Aug-15-22

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

August 15, 2022

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

Summary

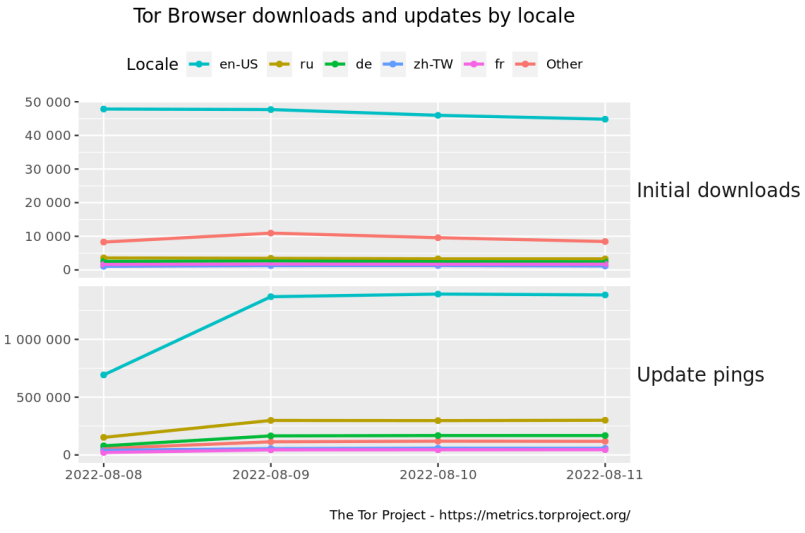
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

Packet Storm Security

* FTC Kicks Off Potentially Massive New Regulation On Commercial Surveillance
* Starlink Successfully Hacked Using $25 Modchip
* FAANGs Failing On Keeping User Data Safe From Bug Hunters
* Facebook's In-App Browser On iOS Tracks Anything You Do On Any Website
* Dutch Detain Suspected Developer Of Crypto Mixer Tornado Cash
* NHS IT Supplier Held To Ransom By Hackers
* Meta's Chatbot Says The Company Exploits People
* Researchers Use Invisible Finger To Remotely Control Touchscreens
* Cisco Confirms Network Breach Via Hacked Employee Google Account
* Stats Say Chinese Researchers Not Deterred By China's Vulnerability Law
* Ukrainian Website Threat Landscape Throughout 2022
* Former Twitter Employee Convicted As Saudi Spy
* APIC Fail: Intel Sunny Cove Chips With SGX Spill Secrets
* Cloudflare: Someone Tried To Pull The Twilio Phishing Tactic On Us
* Microsoft Patches Dogwalk Zero Day And 17 Critical Flaws
* Chinese Scams Target Kids With Promise Of Extra Gaming Hours
* Twilio Customer Data Exposed After Its Staffers Got Phished
* Scientists Hid Encryption Key For Wizard Of Oz Text In Plastic Molecules
* Crypto And The US Government Are Headed For A Decisive Showdown
* China-Linked Spies Used Six Backdoors To Steal Info From Defense, Industrial Enterprise Orgs
* Small Businesses Count Cost Of Apple's Privacy Changes
* San Diego Citizens Wrest Control Of Surveillance Tech Away From Police
* Slack Leaked Hashed Passwords From Its Servers For Years
* Dark Utilities C2 Service Draws Thousands Of Cyber Criminals
* U.S. Imposes Sanctions On Virtual Currency Mixer Tornado Cash

Krebs on Security

* Sounding the Alarm on Emergency Alert System Flaws
* It Might Be Our Data, But It's Not Our Breach
* The Security Pros and Cons of Using Email Aliases
* Microsoft Patch Tuesday, August 2022 Edition
* Class Action Targets Experian Over Account Security
* Scammers Sent Uber to Take Elderly Lady to the Bank
* No SOCKS, No Shoes, No Malware Proxy Services!
* 911 Proxy Service Implodes After Disclosing Breach
* Breach Exposes Users of Microleaves Proxy Service
* A Retrospective on the 2015 Ashley Madison Breach

Dark Reading

* Patch Madness: Vendor Bug Advisories Are Broken, So Broken
* Software Supply Chain Chalks Up a Security Win With New Crypto Effort
* Novel Ransomware Comes to the Sophisticated SOVA Android Banking Trojan
* How to Clear Security Obstacles and Achieve Cloud Nirvana
* Microsoft: We Don't Want to Zero-Day Our Customers
* Krebs: Taiwan, Geopolitical Headwinds Loom Large
* After Colonial Pipeline, Critical Infrastructure Operators Remain Blind to Cyber-Risks
* Supply Chain Security Startup Phylum Wins the First Black Hat Innovation Spotlight
* Cyber-Insurance Fail: Most Businesses Lack Ransomware Coverage
* 4 Flaws, Other Weaknesses Undermine Cisco ASA Firewalls
* New Cross-Industry Group Launches Open Cybersecurity Framework
* Cisco Confirms Data Breach, Hacked Files Leaked
* The Time Is Now for IoT Security Standards
* Dark Reading News Desk: Live at Black Hat USA 2022
* New Open Source Tools Launched for Adversary Simulation
* New HTTP Request Smuggling Attacks Target Web Browsers
* Multiple Vulnerabilities Discovered in Device42 Asset Management Appliance
* Many ZTNA, MFA Tools Offer Little Protection Against Cookie Session Hijacking Attacks
* Rethinking Software in the Organizational Hierarchy
* Mimecast Announces Mimecast X1â„¢ Platform Providing Customers With Email and Collaboration Security

The Hacker News

* Newly Uncovered PyPI Package Drops Fileless Cryptominer to Linux Systems
* Tornado Cash Developer Arrested After U.S. Sanctions the Cryptocurrency Mixer
* Chinese Hackers Backdoored MiMi Chat App to Target Windows, Linux, macOS Users
* Researchers Uncover UEFI Secure Boot Bypass in 3 Microsoft Signed Boot Loaders
* Xiaomi Phones with MediaTek Chips Found Vulnerable to Forged Payments
* U.S. Government Offers $10 Million Reward for Information on Conti Ransomware Gang
* Facebook Testing Default End-to-End Encryption and Encrypted Backups in Messenger
* Cisco Patches High-Severity Vulnerability Affecting ASA and Firepower Solutions
* Fast and Secure VPN on a Budget? Private Internet Access VPN Has You Covered
* Researchers Warn of Ongoing Mass Exploitation of Zimbra RCE Vulnerability
* Conti Cybercrime Cartel Using 'BazarCall' Phishing Attacks as Initial Attack Vector
* Cisco Confirms It's Been Hacked by Yanluowang Ransomware Gang
* Hackers Behind Cuba Ransomware Attacks Using New RAT Malware
* What the Zola Hack Can Teach Us About Password Security
* Critical Flaws Disclosed in Device42 IT Asset Management Software

Security Week

* Killnet Releases 'Proof' of its Attack Against Lockheed Martin
* US Government Shares Photo of Alleged Conti Ransomware Associate
* CISA, FBI Warn Organizations of Zeppelin Ransomware Attacks
* Microsoft Paid $13.7 Million via Bug Bounty Programs Over Past Year
* Realtek SDK Vulnerability Exposes Routers From Many Vendors to Remote Attacks
* FTC Looking at Rules to Corral Tech Firms' Data Collection
* Security Researchers Dig Deep Into Siemens Software Controllers
* Zero-Day Vulnerability Exploited to Hack Over 1,000 Zimbra Email Servers
* Black Hat USA 2022 - Announcements Summary
* Intel Introduces Protection Against Physical Fault Injection Attacks
* Cisco Patches High-Severity Vulnerability in Security Solutions
* OT Security Firm Warns of Safety Risks Posed by Alerton Building System Vulnerabilities
* Researchers Find Stolen Algorithms in Commercial Cybersecurity Products
* Critical Vulnerabilities Found in Device42 Asset Management Platform
* Palo Alto Networks Firewalls Targeted for Reflected, Amplified DDoS Attacks
* Cisco Hacked by Ransomware Gang, Data Stolen
* New Identity Verification Feature Boosts Google Workspace Protections
* Organizations Warned of Critical Vulnerabilities in NetModule Routers
* Cloudflare Also Targeted by Hackers Who Breached Twilio
* NIST Post-Quantum Algorithm Finalist Cracked Using a Classical PC
* Security Firm Finds Flaws in Indian Online Insurance Broker
* How Bot and Fraud Mitigation Can Work Together to Reduce Risk
* Zero Trust Provider Mesh Security Emerges From Stealth Mode
* Number of Ransomware Attacks on Industrial Orgs Drops Following Conti Shutdown
* Intel Patches Severe Vulnerabilities in Firmware, Management Software
* Cyberattack Victims Often Attacked by Multiple Adversaries: Research

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* U.S. Government Warns of Increased Texting Scams as Mobile Attacks are Up 100%
* Massive Network of Over 10,000 Fake Investment Sites Targets Europe
* Phishing-as-a-Service Platform "Robin Banks" Helps Cybercriminals Target Customers of Financial Insti
* 92% of Organizations Have Experienced a Security Incident as a Result of an Email-Borne Threat
* New Paypal Phishing Scam Uses "Legitimate" Invoices to Reach Victim Inboxes
* SolidBit Ransomware Targets League of Legends Players
* Recent Cisco Hack by Ransomware Group Started Because of a Phishing Attack
* The Top 8 Most Common Types of DNS Records
* DPRK Operators Impersonate CoinBase
* New Phishing Campaign is Now Targeting Coinbase Users

ISC2.org Blog

* LATEST CYBERTHREATS AND ADVISORIES - AUGUST 12, 2022
* #ISC2Congress: Empower Your Weekend with Training
* (ISC)² and F5 Examine OWASP'S "Top 10" Report on New Web Application Security Risks
* Submit Your Comments to NIST Regarding HIPAA Security
* #ISC2Congress Theme: EMPOWER

HackRead

* Cisco Confirms Network Breach After Employee's Google Account was Hacked
* Killnet Claim They've Stolen Employee Data from Lockheed Martin
* Ways That VoIP Technology Is Impacting Marketplaces and How to Adapt
* Crucial Cybersecurity Software Features (2022)
* Download New Kali Linux 2022.3
* Nation-State Hackers Targeted Facebook in Cyber Espionage Attacks - Meta
* The top benefits of getting CompTIA Network+ certification

Koddos

* Cisco Confirms Network Breach After Employee's Google Account was Hacked
* Killnet Claim They've Stolen Employee Data from Lockheed Martin
* Ways That VoIP Technology Is Impacting Marketplaces and How to Adapt
* Crucial Cybersecurity Software Features (2022)
* Download New Kali Linux 2022.3
* Nation-State Hackers Targeted Facebook in Cyber Espionage Attacks - Meta
* The top benefits of getting CompTIA Network+ certification

Naked Security

* S3 Ep95: Slack leak, Github onslaught, and post-quantum crypto [Audio + Text]
* APIC/EPIC! Intel chips leak secrets even the kernel shouldn't see…
* Slack admits to leaking hashed passwords for five years
* Traffic Light Protocol for cybersecurity responders gets a revamp
* GitHub blighted by "researcher" who created thousands of malicious projects
* S3 Ep94: This sort of crypto (graphy), and the other sort of crypto (currency!) [Audio + Text]
* Post-quantum cryptography - new algorithm "gone in 60 minutes"
* Cryptocoin "token swapper" Nomad loses $200 million in coding blunder
* GnuTLS patches memory mismanagement bug - update now!
* How to celebrate SysAdmin Day!

Threat Post

* Feds: Zeppelin Ransomware Resurfaces with New Compromise, Encryption Tactics
* Facebook's In-app Browser on iOS Tracks 'Anything You Do on Any Website'
* Starlink Successfully Hacked Using $25 Modchip
* New Hacker Forum Takes Pro-Ukraine Stance
* Cisco Confirms Network Breach Via Hacked Employee Google Account
* Inside the Hackers' Toolkit - Podcast
* Microsoft Patches 'Dogwalk' Zero-Day and 17 Critical Flaws
* Virtual Currency Platform 'Tornado Cash' Accused of Aiding APTs
* Phishers Swim Around 2FA in Coinbase Account Heists
* Open Redirect Flaw Snags Amex, Snapchat User Data

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

IBM Security Intelligence

Unfortunately, at the time of this report, the IBM Security Intelligence Blog resource was not availible.

InfoWorld

* What's new in Rust 1.63
* TypeScript 4.8 shines on intersection and union types
* What goes in a metacloud?
* What's the Go programming language really good for?
* Angular 15 promises to simplify development
* How to implement JWT authentication in ASP.NET Core 6
* Intro to MicroStream: Super-fast serialization in Java
* Visual Studio Code 1.70 eases title bar customization
* IT leaders struggle with application modernization, survey finds
* Manage your tasks with the Microsoft To Do API

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

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 quantum state of Linux kernel garbage collection CVE-2021-0920 (Part I)
* 2022 0-day In-the-Wild Exploitation…so far

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.

* CryptoBurst CTF
* Paradigm CTF 2022
* WMCTF2022
* Midnight Sun CTF 2022 Finals
* Hacker's Playground 2022
* CTFZone 2022
* HITB SECCONF CTF 2022
* MapleCTF 2022
* Balsn CTF 2022
* CakeCTF 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

* GNUnet P2P Framework 0.17.4
* Falco 0.32.2
* American Fuzzy Lop plus plus 4.02c
* GNUnet P2P Framework 0.17.3
* Faraday 4.0.4
* Wireshark Analyzer 3.6.7
* Clam AntiVirus Toolkit 0.105.1
* Logwatch 7.7
* AIEngine 2.2.0
* GNUnet P2P Framework 0.17.2

Kali Linux Tutorials

* Bpflock : eBPF Driven Security For Locking And Auditing Linux Machines
* Laurel : Transform Linux Audit Logs For SIEM Usage
* modDetective : Tool That Chronologizes Files Based On Modification Time In Order To Investigate Recen
* LambdaGuard : AWS Serverless Security
* LiveTargetsFinder : Generates Lists Of Live Hosts And URLs For Targeting, Automating The Usage Of Mas
* RESim : Reverse Engineering Software Using A Full System Simulator
* Cdb : Automate Common Chrome Debug Protocol Tasks To Help Debug Web Applications
* Pinecone : A WLAN Red Team Framework
* Koh : The Token Stealer
* Zenbuster : Multi-threaded URL Enumeration/Brute-Forcing Tool

GBHackers Analysis

* Hackers Use Open Redirect Vulnerabilities in Online Services to Deliver Phishing Content
* Hackers Exploiting High-Severity Zimbra Flaw to Steal Email Account Credentials
* 24-Year-Old Australian Hacker Arrested For Creating and Selling Spyware
* Critical SonicWall Vulnerability Allows SQL Injection - Patch Now!
* Security Giant Entrust Hacked - Attackers Stole Data From Internal Systems

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 30 - Blue Team Village Interview
* DEF CON 30 - Cloud Village interview
* DEF CON 30 - Hardware Hacking Village Interview
* DEF CON 30 - Crypto and Privacy interview with Silk

Hak5

* Introducing the WiFi Coconut - Shannon & Darren @ DEF CON 30!
* NEW 🥥🌴 WiFi Coconut - Full Spectrum Sniffing
* Emergency Alert System Can Be HACKED! - ThreatWire

The PC Security Channel [TPSC]

* Tech Support Scam installs RAT (when asked for refund)
* Kaspersky Plus Review: First Impressions

Eli the Computer Guy

* LEGO ROBOT CAR - Arduino, Ultrasonic Distance Sensors and LEGO's
* eBeggar Wednesday - ELON MUSK did SOMETHING
* Silicon Dojo #4 - Pitching 1Million Cups Asheville
* Dojo Derby Vehicle Mark 4 - LEGO EDITION

Security Now

* The Maker's Schedule - VirusTotal, Daniel Bernstein sues the NSA, Win 11 might damage encrypted data
* Rowhammer's Nine Lives - TLS-Anvil, Chrome cookies stick around, Atlassian Confluence under attack

Troy Hunt

* Weekly Update 308

Intel Techniques: The Privacy, Security, & OSINT Show

* 274-Firewall Stability Modifications
* 273-Credential Exposure Removal

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Windows sxssrv!BaseSrvActivationContextCacheDuplicateUnicodeString Heap Buffer Overflow
* Windows sxs!CNodeFactory::XMLParser_Element_doc_assembly_assemblyIdentity Heap Buffer Overflow
* Gas Agency Management 2022 SQL Injection / XSS / Shell Upload
* Readymade Job Portal Script SQL Injection
* Fiberhome AN5506-02-B Cross Site Scripting
* Intelbras ATA 200 Cross Site Scripting
* Webmin Package Updates Command Injection
* Zimbra zmslapd Privilege Escalation
* AirSpot 5410 0.3.4.1-4 Remote Command Injection
* Sophos XG115w Firewall 17.0.10 MR-10 Authentication Bypass
* Feehi CMS 2.1.1 Cross Site Scripting
* Matrimonial PHP Script 1.0 SQL Injection
* PAN-OS 10.0 Remote Code Execution
* Backdoor.Win32.Guptachar.20 MVID-2022-0631 Insecure Credential Storage
* Prestashop Blockwishlist 2.1.0 SQL Injection
* Thingsboard 3.3.1 Cross Site Scripting
* ManageEngine ADAudit Plus Path Traversal / XML Injection
* WordPress Duplicator 1.4.7.1 Backup Disclosure
* Nortek Linear eMerge E3-Series Account Takeover
* Nortek Linear eMerge E3-Series Command Injection
* Nortek Linear eMerge E3-Series Credential Disclosure
* Zimbra UnRAR Path Traversal
* WordPress Ecwid Ecommerce Shopping Cart 6.10.23 Cross Site Request Forgery
* Backdoor.Win32.Bushtrommel.122 MVID-2022-0630 Remote Command Execution
* Backdoor.Win32.Bushtrommel.122 MVID-2022-0629 Authentication Bypass

CXSecurity

* PAN-OS 10.0 Remote Code Execution
* Webmin Package Updates Command Injection
* Zoho Password Manager Pro XML-RPC Java Deserialization
* Zimbra UnRAR Path Traversal
* VMware Workspace ONE Access Privilege Escalation
* NanoCMS 0.4 Remote Code Execution
* MobileIron Log4Shell Remote Command Execution

Proof of Concept (PoC) & Exploits

Exploit Database

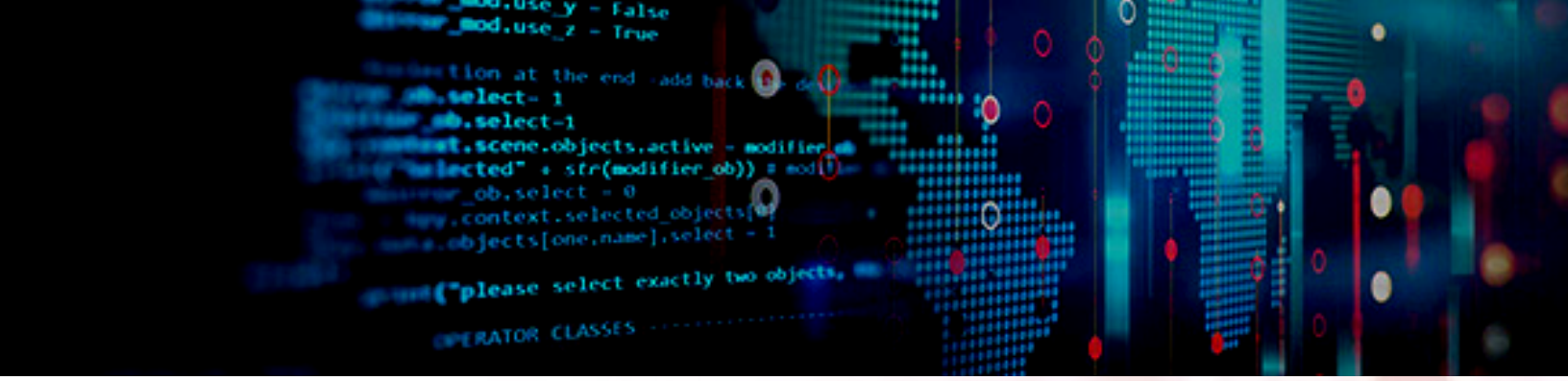
* [remote] PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)
* [webapps] ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)
* [webapps] Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Prestashop blockwishlist module 2.1.0 - SQLi
* [remote] uftpd 2.10 - Directory Traversal (Authenticated)
* [remote] Easy Chat Server 3.1 - Remote Stack Buffer Overflow (SEH)
* [webapps] Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)
* [webapps] NanoCMS v0.4 - Remote Code Execution (RCE) (Authenticated)
* [remote] Omnia MPX 1.5.0+r1 - Path Traversal
* [webapps] mPDF 7.0 - Local File Inclusion
* [webapps] CuteEditor for PHP 6.6 - Directory Traversal
* [webapps] WordPress Plugin Duplicator 1.4.7 - Information Disclosure
* [webapps] WordPress Plugin Duplicator 1.4.6 - Unauthenticated Backup Download
* [webapps] Wavlink WN530HG4 - Password Disclosure
* [webapps] Wavlink WN533A8 - Password Disclosure
* [webapps] Wavlink WN533A8 - Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin WP-UserOnline 2.87.6 - Stored Cross-Site Scripting (XSS)
* [remote] Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) - Remote Code Execution
* [webapps] Carel pCOWeb HVAC BACnet Gateway 2.1.0 - Directory Traversal
* [local] Asus GameSDK v1.0.0.4 - 'GameSDK.exe' Unquoted Service Path
* [webapps] Dingtian-DT-R002 3.1.276A - Authentication Bypass
* [remote] rpc.py 0.6.0 - Remote Code Execution (RCE)
* [webapps] Geonetwork 4.2.0 - XML External Entity (XXE)
* [webapps] WordPress Plugin Visual Slide Box Builder 3.2.9 - SQLi

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*

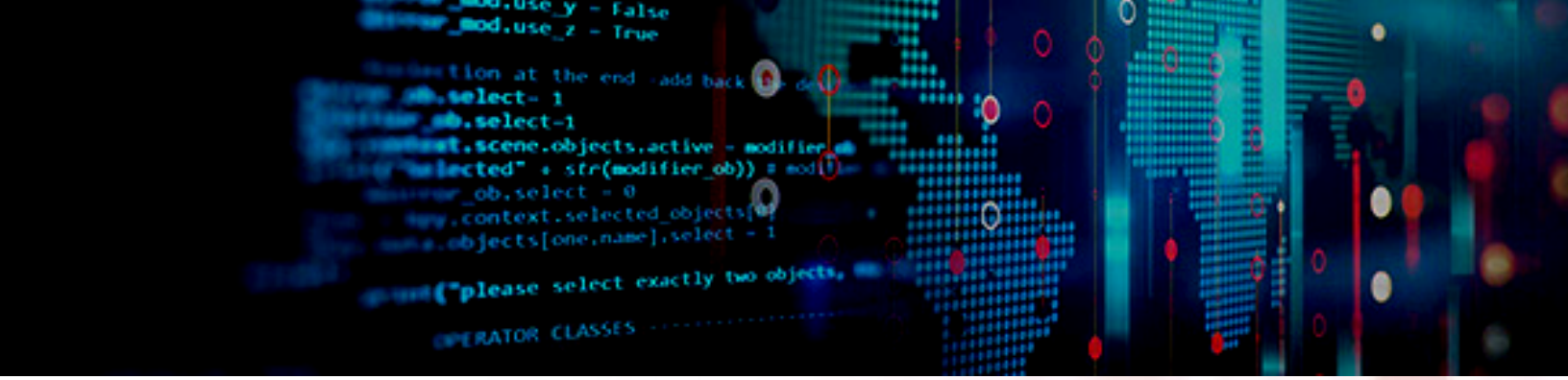
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://distanbun.jatengprov.go.id/fake.php
https://distanbun.jatengprov.go.id/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://minpro.gob.ar/vz.txt
https://minpro.gob.ar/vz.txt notified by aDriv4
https://igf.gouv.ht/1.php
https://igf.gouv.ht/1.php notified by -1
http://arkhangai.gov.mn
http://arkhangai.gov.mn notified by MrNyx
http://nknda.gov.gh
http://nknda.gov.gh notified by 1877
http://www.sajorakhea.go.th/index.php
http://www.sajorakhea.go.th/index.php notified by ./Niz4r
http://www.tungluang.go.th/index.php
http://www.tungluang.go.th/index.php notified by ./Niz4r
http://www.yangngam.go.th/index.php
http://www.yangngam.go.th/index.php notified by ./Niz4r
https://www.secpt.go.th
https://www.secpt.go.th notified by ./Niz4r
http://pta-semarang.go.id/xid.txt
http://pta-semarang.go.id/xid.txt notified by Mister_XID
http://www.bankruatcity.go.th/index.php
http://www.bankruatcity.go.th/index.php notified by ./Niz4r
http://pa-masohi.go.id/templates/beez3/read.txt
http://pa-masohi.go.id/templates/beez3/read.txt notified by Mr.L3RB1
http://pa-ambon.go.id/templates/beez3/read.txt
http://pa-ambon.go.id/templates/beez3/read.txt notified by Mr.L3RB1
http://pa-namlea.go.id/templates/beez3/read.txt
http://pa-namlea.go.id/templates/beez3/read.txt notified by Mr.L3RB1
http://kotajalur.kuansing.go.id/readme.htm
http://kotajalur.kuansing.go.id/readme.htm notified by Mr.L3RB1
http://lakon-ku.kotajalur.kuansing.go.id/readme.htm
http://lakon-ku.kotajalur.kuansing.go.id/readme.htm notified by Mr.L3RB1
http://www.jdih.kuansing.go.id/readme.htm
http://www.jdih.kuansing.go.id/readme.htm notified by Mr.L3RB1



Dark Web News

Darknet Live

International Crypto Exchanges Blocked in Uzbekistan

The websites of international cryptocurrency exchanges have been blocked in Uzbekistan. Binance, Huobi, FTX, and others are among the cryptocurrency exchanges impacted by the action. The National Agency for Perspective Projects (NAPP) announced that international cryptocurrency exchanges were blocked because of licensing or data storage issues. Only one cryptocurrency exchange, UZNEX, has registered with the relevant authorities in the country. Additionally, the international exchanges were storing the data of Uzbekistan citizens outside of the country. "[The exchanges] were asking for personal data from citizens without taking account of the requirements for hosting servers on the territory of the Republic of Uzbekistan in the manner set out by law,” NAPP explained. Eurasianet speculated about the reason for the ban: "The crackdown could be linked to fears about the risks of cryptocurrency being abused as a tool for sanctions dodging by Russians.” lol abused In April 2022, Uzbekistan President Shavkat Mirziyoyev signed a decree "regulating cryptocurrencies and assigned the National Agency for Perspective Projects the role of the industry's watchdog.” The agency explained that after January 2023, citizens of Uzbekistan would only be permitted to use licensed cryptocurrency exchanges. "From the moment [the decree was published], we did not block foreign platforms, as we understand that our citizens have funds on these platforms. But this measure did not mean that citizens can safely trade on foreign platforms until January 1, 2023. There has already been a ban on this since 2019,” the NAPP specified. Predictable! (via darknetlive.com at https://darknetlive.com/post/international-crypto-exchanges-blocked-in-uzbekistan/)

Washington Doctor Pleads Guilty in Murder-for-Hire Case

The Spokane, Washington, doctor accused of hiring a hitman to injure his wife pleaded guilty in federal court. Dr. Ronald Ilg, a neonatal specialist in Washington, tried to hire hitmen on the darkweb to kidnap and injure his estranged wife and a former coworker. "Your honor, I was a broken man,” Ilg said in court Wednesday. "I was broken and I contacted different websites on the dark web to not only injure one of my partners, but also kidnap my wife.” Dr. Ronald Ilg According to court documents, Ilg found a murder-for-hire site on the darkweb and asked for someone to beat and injure a former coworker. The coworker complained about Ilg at a medical practice in Washington, resulting in Ilg losing his job. A Screenshot of DARK WEBSITE #1 | FBI Using the handle "scar215,” Ilg sent a request to the first murder-for-hire site: "The target should be given a significant beating that is obvious. It should injure both hands significantly or break the hands. I tried to attach a pic but it wouldn't load.” A Screenshot of DARK WEBSITE #2 | FBI Later, in a conversation with the operator of another murder-for-hire site, Scar215 spelled out an elaborate plan to stop his wife's divorce from proceeding. Many of the messages are available in the previous Darknetlive article about the case. One of the first messages sent to the second murder-for-hire site is as follows: "I need a rush job for next week. I need the target kidnapped for five to seven days. While being held she is given at least daily doses of heroin. She is also strongly persuaded to do a few things within two weeks.” stop ALL Court proceedings; return to your husband and the chaos you created; tell absolutely no one about this; the team

should plant heroin and used needles with her DNA inside. After about seven days, she is returned to her home. "The target destroyed two families and walked away as if she did nothing. I want the target kidnapped for 7 days. While being held, she will be given injections of heroin at least two times per day. She will be taught to do it herself, and pics and videos of her doing on her own should be collected. Also, while being held, all means necessary will be done to get the following goals with in 2 weeks of her release.” "First, cancel all court proceedings immediately. Second, return to the chaos she left with her husband and the 3rd party she invited into the house, and third, she will tell absolutely no one about her kidnapping and goals. She should be told that her families health, including her father and her kids, depend on her completing these rules. It would be unfortunate if her older boy became addicted to heroin. Or her dad be severely beaten or her dog be slaughtered. Any and all persuasion should be used. This needs to be done in two weeks.” In April 2020, BBC journalists forwarded copies of Ilg's messages to the Federal Bureau of Investigation. Some messages included the Bitcoin transaction hash of Ilg's payments to escrow sites. FBI investigators learned that the payments came from a Coinbase wallet. Records from Coinbase linked Ilg to the transactions and account. The transactions referenced by Dr. Ilg originated from Coinbase. After initially pleading not guilty to the charges, Ilg agreed with the prosecution. Ilg would plead guilty to two counts of making threats using interstate commerce in exchange for a sentence of between five and eight years in prison. In court, the judge said he "agreed with the government that a fair and just sentencing would be between five years and eight years [in prison].” The judge also scheduled Ilg's sentencing hearing for November 8, 2022. Ilg will remain in jail while waiting to be sentenced. Interesting picture of Ilg on this site where he does not look crazy. (via darknetlive.com at https://darknetlive.com/post/washington-man-pleads-guilty-in-murder-for-hire-case/)

Two Charged for Buying 5,200 Alprazolam Pills on the Darkweb

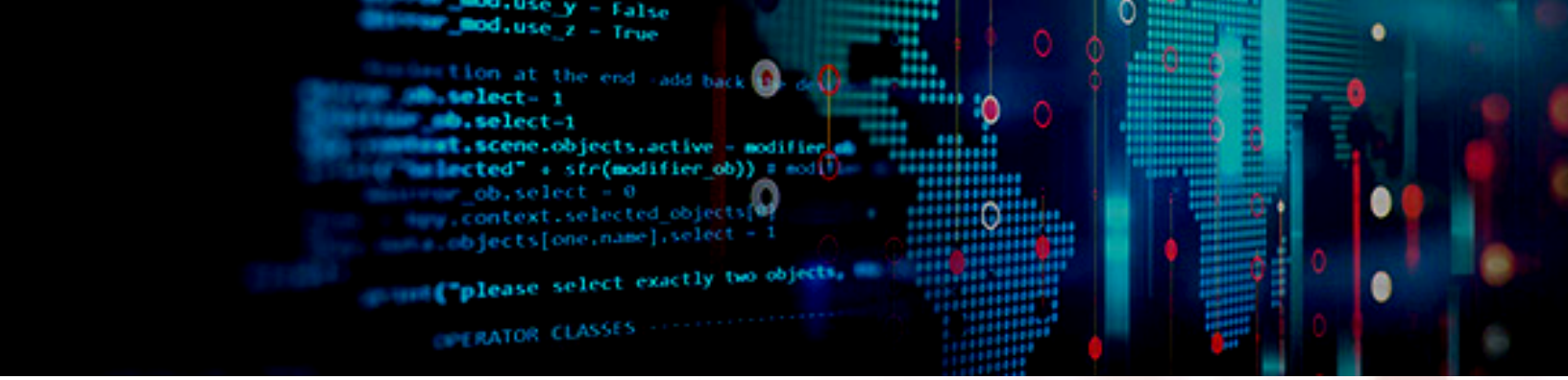
According to the Salzburg Public Prosecutor's Office, a 21-year-old allegedly ordered 5,200 alprazolam pills from vendors on the darkweb. 0.25 mg alprazolam pill The Prosecutor's Office filed a criminal complaint accusing two 21-year-olds from Flachgau of drug trafficking. The first defendant allegedly ordered 5,200 alprazolam pills from the darkweb between the summer of 2019 and the end of 2021. The defendant had packages of pills shipped to his residence or the address of the other 21-year-old. The first defendant sold only a "small number of the pills.” The complaint accuses the defendants of jointly growing 74 cannabis plants between 2018 and 2021. They sold one kilogram of marijuana at the price of ten euros per gram (presumably totaling 10,000 euros or 10,354 US dollars. (via darknetlive.com at https://darknetlive.com/post/two-austrians-charged-for-ordering-5200-xanax-pills/)

Police in the UK Discover Link Between the Darkweb and Crime

Investigators with the Northamptonshire Police in the U.K. have discovered a link between the darkweb and criminal activity, including drug trafficking. The Force's top men are on the case. The Northamptonshire Police published a press release highlighting the Force's "hi-tech war on drug dealers lurking on the so-called Dark Web.” "The Force now uses specialist software to allow detectives to access the Dark Web where criminals can interact using private networks that do not reveal key information such as location.” Northamptonshire Police investigators appear to be operating or investigating a darkweb market for firearms "However, digital media investigators (DMI) now have the Dark Web very clearly in their sights when it comes to detecting online criminality, including drug dealing.” Detective Sergeant Jason Cullum, one of the Force's senior DMIs, said: "During our latest week of action focusing on drug harm, we thought it would be useful to shine a light on the work we are doing in relation to tackling criminality on the Dark Web. We have invested in new software and more officers are receiving specialist training which will enable then to tackle criminals who wrongly think they are operating beyond the reach of the law. Northamptonshire is in the early stages of this journey, but our approach is becoming ever more sophisticated.” The market appears to be called Venus Market. Is that a Glock 17 for $279? It is so over for criminals. Nothing gets past these guys. Detectives investigate "Dark Web” links to drugs and other crime | northants.police.uk (Article is behind a Cloudflare captcha.) (via darknetlive.com at

https://darknetlive.com/post/very-serious-uk-police-investigate-link-to-drugs/)

Dark Web Link



Trend Micro Anti-Malware Blog

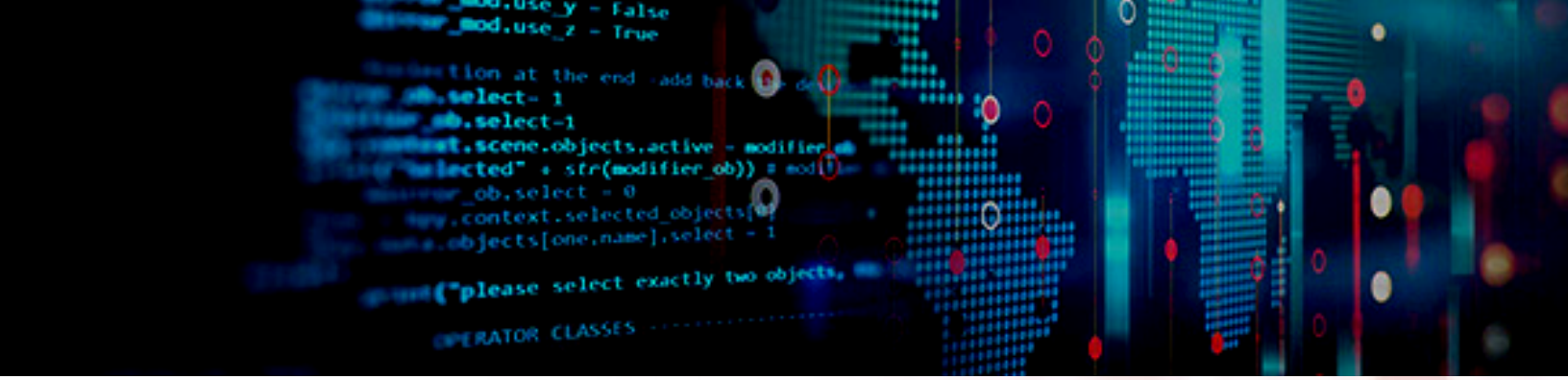
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* 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
* 3 Mistakes Companies Make in Their Detection and Response Programs
* Rapid7 Discovered Vulnerabilities in Cisco ASA, ASDM, and FirePOWER Services Software
* OCSF: Working Together to Standardize Data
* Navigating the Evolving Patchwork of Incident Reporting Requirements
* Patch Tuesday - August 2022
* 6 Reasons Managed Detection and Response Is Hitting Its Stride
* How One Engineer Upskilled Into a Salesforce Engineering Role at Rapid7
* No Damsels in Distress: How Media and Entertainment Companies Can Secure Data and Content
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Update for Multiple Products
* #StopRansomware: Zeppelin Ransomware
* Palo Alto Networks Releases Security Update for PAN-OS
* CISA Releases Cybersecurity Toolkit to Protect U.S. Elections
* Microsoft Releases August 2022 Security Updates
* Adobe Releases Security Updates for Multiple Products
* VMware Releases Security Updates
* AA22-223A: #StopRansomware: Zeppelin Ransomware
* AA22-216A: 2021 Top Malware Strains
* Vulnerability Summary for the Week of August 1, 2022
* Vulnerability Summary for the Week of July 25, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Gentoo Linux Security Advisory 202208-16

Gentoo Linux Security Advisory 202208-16 - A vulnerability in faac could result in denial of service. Versions less than 1.30 are affected.

Gentoo Linux Security Advisory 202208-18

Gentoo Linux Security Advisory 202208-18 - A vulnerability in Motion allows a remote attacker to cause denial of service. Versions less than 4.3.2 are affected.

Gentoo Linux Security Advisory 202208-19

Gentoo Linux Security Advisory 202208-19 - An open redirect vulnerability has been discovered in aiohttp. Versions less than 3.7.4 are affected.

Gentoo Linux Security Advisory 202208-15

Gentoo Linux Security Advisory 202208-15 - Multiple vulnerabilities have been discovered in isync, the worst of which could result in arbitrary code execution. Versions less than 1.4.4 are affected.

Gentoo Linux Security Advisory 202208-17

Gentoo Linux Security Advisory 202208-17 - Multiple vulnerabilities have been found in Nextcloud, the worst of which could result in denial of service. Versions less than 23.0.4 are affected.

Ubuntu Security Notice USN-5567-1

Ubuntu Security Notice 5567-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5566-1

Ubuntu Security Notice 5566-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5563-1

Ubuntu Security Notice 5563-1 - It was discovered that http-parser incorrectly handled certain requests. An attacker could possibly use this issue to bypass security controls or gain unauthorized access to sensitive data.

Red Hat Security Advisory 2022-6040-01

Red Hat Security Advisory 2022-6040-01 - Version 1.24.0 of the OpenShift Serverless Operator is supported on Red Hat OpenShift Container Platform versions 4.6, 4.7, 4.8, 4.9, 4.10, and 4.11. This release includes security and bug fixes, and enhancements. Issues addressed include bypass and denial of service vulnerabilities.

Red Hat Security Advisory 2022-6042-01

Red Hat Security Advisory 2022-6042-01 - Red Hat OpenShift Serverless Client kn 1.24.0 provides a CLI to interact with Red Hat OpenShift Serverless 1.24.0. The kn CLI is delivered as an RPM package for installation on RHEL platforms, and as binaries for non-Linux platforms. Issues addressed include bypass and denial of service vulnerabilities.

Red Hat Security Advisory 2022-6043-01

Red Hat Security Advisory 2022-6043-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 6.0.108 and .NET Runtime 6.0.8.

Ubuntu Security Notice USN-5565-1

Ubuntu Security Notice 5565-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5564-1

Ubuntu Security Notice 5564-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5562-1

Ubuntu Security Notice 5562-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5559-1

Ubuntu Security Notice 5559-1 - It was discovered that Moment.js incorrectly handled certain input paths. An attacker could possibly use this issue to cause a loss of integrity by changing the correct path to one of their choice. It was discovered that Moment.js incorrectly handled certain input. An attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5561-1

Ubuntu Security Notice 5561-1 - It was discovered that GNOME Web incorrectly filtered certain strings. A remote attacker could use this issue to perform cross-site scripting attacks. This issue only affected Ubuntu 20.04 LTS. It was discovered that GNOME Web incorrectly handled certain long page titles. A remote attacker could use this issue to cause GNOME Web to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-5069-01

Red Hat Security Advisory 2022-5069-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.11.0. Issues addressed include code execution, cross site scripting, denial of service, information leakage, and traversal vulnerabilities.

Ubuntu Security Notice USN-5560-2

Ubuntu Security Notice 5560-2 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5560-1

Ubuntu Security Notice 5560-1 - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code. It was discovered that the netfilter subsystem of the Linux kernel did not prevent one nft object from referencing an nft set in another nft table, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or

execute arbitrary code.

Red Hat Security Advisory 2022-6038-01

Red Hat Security Advisory 2022-6038-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

Red Hat Security Advisory 2022-5068-01

Red Hat Security Advisory 2022-5068-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6037-01

Red Hat Security Advisory 2022-6037-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 3.1.422 and .NET Runtime 3.1.28.

Red Hat Security Advisory 2022-5070-01

Red Hat Security Advisory 2022-5070-01 - 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 4.11.0. Issues addressed include denial of service, out of bounds read, and traversal vulnerabilities.

Ubuntu Security Notice USN-5558-1

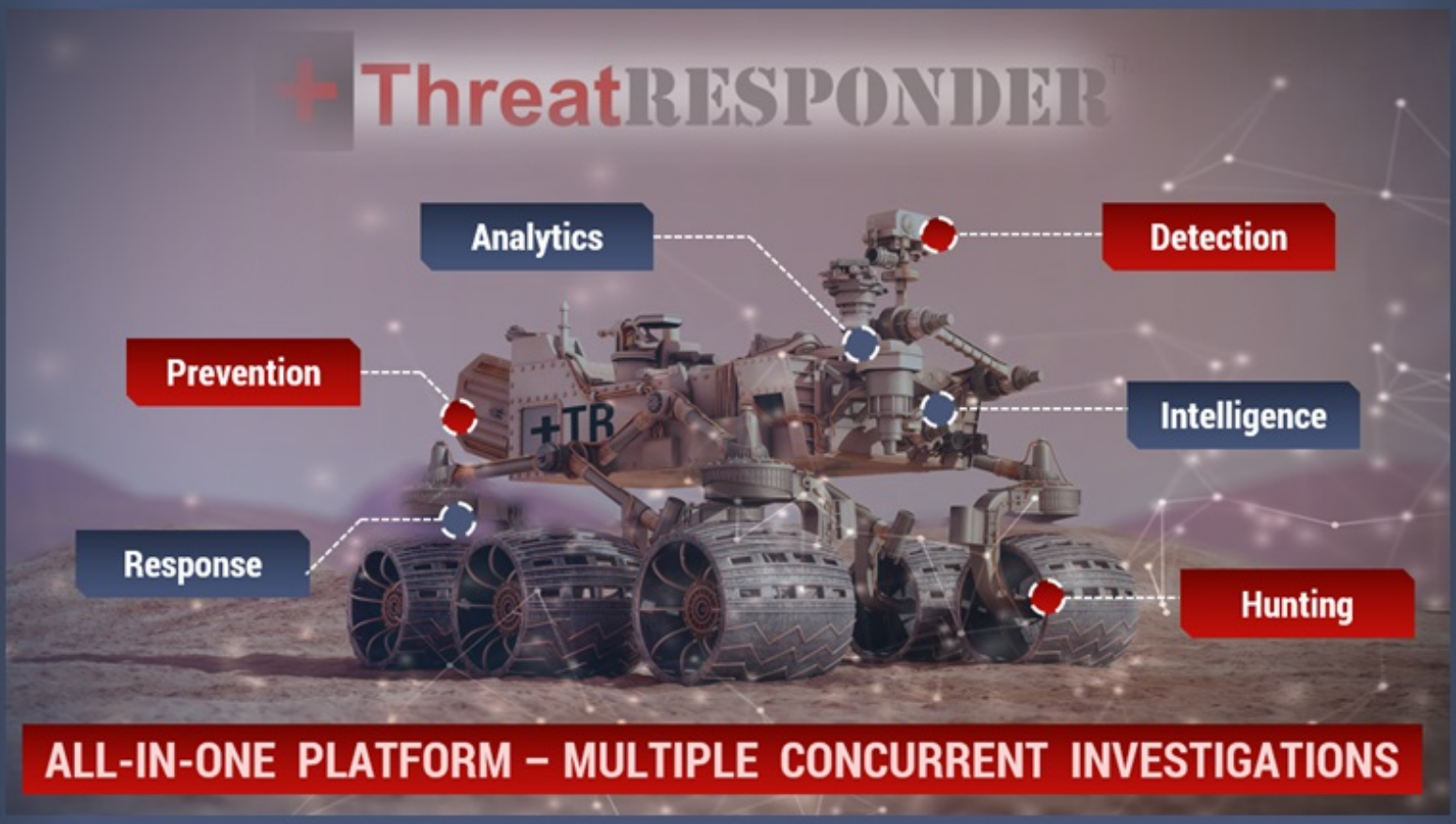
Ubuntu Security Notice 5558-1 - Zhao Liang discovered that libcdio was not properly performing memory management operations when processing ISO files, which could result in a heap buffer overflow or in a NULL pointer dereference. If a user or automated system were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



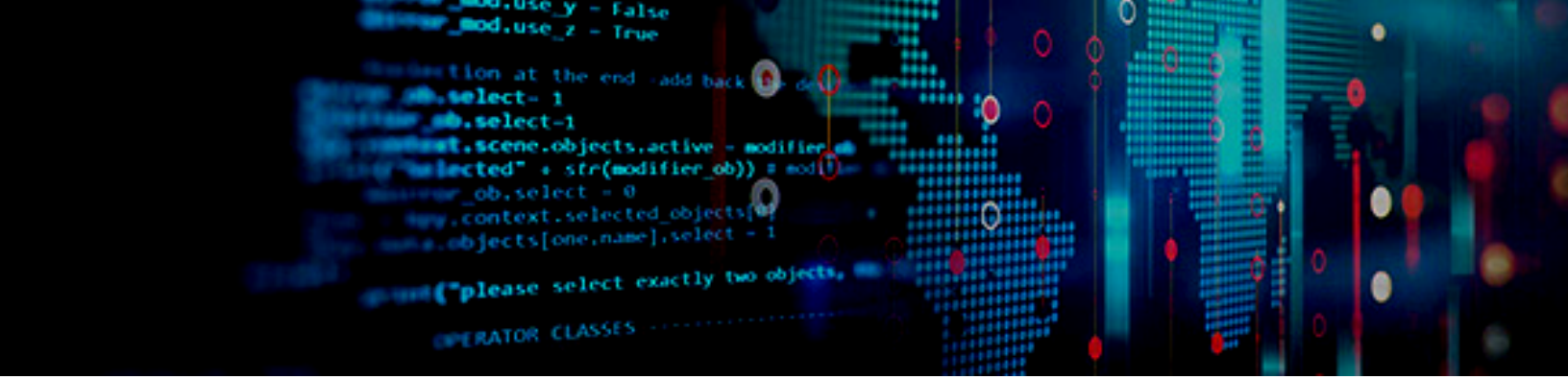
The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

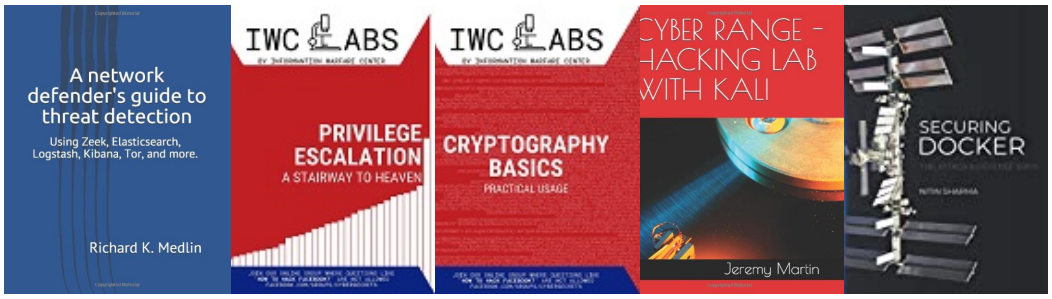


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP