybersecurity Acronyms Mean?
* ICYMI: Critical Cisco RCE Bug, Microsoft Breaks Down Hive, SHI Cyberattack
* Cyber Skills Center Launches in Tulsa to Develop Diverse, Local Tech Talent Pipeline
* Stealthy Cyber-Campaign Ditches Cobalt Strike for Rival 'Brute Ratel' Pen Test Tool
* Fortress Information Security Sponsors Open Web Application Security Project To Work on Industry-Wide
* China's Tonto Team APT Ramps Up Spy Operations Against Russia
* Buggy 'Log in With Google' API Implementation Opens Crypto Wallets to Account Takeover
* Empower Your Security Operations Team to Combat Emerging Threats
* Cybersecurity Has a Talent Shortage & Non-Technical People Offer a Way Out
* Inside NIST's 4 Crypto Algorithms for a Post-Quantum World
* Prevention Takes Priority Over Response

The Hacker News

* Hackers Used Fake Job Offer to Hack and Steal $540 Million from Axie Infinity
* PyPI Repository Makes 2FA Security Mandatory for Critical Python Projects
* Hackers Exploiting Follina Bug to Deploy Rozena Backdoor
* Researchers Warn of Raspberry Robin's Worm Targeting Windows Users
* Researchers Detail Techniques LockBit Ransomware Using to Infect its Targets
* Microsoft Temporarily Rolls Back Plan to Block Office VBA Macros by Default
* Why Developers Hate Changing Language Versions
* Experts Uncover 350 Browser Extension Variants Used in ABCsoup Adware Campaign
* TrickBot Gang Shifted its Focus on "Systematically" Targeting Ukraine
* North Korean Maui Ransomware Actively Targeting U.S. Healthcare Organizations
* Over 1,200 NPM Packages Found Involved in "CuteBoi" Cryptomining Campaign
* Apple's New "Lockdown Mode" Protects iPhone, iPad, and Mac Against Spyware
* The Age of Collaborative Security: What Tens of Thousands of Machines Witness
* Researchers Warn of New OrBit Linux Malware That Hijacks Execution Flow
* Cisco and Fortinet Release Security Patches for Multiple Products

LATEST NEWS

Security Week

* Musk Ditches Twitter Deal, Triggering Defiant Response
* Cisco Patches Critical Vulnerability in Enterprise Communication Solutions
* New 'HavanaCrypt' Ransomware Distributed as Fake Google Software Update
* Fortinet Patches High-Severity Vulnerabilities in Several Products
* Election Officials Face Security Challenges Before Midterms
* 10 Vulnerabilities Found in Widely Used Robustel Industrial Routers
* IT Services Giant SHI International Hit by Cyberattack
* Cyber Insurance Firm Coalition Raises $250 Million at $5 Billion Valuation
* Acting as Own Lawyer, Accused CIA Coder Argues for Acquittal
* Twitter Says it Removes 1 Million Spam Accounts a Day
* OpenSSL Patches Remote Code Execution Vulnerability
* Cybersecurity M&A Roundup: 45 Deals Announced in June 2022
* US: North Korean Hackers Targeting Healthcare Sector With Maui Ransomware
* As Cybercriminals Recycle Ransomware, They're Getting Faster
* Marriott Confirms Small-Scale Data Breach
* Hackers Using 'Brute Ratel C4' Red-Teaming Tool to Evade Detection
* US, UK Leaders Raise Fresh Alarms About Chinese Espionage
* Apple Adds 'Lockdown Mode' to Thwart .Gov Mercenary Spyware
* Researchers Flag 'Significant Escalation' in Software Supply Chain Attacks
* Is an Infrastructure War on the Horizon?
* DoD Launches 'Hack US' Bounties for Major Flaws in Publicly Exposed Assets
* Security Automation Firm Swimlane Closes $70 Million Funding Round
* Evasive Rust-Coded Hive Ransomware Variant Emerges
* NIST Announces Post Quantum Encryption Competition Winners
* Bias in Artificial Intelligence: Can AI be Trusted?
* Alleged Chinese Police Database Hack Leaks Data of 1 Billion

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* [Scam of the Week] Amazon Prime Day or Amazon Crime Day? Don't Fall Victim to Phishing
* [Eye Opener] Lessons Learned from a Big Hotel's Recent Data Breach Caused By Social Engineering
* One Employee's Desire for a New Job Cost His Employer $540 million
* Your KnowBe4 Fresh Content Updates from June 2022
* Breaches & Cyberwar Driving Security Culture
* FBI Issues Warning on China for Attempting to 'Ransack' Western Companies
* Phishing Campaign Impersonates the UAE
* Expect More Travel-Themed Phishing Scams as 80% of Americans Plan to Travel
* New WhatsApp Scam Uses Call Forwarding Social Engineering to Hijack Accounts
* New Phishing Campaign is Targeting TrustWallet With Impersonation Emails

ISC2.org Blog

* Hiring Managers Lead on Entry-Level Cybersecurity Job Descriptions
* #ISC2Congress: Politics, Cybersecurity & Global Issues - Ian Bremmer to Speak as (ISC)&sup2; Keynote
* How can you find and retain new cybersecurity talent?
* Four Steps to Using Metrics to Defend Your Security Budget
* How to Create Successful CISSP and CCSP Study Groups

HackRead

* How Technology Can Help Your Business Succeed
* Hackers Used Fake LinkedIn Job Offer to Hack Off $625M from Axie Infinity
* A Quick Guide to GDPR (General Data Protection Requirements)
* Apple Debuts Lockdown Mode to Prevent State-Sponsored Spying
* What Makes External Attack Surface Management Essential?
* What Are the Security Benefits of Using a Digital Signature?
* Russia Hackers Abusing BRc4 Red Team Penetration Tool in Recent Attacks

Koddos

* How Technology Can Help Your Business Succeed
* Hackers Used Fake LinkedIn Job Offer to Hack Off $625M from Axie Infinity
* A Quick Guide to GDPR (General Data Protection Requirements)
* Apple Debuts Lockdown Mode to Prevent State-Sponsored Spying
* What Makes External Attack Surface Management Essential?
* What Are the Security Benefits of Using a Digital Signature?
* Russia Hackers Abusing BRc4 Red Team Penetration Tool in Recent Attacks

LATEST NEWS

Naked Security

* Apache "Commons Configuration" patches Log4Shell-style bug - what you need to know
* S3 Ep90: Chrome 0-day again, True Cybercrime, and a 2FA bypass [Podcast + Transcript]
* OpenSSL fixes two "one-liner" crypto bugs - what you need to know
* Google patches "in-the-wild" Chrome zero-day - update now!
* Canadian cybercriminal pleads guilty to "NetWalker" attacks in US
* Facebook 2FA phish arrives just 28 minutes after scam domain created
* "Missing Cryptoqueen" hits the FBI's Ten Most Wanted list
* S3 Ep89: Sextortion, blockchain blunder, and an OpenSSL bugfix [Podcast + Transcript]
* Firefox 102 fixes address bar spoofing security hole (and helps with Follina!)
* Harmony blockchain loses nearly $100M due to hacked private keys

Threat Post

* Sneaky Orbit Malware Backdoors Linux Devices
* U.S. Healthcare Orgs Targeted with Maui Ransomware
* Hack Allows Drone Takeover Via 'ExpressLRS' Protocol
* Human Error Blamed for Leak of 1 Billion Records of Chinese Citizens
* Latest Cyberattack Against Iran Part of Ongoing Campaign
* Google Patches Actively Exploited Chrome Bug
* ZuoRAT Can Take Over Widely Used SOHO Routers
* A Guide to Surviving a Ransomware Attack
* Leaky Access Tokens Exposed Amazon Photos of Users
* Patchable and Preventable Security Issues Lead Causes of Q1 Attacks

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.

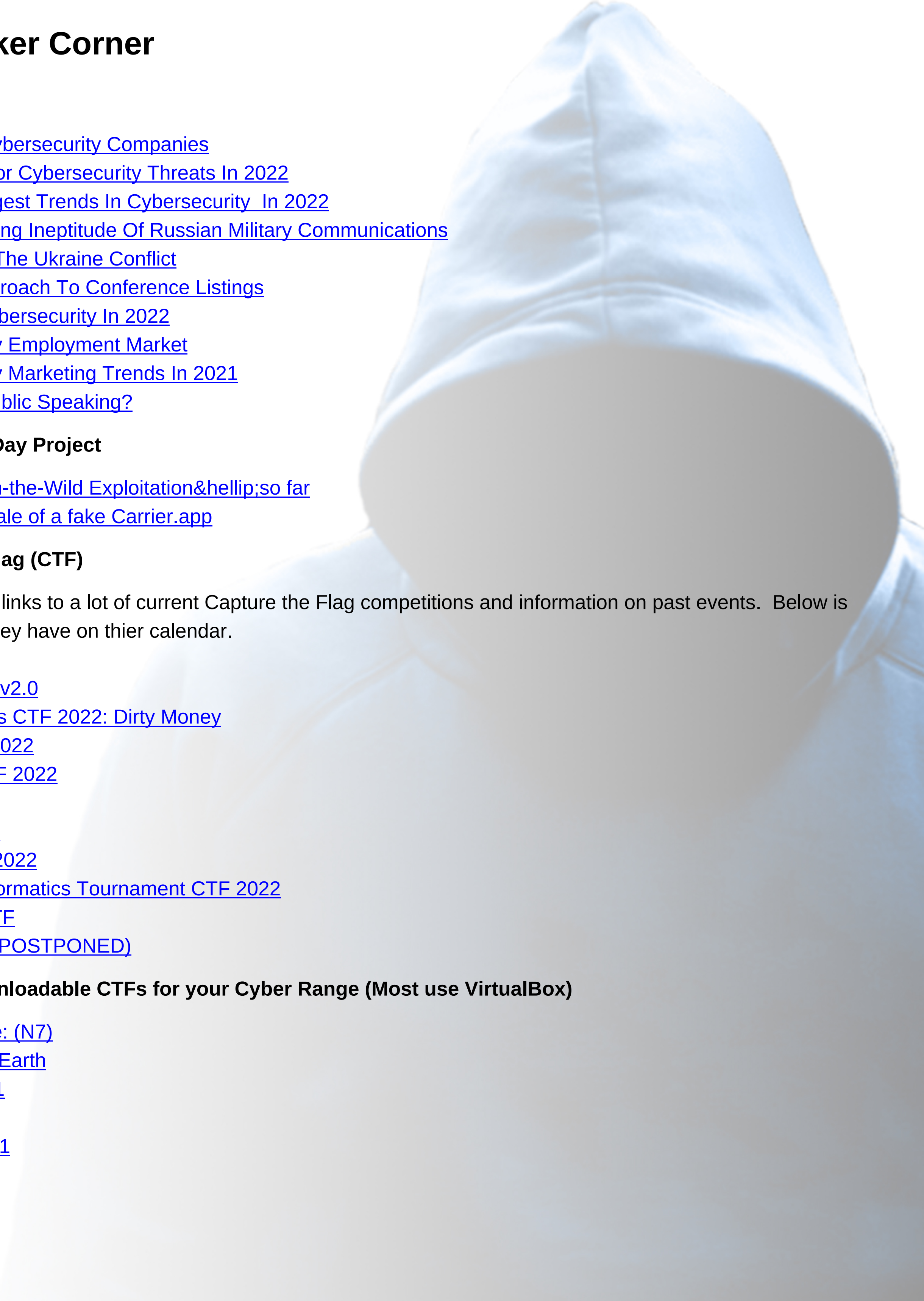
InfoWorld

* Why you should modernize search technologies
* Open source job security through recessions
* 12 examples of old tech that never dies
* What happens when cloud spend surpasses traditional systems
* What is Visual Studio Code? Microsoft's extensible code editor
* How Walmart abstracts its hybrid cloud for developers
* 8 new JavaScript features to start using today
* How to migrate ASP.NET Core 5 code to ASP.NET Core 6
* IBM acquires data observability firm Databand.ai
* Working with Microsoft's .NET Rules Engine

C4ISRNET - Media for the Intelligence Age Military

* Teledyne wins Pentagon order for hundreds of bomb disposal robots
* US Space Force wants new commercial imagery tool to boost resiliency
* Ukraine war tactics reaffirm US Army's modernization thrust, service chief says
* US Space Force rapid capabilities office to deliver first project this year
* Stryker power problem uncovered in test of US Army network gear
* Spaceflight experiment Recurve launches in support of warfighter comms
* Air Force Research Lab begins integration, testing for experimental navigation satellite
* Cyber Yankee exercise hones New England Guard skills to fight digital threats
* AT&T, 26 other companies join Air Force's $950 million JADC2 effort
* US must invest in emerging tech to keep pace with China, Govini report says

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.

* wtfCTF 2022 v2.0
* HTB Business CTF 2022: Dirty Money
* Crypto CTF 2022
* ImaginaryCTF 2022
* UACTF 2022
* ENOWARS 6
* BDSec CTF 2022
* Lexington Informatics Tournament CTF 2022
* MCH2022 CTF
* 3kCTF-2022(POSTPONED)

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

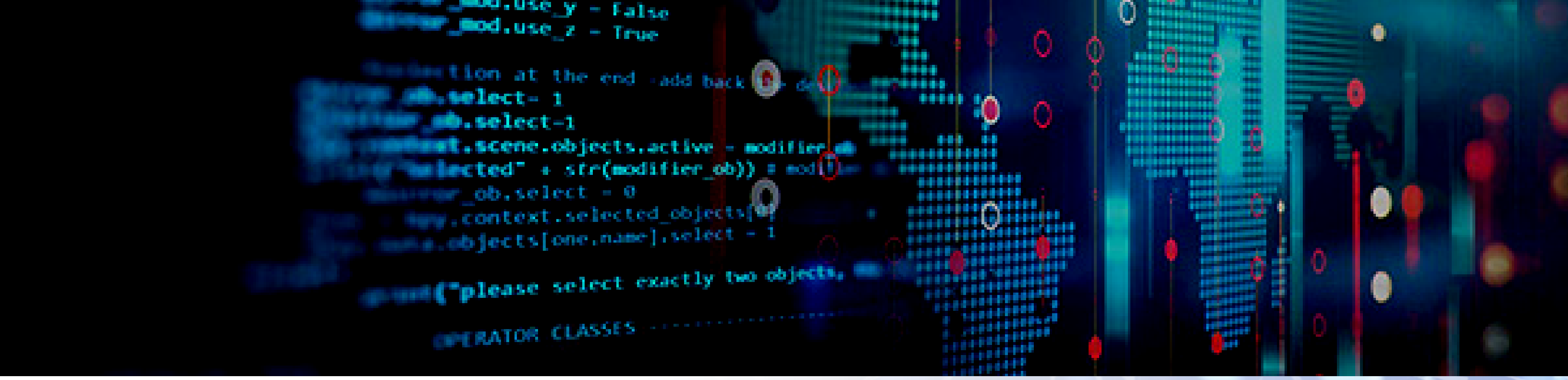
* Zeek 5.0.0
* OpenSSL Toolkit 3.0.5
* OpenSSL Toolkit 1.1.1q
* TripleCross Linux eBPF Rootkit
* C Language Reverse Shell Generator
* Global Socket 1.4.37
* Bash / Netcat Reverse Shells
* Queue Abstract Data Type Tool
* Blue Team Training Toolkit (BT3) 2.9
* Global Socket 1.4.36

Kali Linux Tutorials

* PersistBOF : Tool To Help Automate Common Persistence Mechanisms
* Mitmproxy2Swagger : Automatically Reverse-Engineer REST APIs Via Capturing Traffic
* BinAbsInspector : Vulnerability Scanner For Binaries
* Hakoriginfinder : Tool For Discovering The Origin Host Behind A Reverse Proxy. Useful For Bypassing C
* LEAF : Linux Evidence Acquisition Framework
* Stunner : Tool To Test And Exploit STUN, TURN And TURN Over TCP Servers
* Ransomware-Simulator : Ransomware Simulator Written In Golang
* FindFunc : Advanced Filtering/Finding of Functions in IDA Pro
* Pocsploit : A Lightweight, Flexible And Novel Open Source Poc Verification Framework
* DroidDetective : A Machine Learning Malware Analysis Framework For Android Apps

GBHackers Analysis

* Kids and Teens Forming Hacking Groups Online to Exchange Malware
* Critical PHP Flaws Allows Attackers to Execute Remote Code on QNAP NAS Devices
* Critical Flaws in MEGA Cloud Storage Let Attacker Decrypt User Data
* A 5-Year-Old Bug in Apple Safari Exploited in the Wild - Google Project Zero
* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3



Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

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

Hak5

* Live Hacking Q&A with Kody Kinzie and SheNetworks
* Live Hacking Q&A with Kody and Michael
* Rugged Tactical WiFi Pineapple Mk7

The PC Security Channel [TPSC]

* Malwarebytes: Test vs Ransomware
* Windows Zero Day: MSDT Follina Exploit Demonstration

Eli the Computer Guy

* What is a Firewall
* eBeggar Wednesday - Louis Rossmann YOUTUBE CHANNEL is DEAD (young man gets old)
* What is DHCP (Dynamic Host Configuration Protocol)
* What is DNS (Domain Name System)

Security Now

* The ZuoRAT - 0-Day Chrome, Firefox v102, HackerOne
* The "Hertzbleed&rdquo; Attack - 3rd Party FIDO2, Log4Shell, '311" Proposal

Troy Hunt

* Weekly Update 303

Intel Techniques: The Privacy, Security, & OSINT Show

* 269-New OSINT Tools & Breach Data Lessons
* 268-CCW Permits, UNREDACTED 003, & Linux Questions

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Windows Kerberos KerbRetrieveEncodedTicketMessage AppContainer Privilege Escalation
* Windows Kerberos Redirected Logon Buffer Privilege Escalation
* Xen PV Guest Non-SELFSNOOP CPU Memory Corruption
* EQS Integrity Line Cross Site Scripting / Information Disclosure
* Magnolia CMS 6.2.19 Cross Site Scripting
* Ransom Lockbit 3.0 MVID-2022-0621 Code Execution
* Advanced Testimonials Manager 5.6 SQL Injection
* Windows Defender Remote Credential Guard Authentication Relay Privilege Escalation
* Ransom Lockbit 3.0 MVID-2022-0620 Buffer Overflow
* DouPHP 1.2 Release 20141027 SQL Injection
* Paymoney 3.3 Cross Site Scripting
* Stock Management System 2020 SQL Injection
* Packet Storm New Exploits For June, 2022
* Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal
* PHP Library Remote Code Execution
* BigBlueButton 2.3 / 2.4.7 Cross Site Scripting
* Classified Listing 2.2.9 Cross Site Scripting
* TypeORM SQL Injection
* Backdoor.Win32.Coredoor.10.a MVID-2022-0618 Authentication Bypass
* Backdoor.Win32.EvilGoat.b MVID-2022-0619 Hardcoded Credential
* Backdoor.Win32.Cafeini.b MVID-2022-0617 Hardcoded Credential
* Fruits-Bazar 2021 1.0 SQL Injection
* Laundry Management System 1.0 SQL Injection
* AnyDesk 7.0.9 Arbitrary File Write / Denial Of Service
* OpenCart 3.x So Filter Shop By SQL Injection

CXSecurity

* 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
* Navigate CMS 2.9.4 Server-Side Request Forgery (SSRF) (Authenticated)
* Atlassian Confluence Namespace OGNL Injection

Proof of Concept (PoC) & Exploits

Exploit Database

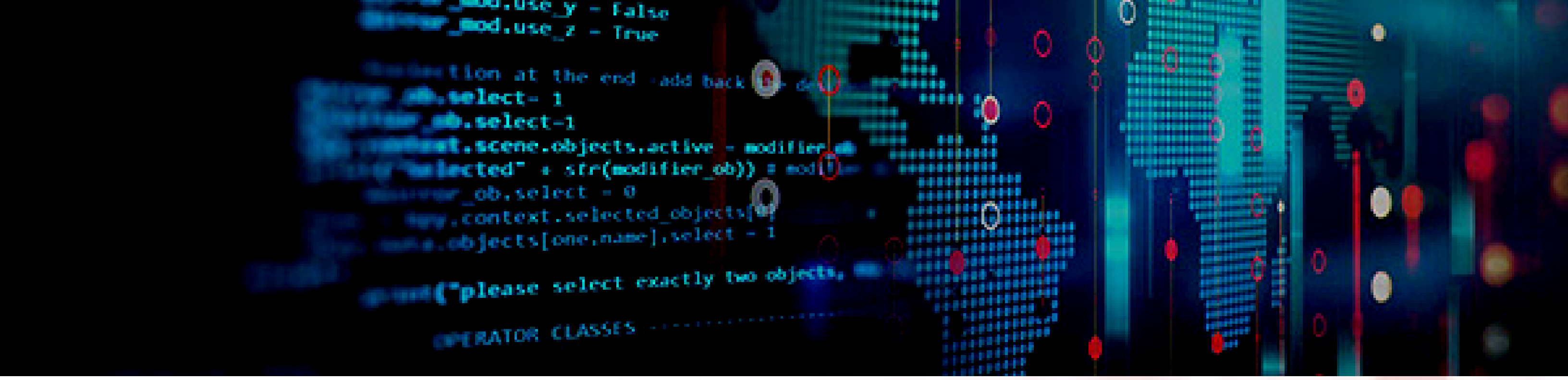
* [remote] WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)
* [webapps] Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)
* [webapps] WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scriptin
* [webapps] WordPress Plugin Weblizar 8.9 - Backdoor
* [webapps] SolarView Compact 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)
* [local] Real Player 16.0.3.51 - 'external::Import()' Directory Traversal to Remote Code Execution (RC
* [local] Real Player v.20.0.8.310 G2 Control - 'DoGoToURL()' Remote Code Execution (RCE)
* [webapps] Confluence Data Center 7.18.0 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)
* [remote] Telesquare SDT-CW3B1 1.1.0 - OS Command Injection

Exploit Database for offline use

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

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

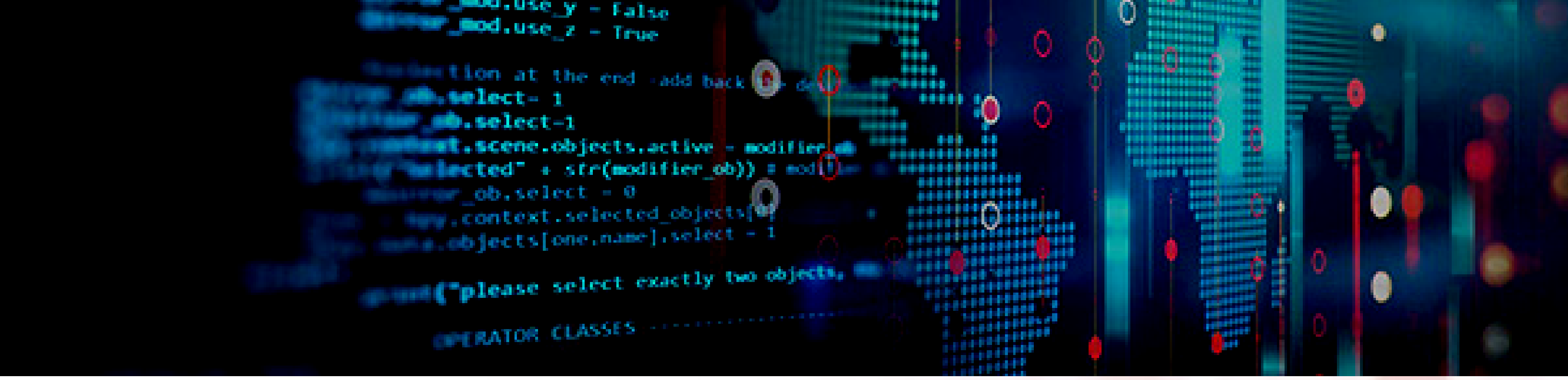
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://nemotonga.gov.to
https://nemotonga.gov.to notified by Reckless Cyber Army
https://camarasaj.ba.gov.br/1.php
https://camarasaj.ba.gov.br/1.php notified by -1
https://www.rhd.gov.bd/anika.html
https://www.rhd.gov.bd/anika.html notified by anon-dr-fox
https://simtaru.sulselprov.go.id/readme.html
https://simtaru.sulselprov.go.id/readme.html notified by AnonSec Team
http://www.plailocal.go.th/index.php
http://www.plailocal.go.th/index.php notified by Jaring
https://malut.bkkbn.go.id/readme.html
https://malut.bkkbn.go.id/readme.html notified by HackerMind.ID
https://camarapalhano.ce.gov.br/vz.txt
https://camarapalhano.ce.gov.br/vz.txt notified by aDriv4
https://plp.old.minzdrav.gov.ru/vz.txt
https://plp.old.minzdrav.gov.ru/vz.txt notified by aDriv4
https://socialauth.ufrr.br/vz.txt
https://socialauth.ufrr.br/vz.txt notified by aDriv4
http://kec-lape.sumbawakab.go.id/o.htm
http://kec-lape.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-labangka.sumbawakab.go.id/o.htm
http://kec-labangka.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-lantung.sumbawakab.go.id/o.htm
http://kec-lantung.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-moyohilir.sumbawakab.go.id/o.htm
http://kec-moyohilir.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-moyohulu.sumbawakab.go.id/o.htm
http://kec-moyohulu.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-lunyuk.sumbawakab.go.id/o.htm
http://kec-lunyuk.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-orongtelu.sumbawakab.go.id/o.htm
http://kec-orongtelu.sumbawakab.go.id/o.htm notified by typicalsadboy
http://kec-ropang.sumbawakab.go.id/o.htm
http://kec-ropang.sumbawakab.go.id/o.htm notified by typicalsadboy



Dark Web News

Darknet Live

[Two Charged for Selling Counterfeit Oxycodone Pills]

A federal grand jury returned an indictment charging two men for selling counterfeit pills on the darkweb. Edited on July 8, 2022, to correct a price listed in a previous version of this article. According to an announcement from the U.S. Attorney's Office for the Southern District of Indiana, Ethan Parker, 29, of Evansville, used a pill press to manufacture fentanyl-laced counterfeit pills. Parker sold the pressed pills to co-conspirators, including Joshua Harvey, 30, of Evansville. Harvey then resold pills to "mid-level distributors&rdquo; in their drug trafficking organization, mainly in the Evansville, Indiana, area. Parker obtained pound quantities of fentanyl powder from "an unknown source of supply&rdquo; in Louisville, Kentucky. Harvey also drove Parker to a supplier to "acquire pound quantities of fentanyl powder to facilitate the manufacture and distribution of fentanyl-laced counterfeit pills,&rdquo; according to the press release. Ethan Parker and Joshua Harvey in mugshots provided by Vanderburgh County Sheriff's Office "During the investigation, it is alleged that Parker and Harvey displayed a high degree of technological sophistication, utilizing encrypted messaging applications to purchase, advertise, and sell fentanyl-laced counterfeit pills, as well as utilizing the "Dark Web&rdquo; and cryptocurrency to pay for drug transactions.&rdquo; A bag of pills seized by police | 14news.com Harvey and other co-conspirators would purchase pills and communicate with Parker through encrypted messaging applications and Facebook messages. In one instance, Parker directed Harvey to a "channel&rdquo; on an encrypted messaging application where Parket sold counterfeit pills. In the channel, Parket advertised 50 pills for $375, 100 pills for $750, and 1,000 pills for $5,000. The indictment does not identify the "encrypted&rdquo; messaging application but based on the description provided, it appears to be referencing Telegram. On March 10, 2022, Harvey sent Parker a message through Facebook about aquiring counterfeit pills. Parker directed Harvey to a "webpage on the darkweb&rdquo; where Parker sold pills. Police found a pill press during execution of a search warrant. On March 15, 2022, Harvey sent Parker $900 through Cash App; investigators believe the march 15 payment was for Parker's counterfeit pills. During the investigation, law enforcement officers seized approximately 140 grams of fentanyl-laced counterfeit pills and powder, two pill presses, and various dies and punches utilized to press pills. On July 6, 2022, federal law enforcement officers arrested the defendants. Parker faces counts of Conspiracy to Distribute Fentanyl, Distribution of Tableting Machine, and Possession of Tableting Machine. Harvey faces only the Conspiracy to Distribute Fentanyl charge. A warning placed on the door of Parker's home. Two Evansville Men Indicted for Trafficking Fentanyl and Allegedly Manufacturing Fentanyl-Laced Counterfeit Pills Using a Pill Press | archive.is, justice.gov Indictment pdf A previous version of this article listed the price point for 50 pills as $350. The correct number advertised by Parker was $375. (via darknetlive.com at https://darknetlive.com/post/indiana-men-charged-for-fentanyl-trafficking/)

[Fraudulent Credit Card Maker Sentenced to 108 Months in Prison]

A prolific fraudster who produced fraudulent credit cards using stolen card numbers from the darkweb was sentenced to 108 months in prison. United States District Judge Eldon E. Fallon sentenced Maurice Durio, 42, to 108 months in prison. Durio had previously pleaded guilty to a credit card fraud charge. According to U.S. Attorney Duane A. Evans, Durio operated "a card manufacturing plant&rdquo; at an office space in an office park in Houston. Durio's co-defendant, Edward Toliver, also rented office space in the same office park for the same purpose. The duo outfitted the office spaces with equipment used to manufacture fraudulent credit cards. __ U.S. Attorney Duane A. Evans announced the sentence. Durio and Toliver purchased stolen credit card numbers from sources on the darkweb, according to a press release from the U.S. Attorney's Office for the Eastern District of Louisiana. Toliver also purchased cards from a source he had met in prison. With the assistance of several co-conspirators, Durio and Toliver created templates for credit cards on their computers and "downloaded credit card templates on laptop computers and transferred the stolen credit card numbers into the templates, which were then used to create tens of thousands of fraudulent access devices. The cards would generally be printed in batches with the same name appearing on numerous cards. The name was typically the real name of a co-conspirator. The cards were embossed with numbers, and corresponding account information was encoded on the strips on the back of the cards.&rdquo; Durio and Toliver distributed thousands of fraudulent credit cards to people who purchased valuable merchandise or gift cards. Investigators learned about the operation after arresting people who had cards produced by Durio in their possession. Law enforcement officers from the Secret Service "were able to tie these card seizures to the plants&rdquo; operated by Durio. During the execution of a search warrant at the office park in Houston, feds seized access to device-making equipment, embossers, scanners, high-end printers, thousands of fraudulent credit cards, and a laptop computer. Durio had saved 80,000 stolen credit card numbers in files on the computer. On other computers used by Durio, feds found approximately 300,000 additional stolen card numbers. New Orleans Man Sentenced to Nine Years in Federal Prison for Massive Credit Card Fraud Scheme | archive.is, archive.org, justice.gov (via darknetlive.com at https://darknetlive.com/post/credit-card-fraudster-sentenced-to-prison/)

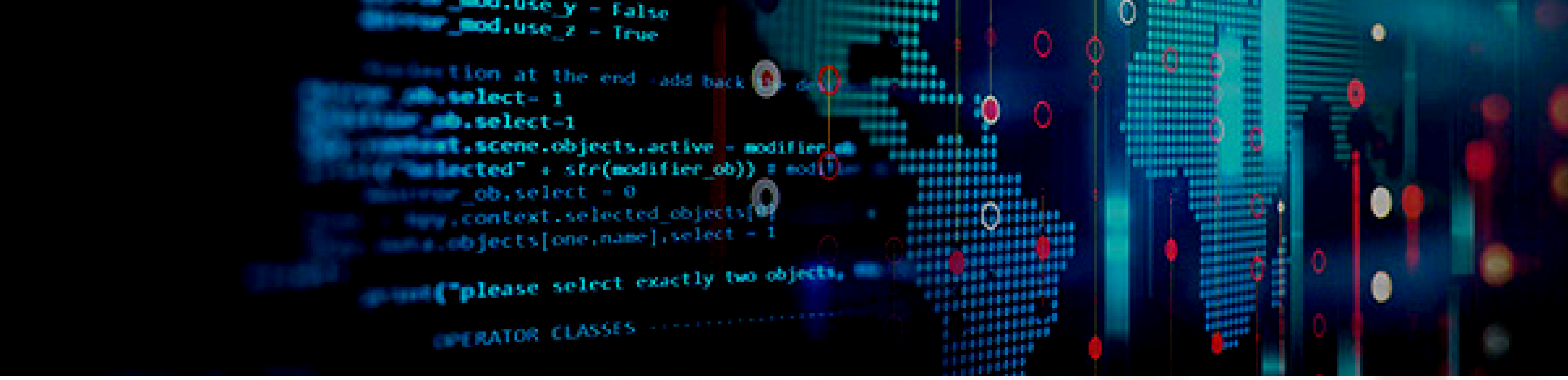
'Welcome To Video' Admin Sentenced to Prison for Two Years

The administrator of one of the "world's largest child pornography websites&rdquo; was sentenced to two years in prison for hiding proceeds from the forum. Son Jong-woo, the convicted operator of the Welcome To Video forum on the darkweb, was sentenced to five years in prison for concealing about 400 million won ($305,000). The money came from users of Son's forum who spent Bitcoin to access child sexual abuse material (CSAM). The defendant has already served an 18-month sentence for violating child protection laws. A grand jury in the United States returned an indictment, accusing Son of: Conspiracy to Advertise Child Pornography; Advertising Child Pornography; Production of Child Pornography for Importation to the United States; Conspiracy to Distribute Child Pornography; Distribution of Child Pornography; and Money Laundering. Before Son completed his sentence, his father filed a criminal complaint against him for "violation of the law on criminal proceeds concealment.&rdquo; The move was interpreted as an attempt to prevent Son's extradition to the United States. __ The 'Welcome to Video' seizure banner uploaded by law enforcement. The Seoul High Court blocked Son's extradition because Son's cooperation would assist authorities in investigating "sexually exploitative content.&rdquo; Authorities then filed new charges against Son, including criminal proceeds concealment and gambling with the concealed proceeds. The Korean National Police in South Korea arrested Son on March 5, 2018. Agents from the IRS-CI, HSI, and National Crime Agency in the United Kingdom seized the servers Son had used to host the onion service. The operation resulted in the seizure of eight terabytes of CSAM. A Department of Justice press release revealed that 45% of the 250,000 unique videos seized by police contained new images. "Welcome To Video offered these videos for sale using the cryptocurrency bitcoin. Typically, sites of this kind give users a forum to trade in these depictions. This Darknet website is among the first of its kind to monetize child exploitation videos using bitcoin. In fact, the site itself boasted over one million downloads of child exploitation videos by users. Each user received a unique bitcoin address when the user created an account on the website. An analysis of the server revealed that the website had more than one million bitcoin addresses, signifying that the website had capacity for at least one million users.&rdquo; "The agencies have shared data from the seized server with law enforcement around the world to assist in identifying and prosecuting customers of the site. This has resulted in leads sent to 38 countries and yielded arrests of 337 subjects around the world. The operation has resulted in searches of residences and businesses of approximately 92 individuals in the United States. Notably, the operation is responsible for the rescue of at least 23 minor victims residing in the United States, Spain and the United Kingdom, who were being actively abused by the users of the site.&rdquo;   South Korean man jailed over proceeds from child porn site, Yonhap reports | archive.is, archive.org, reuters.com (via darknetlive.com at https://darknetlive.com/post/welcome-to-video-admin-sentenced-again/)

Washington Man Heads to Prison for Selling Meth on the Darkweb

A Washington man who sold methamphetamine on the darkweb was sentenced to five years in prison. U.S. Attorney Nick Brown announced that Ryan Kane, 34, of Bothell, Washington, had been sentenced to five years in prison. Kane had pleaded guilty to one count of Possession of Methamphetamine with Intent to Distribute in March 2022. The investigation that resulted in Kane's arrest began in March 2021 after the Australian Border Force (ABF) had seized 39 computer hard drives containing crystal methamphetamine from a UPS package. The "seizure weight&rdquo; was fou kilograms. On April 25, 2021, a United States Postal Service (USPS) outbound mail parcel arrived at the SFO International Mail Facility destined for Australia. The package was declared a "3.5IN DESKTOP HARDDRIVE,&rdquo; and a Customs and Border Protention officer referred the package for inspection. Officers x-rayed the package, which revealed inconsistencies between the description and the image, according to the criminal complaint. _ Kane shipped methamphetamine to customers inside hard drives. "In the image, the inside of the hard drives appeared granular, as if they were full of thousands of small particles. This is in stark contrast to a smooth solid piece of metal or plastic seen from a legitimate hard drive. A physical examination of USPS Package 1 revealed 18 vacuum sealed hard drives. Furthermore, CBPO Salas opened a hard drive and observed a crystalline substance inside. CBPO Coleman tested the suspected substance inside the hard drive and it field-tested positive for methamphetamine. CBPO Salas calculated the gross weight of the hard drives with the methamphetamine to be 8,096 grams.&rdquo; On April 27, 2021, a similar USPS package arrived at the San Francisco International Mail Facility destined for Australia. The package was declared as a "3.5IN DESKTOP HARDDRIVE.&rdquo; Customs officers refereed the package for inspection. Officers x-rayed the package, noted the same inconsistencies in the first package, and then opened the package. "The wrapping and feel of the hard drives were inconsistent with what's expected of a new drive. Furthermore, CBPO Salas opened a hard drive and a crystalline substance was found inside. CBPO Salas conducted a field test on the substance contained inside the hard drive and determined that the substance was methamphetamine. CBPO Salas determined that the total gross weight of the meth and hard drives was 8,173 grams.&rdquo; USPS business records revealed that someone using the I.P. address 50.106.18.109 had tracked the first USPS package eight times and the second USPS package three times. The I.P. address was assigned to Ziply Fiber, an Internet Service Provider. Records from Ziply Fiber identify the subscriber for the I.P. address as Ryan Kane at 12618 NE 180th S.T., Apt EE302 Bothell, WA 98011. On June 7, 2021, agents executed a search warrant at Kane's apartment, vehicle, and person. Agents found 1,844.1 grams of methamphetamine inside a jar in Kane's bedroom. _ Agents found 1,844.1 grams of methamphetamine inside a jar in Kane's room. In the same room as the methamphetamine, agents found 15 hollowed-out hard drives containing more methamphetamine. _ Kane had a stack of hard drives containing methamphetamine. Agents also found a notebook containing the username of Kane's darkweb vendor account, artwork related to the same vendor account, USPS Priority Mail Express Boxes, FedEx Boxes, multiple shipping labels, and a 9mm pistol. Kane told agents that he knew about the methamphetamine in his apartment and admitted that he had been selling it. However, Kane also told agents that an outlaw motorcycle gang had extorted him into selling the methamphetamine. "The Defendant refused to provide any names of individuals who had threatened him or supplied the methamphetamine,&rdquo; Special Agent Matt Eidinger wrote in the criminal complaint. _ Court documents do not disclose the username of Kane's vendor account. They do identify Wallstreet Market as one of the marketplaces Kane had used. "Specifically, on October 17, 2019, Mr. Kane received an order for five grams of methamphetamine from the Dark Web marketplace Wall Street. Mr. Kane processed and packaged the methamphetamine and shipped the package. The parcel contained approximately five grams of a mixture or substance containing a detectable amount of methamphetamine.&rdquo; The total gross weight of the methamphetamine was 8,280.4 grams. U.S. District Judge James L. Robart said at the sentencing hearing, addressing Kane, "This isn't about you&hellip;. This is about what you did to the community &hellip;sending drugs not just into our community, but the world. What you did is decidedly wrong.&rdquo; "Mr. Kane's conviction and today's sentence demonstrates how smugglers cannot hide behind the perceived veil of secrecy associated with Dark Web marketplaces,&rdquo; said Special Agent in Charge (SAC) Robert Hammer, who oversees Homeland Security Investigations (HSI) operations in the Pacific Northwest. "HSI through its transnational law enforcement footprint will doggedly pursue these cases with our law enforcement partners within the U.S. and abroad.&rdquo; Bothell, Washington, man sentenced to 5 years in prison for dealing drugs hidden in computer hard drives | archive.is, archive.org, justice.gov Indictment pdf (via darknetlive.com at https://darknetlive.com/post/washington-man-sentenced-to-prison-for-selling-meth/)

Dark Web Link



Trend Micro Anti-Malware Blog

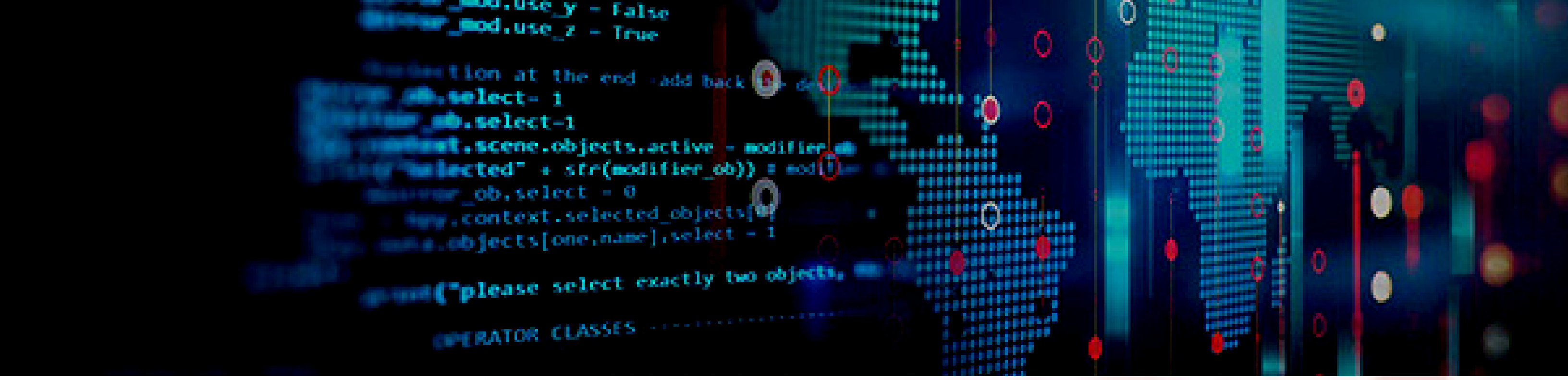
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Today's SOC Strategies Will Soon Be Inadequate
* How to Build and Enable a Cyber Target Operating Model
* Exploitation of Mitel MiVoice Connect SA CVE-2022-29499
* For Finserv Ransomware Attacks, Obtaining Customer Data Is the Focus
* [Security Nation] Pete Cooper and Irene Pontisso on the Results of the UK Government's Security Cultu
* What's New in InsightIDR: Q2 2022 in Review
* Cloud Complexity Requires a Unified Approach to Assessing Risk
* Metasploit Weekly Wrap-Up
* Rapid7 Belfast Recognized for "Company Connection" During COVID-19 Pandemic



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for Multiple Products
* OpenSSL Releases Security Update
* North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Hea
* Google Releases Security Update for Chrome
* Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats
* CISA Adds One Known Exploited Vulnerability to Catalog
* #StopRansomware: MedusaLocker
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* 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 June 27, 2022
* Vulnerability Summary for the Week of June 20, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5505-1

Ubuntu Security Notice 5505-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Likang Luo discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to 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-5488-2

Ubuntu Security Notice 5488-2 - USN-5488-1 fixed vulnerabilities in OpenSSL. This update provides the corresponding updates for Ubuntu 16.04 ESM. Chancen and Daniel Fiala 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.

Red Hat Security Advisory 2022-5498-01

Red Hat Security Advisory 2022-5498-01 - Red Hat Satellite is a systems management tool for Linux-based infrastructure. It allows for provisioning, remote management, and monitoring of multiple Linux deployments with a single centralized tool. Issues addressed include HTTP request smuggling, buffer overflow, bypass, code execution, cross site scripting, denial of service, heap overflow, information leakage, privilege escalation, remote shell upload, remote SQL injection, and traversal vulnerabilities.

Ubuntu Security Notice USN-5502-1

Ubuntu Security Notice 5502-1 - Alex Chernyakhovsky discovered that OpenSSL incorrectly handled AES OCB mode when using the AES-NI assembly optimized implementation on 32-bit x86 platforms. A remote attacker could possibly use this issue to obtain sensitive information.

Ubuntu Security Notice USN-5503-1

Ubuntu Security Notice 5503-1 - Demi Marie Obenour discovered that GnuPG incorrectly handled injection in the status message. A remote attacker could possibly use this issue to forge signatures.

Ubuntu Security Notice USN-5479-2

Ubuntu Security Notice 5479-2 - USN-5479-1 fixed vulnerabilities in PHP. This update provides the corresponding updates for Ubuntu 16.04 ESM. Charles Fol discovered that PHP incorrectly handled initializing certain arrays when handling the pg_query_params function. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code. Charles Fol discovered that PHP incorrectly handled passwords in mysqlnd. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-5491-01

Red Hat Security Advisory 2022-5491-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. Issues addressed include buffer overflow and privilege escalation vulnerabilities.

Ubuntu Security Notice USN-5501-1

Ubuntu Security Notice 5501-1 - It was discovered that Django incorrectly handled certain SQL. An attacker could possibly use this issue to expose sensitive information.

Ubuntu Security Notice USN-5500-1

Ubuntu Security Notice 5500-1 - 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. Lin Ma discovered that the NFC Controller Interface implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5493-2

Ubuntu Security Notice 5493-2 - It was discovered that the 8 Devices USB2CAN interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-5485-2

Ubuntu Security Notice 5485-2 - It was discovered that some Intel processors did not completely perform cleanup actions on multi-core shared buffers. A local attacker could possibly use this to expose sensitive information. It was discovered that some Intel processors did not completely perform cleanup actions on microarchitectural fill buffers. A local attacker could possibly use this to expose sensitive information. It was discovered that some Intel processors did not properly perform cleanup during specific special register write operations. A local attacker could possibly use this to expose sensitive information.

Red Hat Security Advisory 2022-5483-01

Red Hat Security Advisory 2022-5483-01 - 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. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-5481-01

Red Hat Security Advisory 2022-5481-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5245-01

Red Hat Security Advisory 2022-5245-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Issues addressed include bypass and password leak vulnerabilities.

Red Hat Security Advisory 2022-5475-01

Red Hat Security Advisory 2022-5475-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5257-01

Red Hat Security Advisory 2022-5257-01 - libinput is a library that handles input devices for display servers and other applications that need to directly deal with input devices. Issues addressed include format string and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-5439-01

Red Hat Security Advisory 2022-5439-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include heap overflow, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5249-01

Red Hat Security Advisory 2022-5249-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, information leakage, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5251-01

Red Hat Security Advisory 2022-5251-01 - The pcre2 package contains a new generation of the Perl Compatible Regular Expression libraries for implementing regular expression pattern matching using the same syntax and semantics as Perl. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2022-5244-01

Red Hat Security Advisory 2022-5244-01 - Expat is a C library for parsing XML documents. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-5479-01

Red Hat Security Advisory 2022-5479-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5476-01

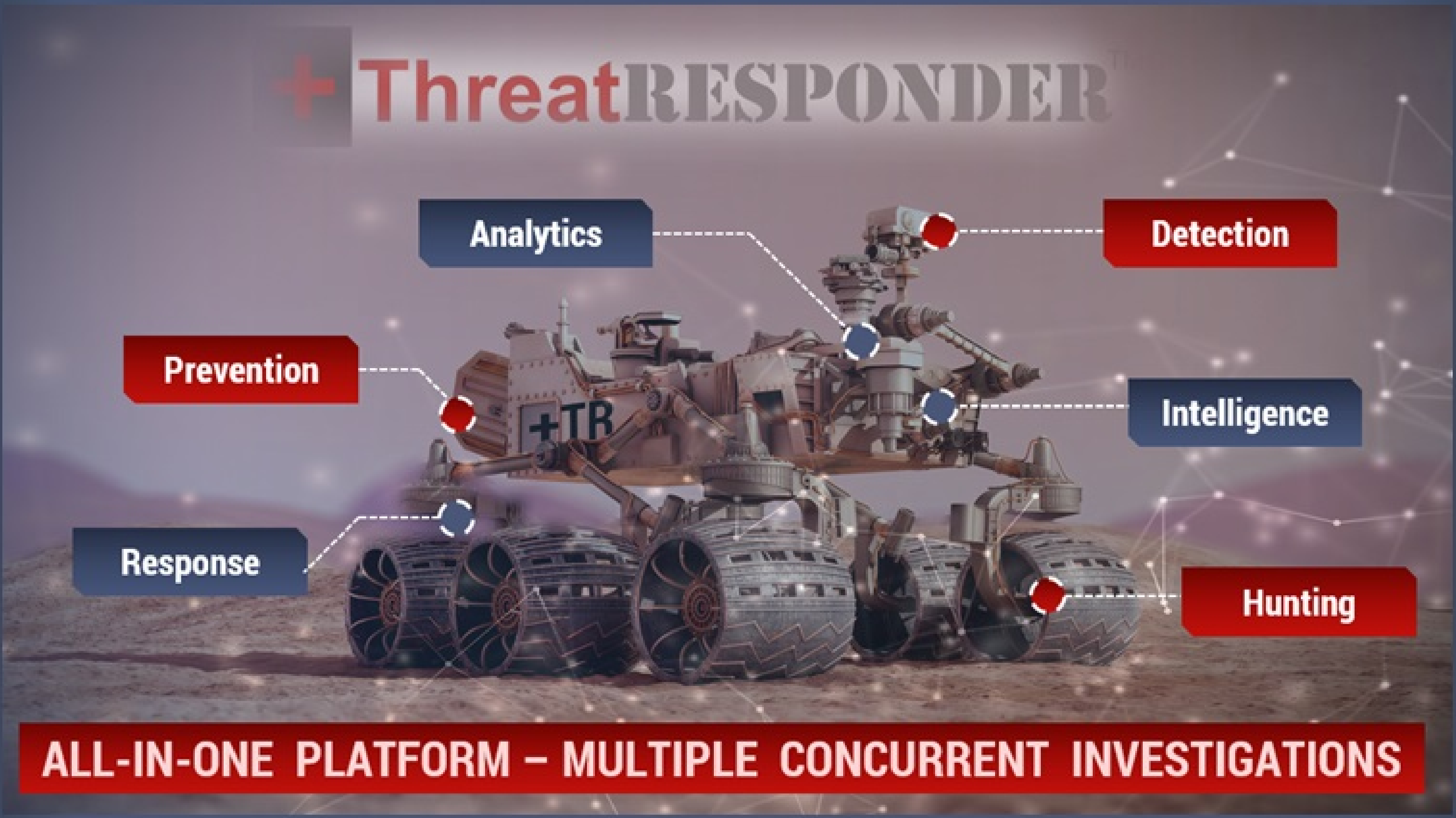
Red Hat Security Advisory 2022-5476-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include buffer overflow, privilege escalation, and use-after-free vulnerabilities.

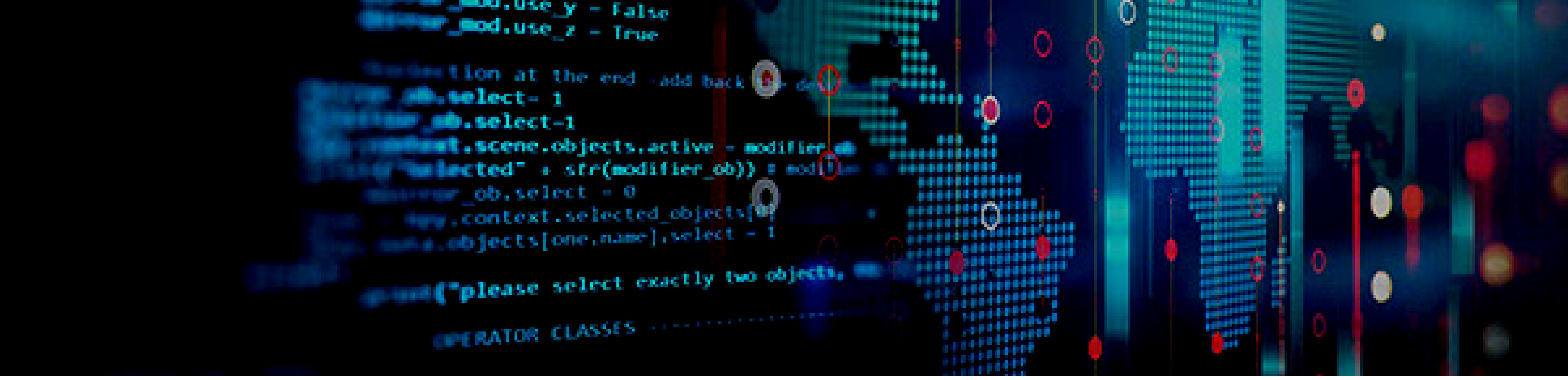
Red Hat Security Advisory 2022-5263-01

Red Hat Security Advisory 2022-5263-01 - Kernel-based Virtual Machine is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm packages provide the user-space component for running virtual machines that use KVM. Issues addressed include a memory leak vulnerability.

Red Hat Security Advisory 2022-5482-01

Red Hat Security Advisory 2022-5482-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.


+ThreatRESPONDER
Analytics
Detection
Prevention
Intelligence
+TR
Response
Hunting
ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

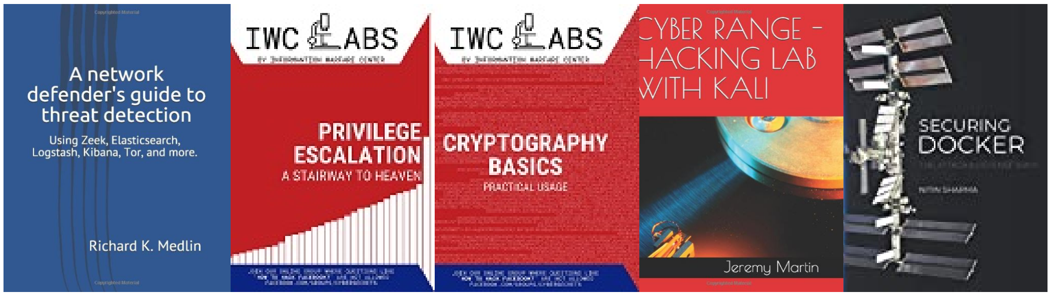

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier
"elected" + str(modifier_ob)) + mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP