Aug-22-22

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 22, 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

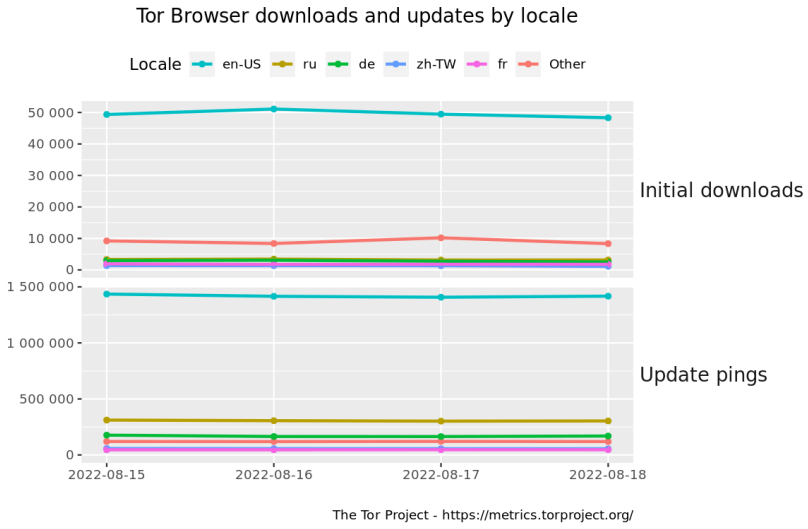
Internet Storm Center Infocon Status

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

* Sudden Crypto Drop Sends Bitcoin To Three Week Low
* Apple Security Flaw Actively Exploited By Hackers To Fully Control Devices
* Two Years On, Apple iOS VPNs Still Leak IP Addresses
* About That Draft Law Banning Uncle Sam Buying Insecure Software
* APT Lazarus Targets Engineers With macOS Malware
* Update Chrome Now To Patch Actively Exploited Zero Day
* Hacker Tournament Brings Together World's Best In Las Vegas
* Ring Patched An Android Bug That Could Have Exposed Video Footage
* Google Blocks Third Record Breaking DDoS Attack In As Many Months
* Janet Jackson Music Video Declared A Cybersecurity Exploit
* How A Third Party SMS Service Was Used To Take Over Signal Accounts
* Russian Military Uses Chinese Drones And Bots In Combat
* Vulnerability Wholesaler Cuts Disclosure Times Over Poor Quality Patches
* Mozilla Finds 18 Of 25 Popular Reproductive Health Apps Leak Data
* SEC Says Brokerage Accounts Hijacked For $1.3m Scam
* Users Of Zoom On Macs Told To Update App As Company Issues Security Fix
* Lawmakers Accuse DHS Watchdog Of Obstruction In Probe Of Secret Service Texts
* U.K. Water Supplier Hit With Clop Ransomware Attack
* Xiaomi Phone Bug Allowed Payment Forgery
* 1,900 Signal Users Exposed: Twilio Attacker Explicitly Looked For Certain Numbers
* Microsoft Employees Exposed Own Company's Internal Logins
* Google Wants To Make Linux Kernel Flaws Harder To Exploit
* Hacker Conference DEF CON Bans Pro Trump Outlet OAN
* This String Of Emojis Is Actually Malware
* Indian Military Puts Quantum Key Distribution On The Line

Krebs on Security

* PayPal Phishing Scam Uses Invoices Sent Via PayPal
* When Efforts to Contain a Data Breach Backfire
* 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

Dark Reading

* Mimecast: Mitigating Risk Across a Complex Threat Landscape
* Banyan Recommends Phased Approach When Introducing Zero Trust
* DeepSurface Adds Risk-Based Approach to Vulnerability Management
* The HEAT Is On, Says Menlo Security
* PIXM: Stopping Targeted Phishing Attacks With 'Computer Vision'
* Intel Adds New Circuit to Chips to Ward Off Motherboard Exploits
* NIST Weighs in on AI Risk
* Patch Now: 2 Apple Zero-Days Exploited in Wild
* Cybersecurity Solutions Must Evolve, Says Netography CEO
* State-Sponsored APTs Dangle Job Opps to Lure In Spy Victims
* BlackByte Ransomware Gang Returns With Twitter Presence, Tiered Pricing
* Cyber Resiliency Isn't Just About Technology, It's About People
* Easing the Cyber-Skills Crisis With Staff Augmentation
* China's APT41 Embraces Baffling Approach for Dropping Cobalt Strike Payload
* Mac Attack: North Korea's Lazarus APT Targets Apple's M1 Chip
* 5 Russia-Linked Groups Target Ukraine in Cyberwar
* Which Security Bugs Will Be Exploited? Researchers Create an ML Model to Find Out
* Summertime Blues: TA558 Ramps Up Attacks on Hospitality, Travel Sectors
* How to Upskill Tech Staff to Meet Cybersecurity Needs
* OpenSSF Announces 13 New Members Committed to Strengthening the Security of the Open Source Software

The Hacker News

* Hackers Stole Crypto from Bitcoin ATMs by Exploiting Zero-Day Vulnerability
* New Grandoreiro Banking Malware Campaign Targeting Spanish Manufacturers
* Become a Cybersecurity Expert with 18 New Online Courses @ 98% OFF
* CISA Adds 7 New Actively Exploited Vulnerabilities to Catalog
* DoNot Team Hackers Updated its Malware Toolkit with Improved Capabilities
* Cybercrime Group TA558 Targeting Hospitality, Hotel, and Travel Organizations
* Google Cloud Blocks Record DDoS attack of 46 Million Requests Per Second
* New Amazon Ring Vulnerability Could Have Exposed All Your Camera Recordings
* Researchers Detail Evasive DarkTortilla Crypter Used to Deliver Malware
* China-backed APT41 Hackers Targeted 13 Organisations Worldwide Last Year
* Hackers Using Bumblebee Loader to Compromise Active Directory Services
* Penetration Testing or Vulnerability Scanning? What's the Difference?
* Apple Releases Security Updates to Patch Two New Zero-Day Vulnerabilities
* Cybercriminals Developing BugDrop Malware to Bypass Android Security Features
* New Google Chrome Zero-Day Vulnerability Being Exploited in the Wild

Security Week

* FBI Warns of Proxies and Configurations Used in Credential Stuffing Attacks
* Ring Camera Recordings Exposed Due to Vulnerability in Android App
* China's Winnti Group Hacked at Least 13 Organizations in 2021: Security Firm
* Ransomware Group Threatens to Leak Data Stolen From Security Firm Entrust
* Google Blocks Record-Setting DDoS Attack That Peaked at 46 Million RPS
* Cybersecurity M&A Roundup for August 1-15, 2022
* Chinese Cyberspy Group 'RedAlpha' Targeting Governments, Humanitarian Entities
* SAP Vulnerability Exploited in Attacks After Details Disclosed at Hacker Conferences
* TXOne Networks Scores $70M Series B Investment
* Universal ZTNA is Fundamental to Your Zero Trust Strategy
* Estonia Blocks Cyberattacks Claimed by Russian Hackers
* Russian Use of Cyberweapons in Ukraine and the Growing Threat to the West
* Cisco Squashes High-Severity Bug in Web Protection Solution
* North Korean Hackers Use Fake Job Offers to Deliver New macOS Malware
* Evasive 'DarkTortilla' Crypter Delivers RATs, Targeted Malware
* SynSaber Raises $13 Million for OT Asset and Network Monitoring Solution
* Russian Man Extradited to US for Laundering Ryuk Ransomware Money
* DigitalOcean Discloses Impact From Recent Mailchimp Cyberattack
* Apple Patches New macOS, iOS Zero-Days
* Vulnerability Broker Applies Pressure on Software Vendors Shipping Faulty, Incomplete Patches
* 81% of Malware Seen on USB Drives in Industrial Facilities Can Disrupt ICS: Honeywell
* SEC Charges 18 Over Scheme Involving Hacked Brokerage Accounts
* Iranian Group Targeting Israeli Shipping and Other Key Sectors
* Quarterly Security Patches Released for Splunk Enterprise
* The Future of Endpoint Management
* Security Analysis Leads to Discovery of Vulnerabilities in 18 Electron Applications

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [Whoa] Ransomware Strains Almost Double in Six Months from 5,400 to 10,666
* Piggybacking: Social Engineering for Physical Access
* One-Third of Organizations Experience Ransomware Attacks At Least Weekly
* Impersonation Phishing Attacks Increase as Credentials Take the Lead as the Primary Target
* Hybrid Vishing Attacks Increase 625% in Q2
* Organizations Holding Cyber Insurance Policies May Get Stuck with the Bill in a Phishing Loss
* Social Engineering for Espionage and Influence
* More Super Targeted Spear Phishing Ahead
* Children of Conti go Phishing
* CyberheistNews Vol 12 #33 [Eye Opener] Recent Cisco Hack by Ransomware Group Started Because of a Phi

ISC2.org Blog

* LATEST CYBERTHREATS AND ADVISORIES - AUGUST 19, 2022
* Black Hat USA 2022: Are Cybersecurity Tool Standards on the Way?
* New U.S. Legislation Introduced to Help Small Business Provide Cybersecurity Training
* Effective Security Using Zero Trust Architecture
* LATEST CYBERTHREATS AND ADVISORIES - AUGUST 12, 2022

HackRead

* Critical Amazon Ring Vulnerability Could Expose Camera Recordings
* Google Fended Off Largest Ever Layer 7 DDoS Attack
* Cybersecurity | How to Become a Cybersecurity Expert
* 35 malicious apps found on Google Play Store, installed by 2m users
* White Hat Hacker at DefCon Jaikbreaks Tractor to Play Doom
* Windows, Linux and macOS Users Targeted by Chinese Iron Tiger APT Group
* Cybersecurity Has Never Been More Unstable Than It Is Now

Koddos

* Critical Amazon Ring Vulnerability Could Expose Camera Recordings
* Google Fended Off Largest Ever Layer 7 DDoS Attack
* Cybersecurity | How to Become a Cybersecurity Expert
* 35 malicious apps found on Google Play Store, installed by 2m users
* White Hat Hacker at DefCon Jaikbreaks Tractor to Play Doom
* Windows, Linux and macOS Users Targeted by Chinese Iron Tiger APT Group
* Cybersecurity Has Never Been More Unstable Than It Is Now

Naked Security

* Apple patches double zero-day in browser and kernel - update now!
* S3 Ep96: Zoom 0-day, AEPIC leak, Conti reward, healthcare security [Audio + Text]
* Chrome browser gets 11 security fixes with 1 zero-day - update now!
* US offers reward "up to $10 million" for information about the Conti gang
* Zoom for Mac patches critical bug - update now!
* 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

Threat Post

* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year
* APT Lazarus Targets Engineers with macOS Malware
* U.K. Water Supplier Hit with Clop Ransomware Attack
* Xiaomi Phone Bug Allowed Payment Forgery
* Black Hat and DEF CON Roundup
* 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

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

* Complex cloud architecture is finally causing budgetary pain
* What is an API? Application programming interfaces explained
* Deno tees up easy NPM imports, speed boosts
* BrandPost: Run Databricks Queries in Up to 76% Less Time and Reduce Costs with AmazonÂ® R5d Instan
* Microsoft Dev Box cloud-based workstations enter public preview
* What software developers should know about design: An interview with Soleio
* Lift and shift Windows applications to containers
* Kubescape boosts Kubernetes scanning capabilities
* Microsoft .NET 6 bundled with Ubuntu Linux
* 7 YAML gotchas to avoid-and how to avoid them

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.

* CTFZone 2022
* HITB SECCONF CTF 2022
* MapleCTF 2022
* Balsn CTF 2022
* CakeCTF 2022
* [POSTPONED] CyberSpace CTF
* Winja CTF | Nullcon Goa 2022
* CSAW CTF Qualification Round 2022
* VolgaCTF 2022 Final
* 0CTF/TCTF 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

* TOR Virtual Network Tunneling Tool 0.4.7.10
* 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

Kali Linux Tutorials

* Cirrusgo : A Fast Tool To Scan SAAS, PAAS App Written In Go
* Kage : Graphical User Interface For Metasploit Meterpreter And Session Handler
* SaaS security: Achieving a clean IAM System Audit
* PR-DNSd : Passive-Recursive DNS Daemon
* SilentHound : Quietly Enumerate An Active Directory Domain Via LDAP Parsing Users, Admins, Groups, Et
* 5 Reasons Why You Should Choose a Career in Cybersecurity
* Maldev-For-Dummies : A Workshop About Malware Development
* TerraformGoat : "Vulnerable By Design" Multi Cloud Deployment Tool
* Pretender : Your MitM Sidekick For Relaying Attacks Featuring DHCPv6 DNS Takeover As Well As mDNS
* Doenerium : Fully Undetected Grabber (Grabs Wallets, Passwords, Cookies, Modifies Discord Client Etc.

GBHackers Analysis

* Researchers Hacked SpaceX Operated Starlink Satellite Using $25 Modchip
* 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!

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown (STAR) | Live Stream
* Introducing the Enterprise Cloud Forensics & Incident Response Poster
* FOR585 Course Animation: Potential Crime Scene iPhone and Android
* FOR585 Course Animation: IMEI vs GSM

Defcon Conference

* DEF CON 30 - ICS Village Interview
* DEF CON 30 - DEF CON X Hak5 collab!
* DEF CON 30 - Silk vs. the NOC
* DEF CON 30 - Voting Machine Village Interview

Hak5

* DEF CON 30: The Wireless Sh*t Show With El Kentaro and D4rkM4tter
* DEF CON 30: A Conversation With The Dark Tangent
* Live Hacking Q&A with Kody Kinzie and Alex Lynd

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* A Robot That Really Understands the Modern World - Silicon Dojo Projects
* eBeggar Wednesday - TRUMP 2024... is looking dreadfully possible...
* LEGO ROBOT CAR - Arduino, Ultrasonic Distance Sensors and LEGO's
* eBeggar Wednesday - ELON MUSK did SOMETHING

Security Now

* TLS Private Key Leakage - BIG patch Tuesday, Facebook E2E encryption, VNC insecurity, Cyotek WebCopy
* The Maker's Schedule - VirusTotal, Daniel Bernstein sues the NSA, Win 11 might damage encrypted data

Troy Hunt

* Weekly Update 309

Intel Techniques: The Privacy, Security, & OSINT Show

* 275-Archived Site Removal & Breaches Galore
* 274-Firewall Stability Modifications

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Transposh WordPress Translation 1.0.8.1 Incorrect Authorization
* FLIR AX8 1.46.16 Traversal / Access Control / Command Injection / XSS
* Chrome content::ServiceWorkerVersion::MaybeTimeoutRequest Heap Use-After-Free
* FLIX AX8 1.46.16 Remote Command Execution
* Advantech iView NetworkServlet Command Injection
* Polar Flow Android 5.7.1 Secret Disclosure
* FreeBSD 13.0 aio_aqueue Kernel Refcount Local Privilege Escalation
* Race Against The Sandbox
* TypeORM 0.3.7 Information Disclosure
* Windows Credential Guard Domain-Joined Device Public Key Privilege Escalation
* Win32.Ransom.BlueSky MVID-2022-0632 Code Execution
* Inout RealEstate 2.1.2 SQL Injection
* Inout SiteSearch 2.0.1 Cross Site Scripting
* Gigaland NFT Marketplace 1.9 Shell Upload / Key Disclosure
* 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

CXSecurity

* FLIX AX8 1.46.16 Remote Command Execution
* Advantech iView NetworkServlet Command Injection
* 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

Proof of Concept (PoC) & Exploits

Exploit Database

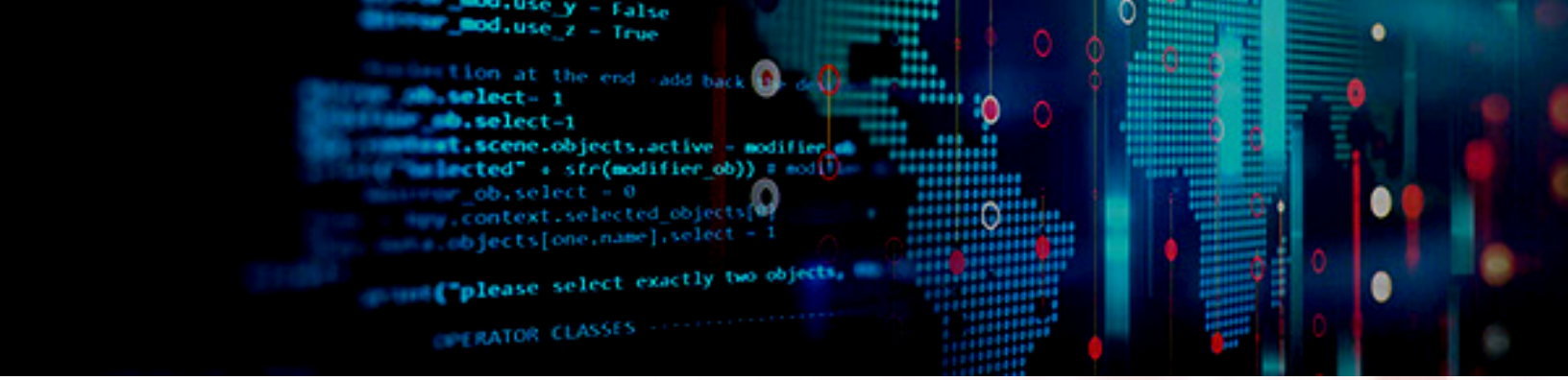
* [remote] PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)
* [webapps] ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)
* [webapps] Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Prestashop 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*

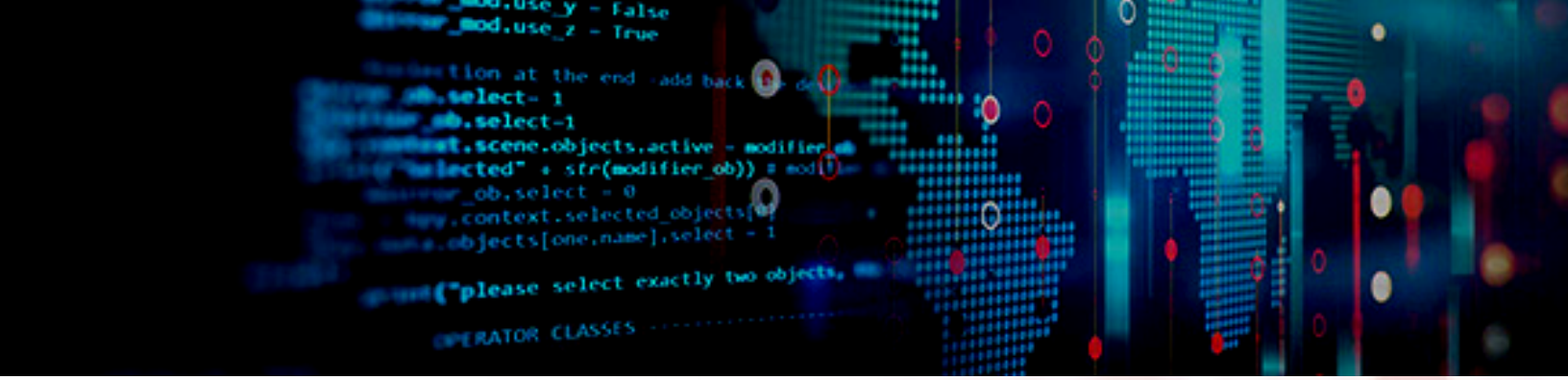
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://sultraprov.go.id/root.html
https://sultraprov.go.id/root.html notified by Black_X12
https://cri.nfe.go.th
https://cri.nfe.go.th notified by 1877
http://www.pis.gov.np/0.htm
http://www.pis.gov.np/0.htm notified by ./Cyber00t
https://cedp.gov.bd/vz.txt
https://cedp.gov.bd/vz.txt notified by aDriv4
http://www.commune-sakieteddaier.gov.tn
http://www.commune-sakieteddaier.gov.tn notified by Mf4 Team
https://jgdm.gov.za/and.php
https://jgdm.gov.za/and.php notified by mr.anderson
https://hospitalcentral.gob.mx/dz.php
https://hospitalcentral.gob.mx/dz.php notified by djebbaranon
https://www.caska.gov.mk/vz.txt
https://www.caska.gov.mk/vz.txt notified by aDriv4
http://cee.am.gov.br/vz.txt
http://cee.am.gov.br/vz.txt notified by aDriv4
http://coggeshall-pc.gov.uk/indonesia.php
http://coggeshall-pc.gov.uk/indonesia.php notified by /Rayzky_
http://kelurahanpartim.balangankab.go.id/root.txt
http://kelurahanpartim.balangankab.go.id/root.txt notified by Black_X12
http://balangankab.go.id/root.txt
http://balangankab.go.id/root.txt notified by Black_X12
http://dishub.balangankab.go.id/root.txt
http://dishub.balangankab.go.id/root.txt notified by Black_X12
http://skm.balangankab.go.id/root.txt
http://skm.balangankab.go.id/root.txt notified by Black_X12
http://www.jdih.balangankab.go.id/root.txt
http://www.jdih.balangankab.go.id/root.txt notified by Black_X12
http://mediacenter.balangankab.go.id/root.txt
http://mediacenter.balangankab.go.id/root.txt notified by Black_X12
http://www.pn-kualatungkal.go.id/readme.html
http://www.pn-kualatungkal.go.id/readme.html notified by ./Fake Root



Dark Web News

Darknet Live

Robinhood Crypto Fined $30 Million for AML Violations in NY

In August 2022, New York State's Department of Financial Services ("DFS”) announced that Robinhood Crypto agreed to pay a $30 million fine for failing to comply with anti-money laundering and cybersecurity regulations. "As its business grew, Robinhood Crypto failed to invest the proper resources and attention to develop and maintain a culture of compliance—a failure that resulted in significant violations of the Department's anti-money laundering and cybersecurity regulations,” Superintendent of Financial Services Adrienne A. Harris said. "All virtual currency companies licensed in New York State are subject to the same anti-money laundering, consumer protection, and cybersecurity regulations as traditional financial services companies. DFS will continue to investigate and take action when any licensee violates the law or the Department's regulations, which are critical to protecting consumers and ensuring the safety and soundness of the institutions.” New York's DFS discovered "significant” violations of the Department's Virtual Currency Regulation (23 NYCRR Part 200), Money Transmitter Regulation (3 NYCRR Part 417), Transaction Monitoring Regulation (23 NYCRR Part 504), and Cybersecurity Regulation (23 NYCRR Part 500) during an audit in 2020. Still not fined for freezing certain trades though According to the DFS, Robinhood Crypto monitored transactions manually. The Department that monitored transactions was understaffed. With more than 100,000 transactions a day, there was a backlog of transactions waiting to be reviewed. Robinhood failed to "foster and maintain an adequate culture of compliance.” What…? As a part of the settlement, Robinhood Crypto will need to hire an independent consultant to evaluate the company's compliance with New York's money laundering regulations. DFS SUPERINTENDENT HARRIS ANNOUNCES $30 MILLION PENALTY ON ROBINHOOD CRYPTO FOR SIGNIFICANT ANTI-MONEY LAUNDERING, CYBERSECURITY & CONSUMER PROTECTION VIOLATIONS | archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/robinhood-crypto-to-pay-30-million-fine-for-aml-violations-in-ny/)

Russian Extradited to the US for Laundering $400K in Crypto

A Russian citizen was extradited from the Netherlands to the United States to face charges for allegedly laundering $400,000 in cryptocurrency. According to an announcement from the Department of Justice, Denis Mihaqlovic Dubnikov, 29, appeared in court in Portland, Oregon, on August 17 after being extradited from the Netherlands to the United States. Dubnikov faces charges for his alleged role in the laundering of money earned through the use of ransomware. Specifically, the defendant and his co-conspirators laundered payments from victims of the Ryuk ransomware. Ryuk 'polite' ransom note | Malwarebytes "First identified in August 2018, Ryuk is a type of ransomware software that, when executed on a computer or network, encrypts files and attempts to delete any system backups. Of note, Ryuk can target storage drives contained within or physically connected to a computer, including those accessible remotely via a network connection. Ryuk has been used to target thousands of victims worldwide across various sectors. In October 2020, law enforcement officials identified Ryuk as an imminent and increasing cybercrime threat to hospitals and healthcare providers in the United States.” In July 2019, Dubnikov allegedly laundered

over $400,000 in ransomware payments. Collectively, his co-conspirators laundered more than $70 million in ransom proceeds. Although those involved in the conspiracy used different money laundering methods to avoid detection, funds were often laundered as follows. Victims would pay ransoms in Bitcoin to private wallets controlled by Dubnikov and his co-conspirators. Defendants then split the payments into smaller amounts and moved Bitcoin to numerous private wallets. They also laundered the proceeds in ways we cannot know apparently. Then, the defendants transferred the Bitcoin to an exchange and swapped the Bitcoin for Tether or another cryptocurrency. After turning the Bitcoin into Tether, defendants would send the Tether (or other cryptocurrencies) to different exchanges where they would sell the Tether for fiat currency. They typically traded the Tether for the Chinese Renminbi and moved the fiat to accounts at banks outside of the United States. In court, Dubnikov pleaded not guilty. A jury trial has been scheduled for October 4, 2022. If convicted, Dubnikov faces up to 20 years in federal prison. Alleged Russian Money Launderer Extradited from the Netherlands to U.S. | archive.is, archive.org Indictment pdf (via darknetlive.com at https://darknetlive.com/post/russian-extradited-to-us-for-laundering-400k-in-bitcoin/)

Chainalysis Report: Illicit Crypto Activity (Mostly) Down in 2022

According to a report from the blockchain analytics firm Chainalysis, criminal activity involving cryptocurrency is declining. The report first touched on the declining activity across the market; there is less activity than in 2021 through July. However, criminal activity appears more stable: "illicit volumes are down just 15% year over year, compared to 36% for legitimate volumes.” Monthly cryptocurrency value received by illicit actors in 2022 | Chainalysis Scams _ According to the company, the total revenue for cryptocurrency scams is $1.6 billion, which is 65% lower than in July 2021. Also, the cumulative number of transfers to scams is lower than in four years. 2022's Top scams 2021's Top scams Scam name Vvalue received thru July Scam name Value received thru July JuicyFields.io $273,935,606 Finiko $1,164,115,620 Unique-Exchange.co/PARAIBA.world $267,487,674 Mind.capital $506,240,555 OmegaPro.world $106,449,195 CashFXGroup.com $291,597,650 Chainalysis speculated as to the reasons behind the decline in scam-related activity: "Those numbers suggest that fewer people than ever are falling for cryptocurrency scams. One reason for this could be that with asset prices falling, cryptocurrency scams — which typically present themselves as passive crypto investing opportunities with enormous promised returns — are less enticing to potential victims. We also hypothesize that new, inexperienced users who are more likely to fall for scams are less prevalent in the market now that prices are declining, as opposed to when prices are rising and they're drawn in by hype and the promise of quick returns.” Darknet Markets _ Cumulative monthly value received by darknet markets by year | Chainalysis Chainalysis reported that darknet marketplace revenue is currently 43% lower than the same period in 2021. However, darknet market activity has not been down all year, unlike with scams. In fact, darknet market revenue was tracking higher than in 2021 until April this year. The sudden drop in April is almost certainly due to the shutdown and sanctioning of Hydra Market.

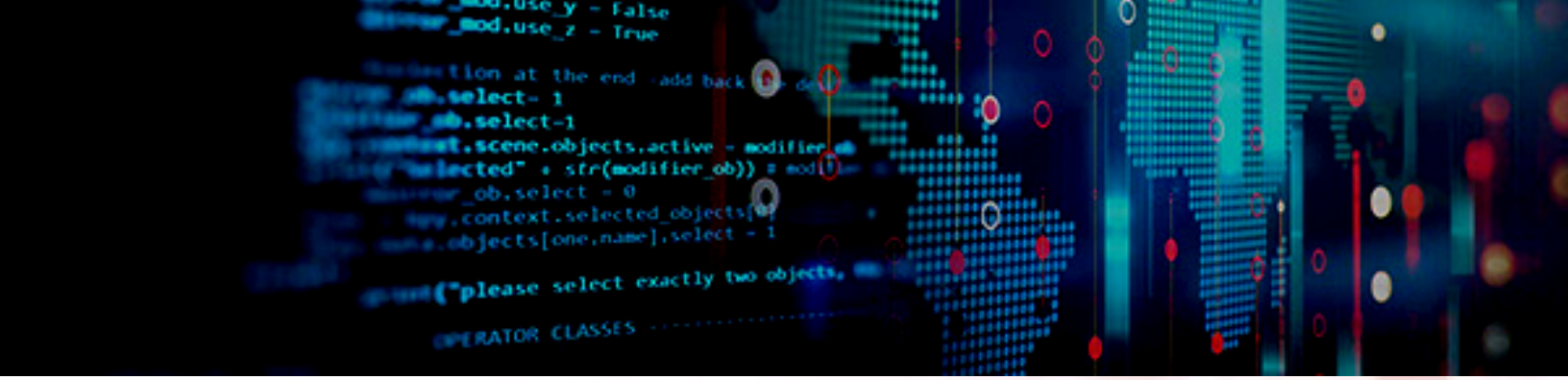
The seizure banner uploaded by German law enforcement. Although overall darknet marketplace revenue fell after Hydra's shutdown, the number of transactions to the remaining marketplaces increased. Chainalysis: "We suspect that this increase represents Hydra vendors and customers moving their funds to new markets in search of a replacement. Nevertheless, the decline in darknet market revenue — and indeed, cryptocurrency value received by all criminal categories — following Hydra's shutdown shows the tangible impact of law enforcement's growing ability to fight cryptocurrency-based crime.” cumulative monthly value received by darknet markets by year | Chainalysis Stolen Funds _ The company noticed an increase in the amount of stolen cryptocurrency. Through July 2022, $1.9 billion worth of cryptocurrency has been stolen. During the same period in 2021, only $1.2 billion worth of cryptocurrency had been stolen. This trend may continue to rise: in the first week of August, the cross-chain bridge Nomad suffered a $190 million hack, and someone stole $5 million from several Solana wallets. Chainalysis thinks the increase in the amount of stolen cryptocurrency is due to the rise in funds stolen from DeFi protocols. They believe that DeFi protocols are uniquely vulnerable because "their open source code can be studied ad nauseum by cybercriminals looking for exploits.”

Cumulative cryptocurrency value stolen in hacks. | Chainalysis The company wants law enforcement to continue to use Chainalysis' services and software in an attempt to catch the hackers responsible for lucrative cryptocurrency thefts. Additionally, they want law enforcement to develop new methods through which they can seize stolen cryptocurrency. "Nobody likes a crypto bear market, but the one silver lining is that illicit cryptocurrency activity has fallen along with legitimate activity, albeit not as sharply. This is especially encouraging in scams, where the decrease in market hype seems to mean fewer are fooled by scammers, and in darknet markets, where law enforcement's shutdown of Hydra Market appears to have dampened the entire sector. Still, with huge increases in stolen funds, we can't afford to rest on our laurels. The public and private sectors must continue to work together and hone their ability to fight cryptocurrency-based crime.” Mid-year Crypto Crime Update: Illicit Activity Falls With Rest of Market, With Some Notable Exceptions | archive.is, archive.org I bet this crypto activity is up though (via darknetlive.com at https://darknetlive.com/post/chainalysis-report-about-decrease-in-illicit-crypto-activity/)

Court Authorizes IRS Fishing Trip Against Crypto Prime Dealer

A court authorized the Internal Revenue Service to serve a John Doe summons on a cryptocurrency prime dealer in California. On August 15, 2022, a federal court in the Central District of California entered an order authorizing the IRS to serve a John Doe summons on sFOX. The IRS is seeking information about any U.S. taxpayers who transacted at least $20,000 in cryptocurrency through the platform. Per the company's website: "sFOX is the full-service crypto prime dealer for institutional investors, providing the liquidity, security, and infrastructure needed to unlock the full potential of digital assets.” "Taxpayers who transact with cryptocurrency should understand that income and gains from cryptocurrency transactions are taxable,” said Deputy Assistant Attorney General David A. Hubbert of the Justice Department's Tax Division. "The information sought by the summons approved today will help to ensure that cryptocurrency owners are following the tax laws.” sFOX claims to help its users 'secure their edge in crypto.' "The John Doe summons remains a highly valuable enforcement tool that the U.S. government will use again and again to catch tax cheats and this is yet one more example of that,” said IRS Commissioner Chuck Rettig. "I urge all taxpayers to come into compliance with their filing and reporting responsibilities and avoid compromising themselves in schemes that may ultimately go badly for them.” In the court's order, United States District Court Judge Otis D. Wright found that there is a reasonable basis to believe that people transacting $20,000 or more might not be complying with tax laws. The John Doe summons allows the IRS to obtain information about all U.S. taxpayers who use the sFOX without knowing their identity. "This John Doe summons directs SFOX to produce records identifying U.S. taxpayers who have used its services, along with other documents relating to their cryptocurrency transactions,” an announcement explained. Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Cryptocurrency | archive.is, archive.org I would not trust Z-Cash I can tell you that. (via darknetlive.com at https://darknetlive.com/post/court-authorizes-irs-fishing-trip-against-crypto-prime-dealer/)

Dark Web Link



Trend Micro Anti-Malware Blog

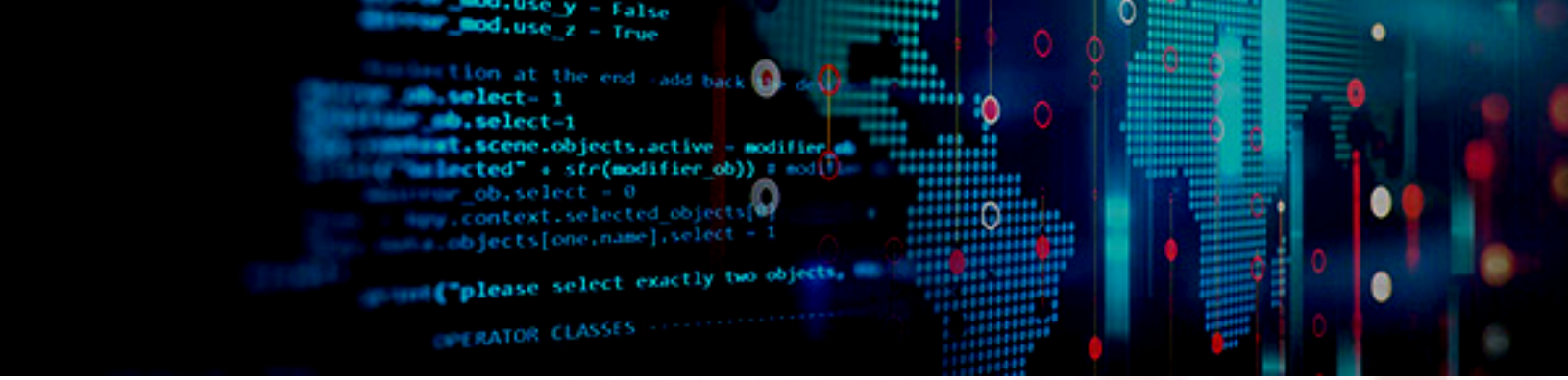
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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 Wrap-Up
* Pushing Open-Source Security Forward: Insights From Black Hat 2022
* 360-Degree XDR and Attack Surface Coverage With Rapid7
* [Security Nation] Jen and Tod on Hacker Summer Camp 2022
* Leading the Way in Tampa
* Active Exploitation of Multiple Vulnerabilities in Zimbra Collaboration Suite
* Are Your Apps Exposed? Know Faster With Application Discovery in InsightAppSec
* [VIDEO] An Inside Look at Black Hat 2022 From the Rapid7 Team
* Metasploit Weekly Wrap-Up
* 3 Mistakes Companies Make in Their Detection and Response Programs



Advisories

US-Cert Alerts & bulletins

* CISA releases 5 Industrial Control Systems Advisories
* Cisco Releases Security Update for Cisco Secure Web Appliance
* CISA Adds Seven Known Exploited Vulnerabilities to Catalog
* Apple Releases Security Updates for Multiple Products
* Threat Actors Exploiting Multiple Vulnerabilities Against Zimbra Collaboration Suite
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Update for Multiple Products
* #StopRansomware: Zeppelin Ransomware
* AA22-228A: Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite
* AA22-223A: #StopRansomware: Zeppelin Ransomware
* Vulnerability Summary for the Week of August 8, 2022
* Vulnerability Summary for the Week of August 1, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Apple Security Advisory 2022-08-17-1

Apple Security Advisory 2022-08-17-1 - iOS 15.6.1 and iPadOS 15.6.1 addresses code execution and out of bounds write vulnerabilities.

Apple Security Advisory 2022-08-17-2

Apple Security Advisory 2022-08-17-2 - macOS Monterey 12.5.1 addresses code execution and out of bounds write vulnerabilities.

Ubuntu Security Notice USN-5573-1

Ubuntu Security Notice 5573-1 - Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-6051-01

Red Hat Security Advisory 2022-6051-01 - An update is now available for RHOL-5.5-RHEL-8. Issues addressed include denial of service, man-in-the-middle, and out of bounds read vulnerabilities.

Red Hat Security Advisory 2022-6113-01

Red Hat Security Advisory 2022-6113-01 - Red Hat Application Interconnect 1.0 introduces a service network, linking TCP and HTTP services across the hybrid cloud. A service network enables communication between services running in different network locations or sites. It allows geographically distributed services to connect as if they were all running in the same site. This is an update to the rpms for Red Hat Application Interconnect 1.0 to fix some security issues in the golang compiler.

Ubuntu Security Notice USN-5572-1

Ubuntu Security Notice 5572-1 - Roger Pau Monné discovered that the Xen virtual block driver in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information. Roger Pau Monné discovered that the Xen paravirtualization frontend in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information.

Ubuntu Security Notice USN-5571-1

Ubuntu Security Notice 5571-1 - Sven Klemm discovered that PostgreSQL incorrectly handled extensions. An attacker could possibly use this issue to execute arbitrary code when extensions are created or updated.

Ubuntu Security Notice USN-5570-1

Ubuntu Security Notice 5570-1 - Evgeny Legerov discovered that zlib incorrectly handled memory when performing certain inflate operations. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5526-2

Ubuntu Security Notice 5526-2 - USN-5526-1 fixed vulnerabilities in PyJWT. Unfortunately this caused a regression by incrementing the internal package version number on Ubuntu 22.04 LTS. This update fixes the problem. Aapo Oksman discovered that PyJWT incorrectly handled signatures constructed from SSH public keys. A remote attacker could use this to forge a JWT signature.

Red Hat Security Advisory 2022-6079-01

Red Hat Security Advisory 2022-6079-01 - Red Hat Ansible Automation Platform provides an enterprise framework for building, deploying and managing IT automation at scale. IT Managers can provide top-down guidelines on how automation is applied to individual teams, while automation developers retain the freedom to write tasks that leverage existing knowledge without the overhead. Ansible Automation Platform makes it possible for users across an organization to share, vet, and manage automation content by means of a simple, powerful, and agentless language. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2022-6073-01

Red Hat Security Advisory 2022-6073-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6075-01

Red Hat Security Advisory 2022-6075-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6078-01

Red Hat Security Advisory 2022-6078-01 - Red Hat Ansible Automation Platform provides an enterprise framework for building, deploying and managing IT automation at scale. IT Managers can provide top-down guidelines on how automation is applied to individual teams, while automation developers retain the freedom to write tasks that leverage existing knowledge without the overhead. Ansible Automation Platform makes it possible for users across an organization to share, vet, and manage automation content by means of a simple, powerful, and agentless language. Issues addressed include a privilege escalation vulnerability.

Ubuntu Security Notice USN-5569-1

Ubuntu Security Notice 5569-1 - Xiang Li discovered that Unbound incorrectly handled delegation caching. A remote attacker could use this issue to keep rogue domain names resolvable long after they have been revoked.

Ubuntu Security Notice USN-5568-1

Ubuntu Security Notice 5568-1 - Several security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Red Hat Security Advisory 2022-6061-01

Red Hat Security Advisory 2022-6061-01 - The etcd packages provide a highly available key-value store for shared configuration. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6065-01

Red Hat Security Advisory 2022-6065-01 - Collectd plugin for gathering resource usage statistics from containers created with the libpod library.

Red Hat Security Advisory 2022-6062-01

Red Hat Security Advisory 2022-6062-01 - Collectd plugin for gathering resource usage statistics from containers created with the libpod library.

Red Hat Security Advisory 2022-6066-01

Red Hat Security Advisory 2022-6066-01 - The etcd packages provide a highly available key-value store for shared configuration. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6057-01

Red Hat Security Advisory 2022-6057-01 - .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 2022-6058-01

Red Hat Security Advisory 2022-6058-01 - .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.

Gentoo Linux Security Advisory 202208-31

Gentoo Linux Security Advisory 202208-31 - Multiple vulnerabilities have been found in GStreamer and its plugins, the worst of which could result in arbitrary code execution. Versions less than 1.16.3 are affected.

Gentoo Linux Security Advisory 202208-30

Gentoo Linux Security Advisory 202208-30 - Multiple vulnerabilities have been discovered in Binutils, the worst of which could result in denial of service. Versions less than 2.38 are affected.

Gentoo Linux Security Advisory 202208-29

Gentoo Linux Security Advisory 202208-29 - Multiple vulnerabilities have been discovered in Nokogiri, the

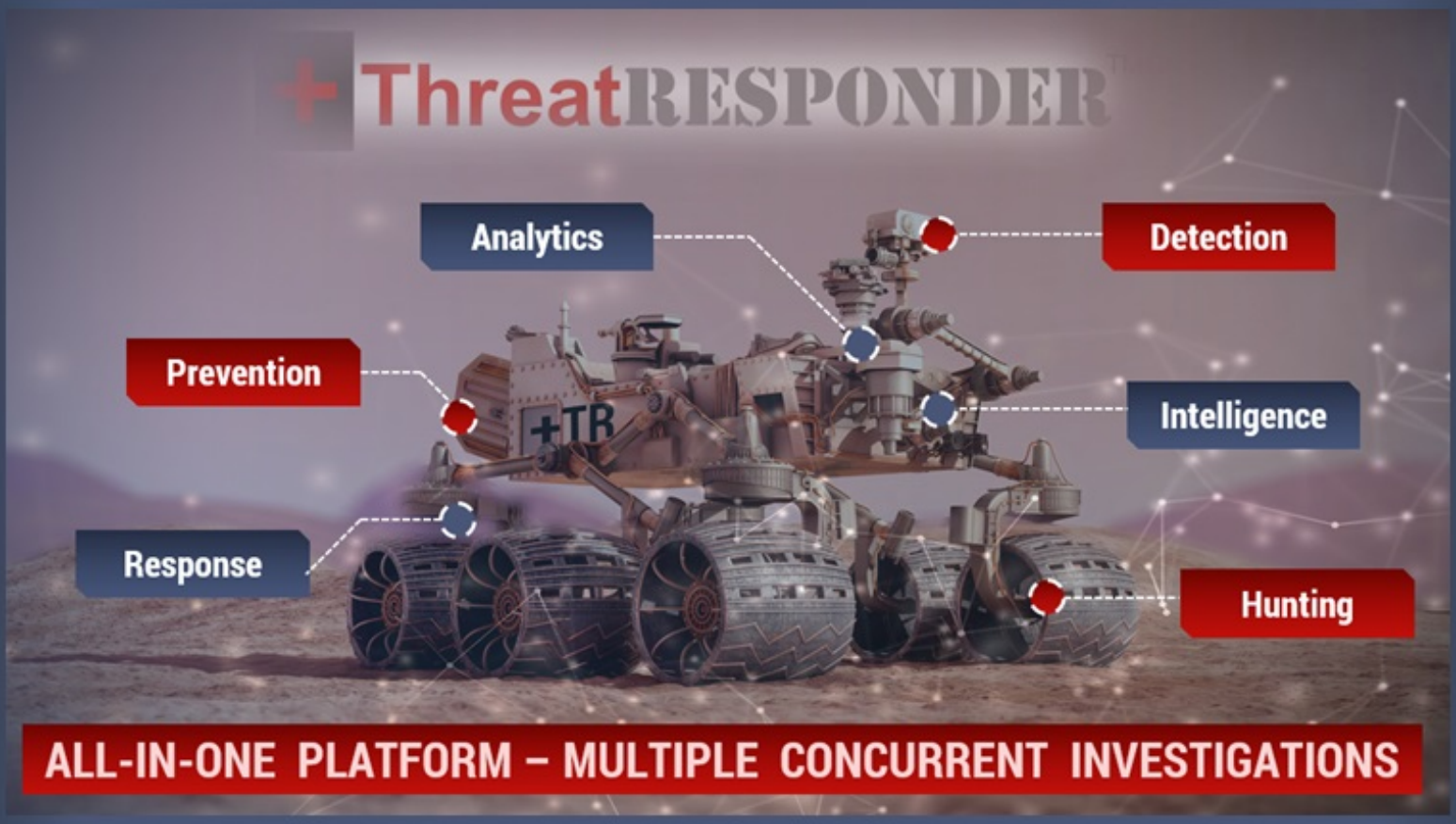
worst of which could result in denial of service. Versions less than 1.13.6 are affected.

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



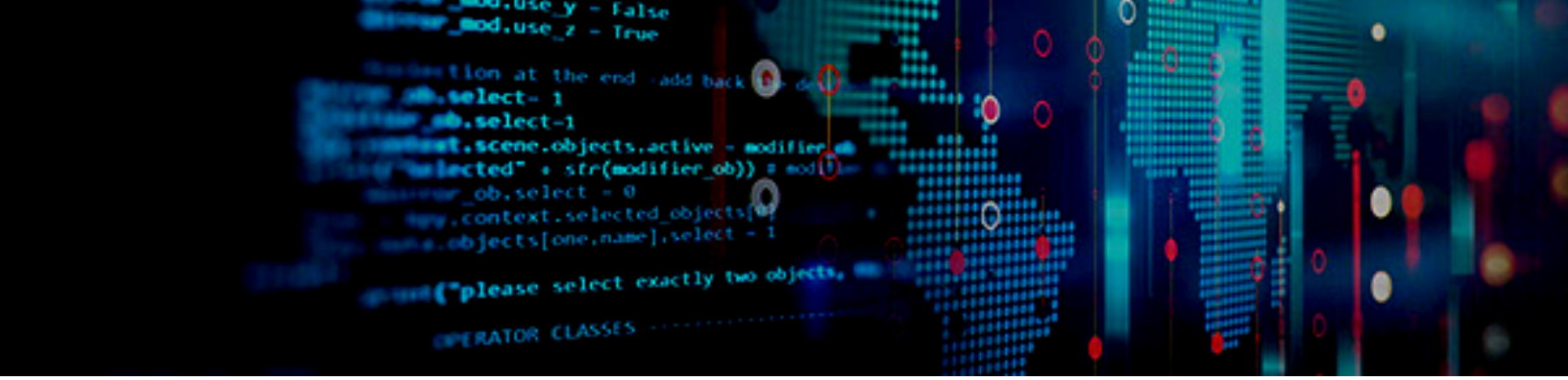
The Solution – ThreatResponder® Platform

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

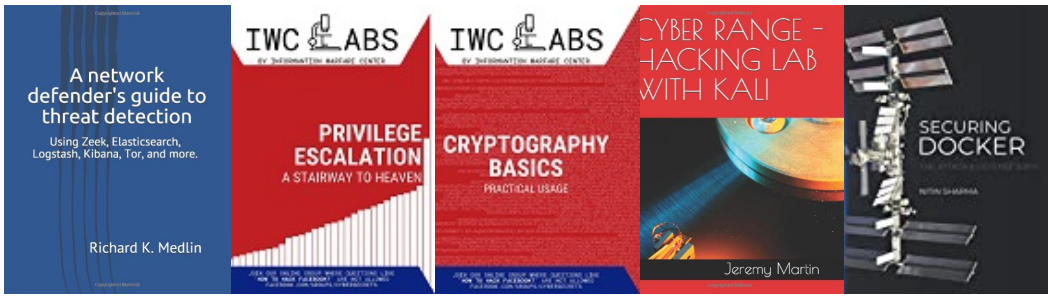


The Cyber Secrets publications on Amazon

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