Aug-08-22

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 8, 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

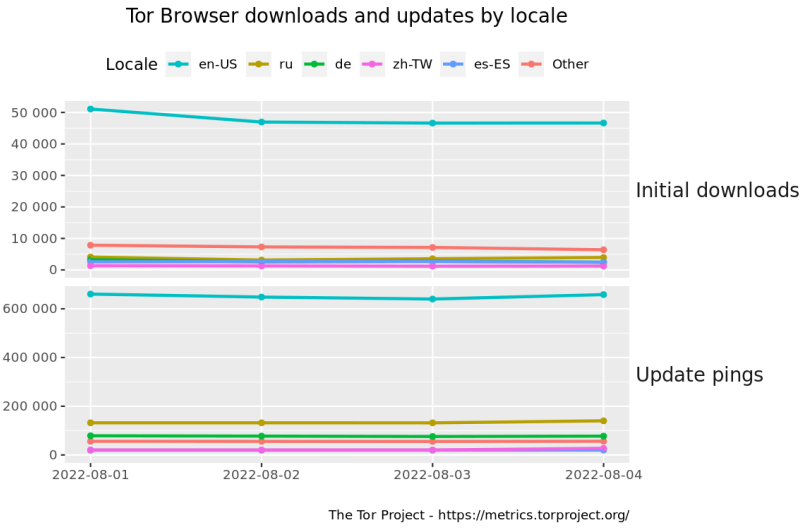
Internet Storm Center Infocon Status

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

* Senator Wants To Set Aside Millions For Small Biz Cybersecurity Training
* Critical Flaws Found In Four Cisco SMB Router Ranges
* Open Redirect Flaw Snags Amex, Snapchat User Data
* Huge Flaw Threatens US Emergency Alert System, DHS Researcher Warns
* Chinese Government Website Defaced Welcoming Pelosi To Taiwan
* Newly Launched Russian Spy Satellite Might Be Stalking A US Satellite
* VMWare Urges Users To Patch Critical Authentication Bypass Bug
* North Korea-Backed Hackers Have A Clever Way To Read Your Gmail
* Ransomware Task Force Releases SMB Blueprint For Defense And Mitigation
* Tonight We're Gonna Log On Like It's 1979
* Hack Drains Over A Million Dollars From Solana Crypto Wallets
* Nancy Pelosi Ties Chinese Cyber-Attacks To Need For Taiwan Visit
* The Age Of Brain-Computer Interfaces Is On the Horizon
* Lawsuit Claims Facebook Scraping Data From Hospital Sites
* U.S. Crypto Firm Nomad Hit By $190 Million Theft
* CIA Likely Used Ninja Bomb To Kill Terrorist Leader Ayman al-Zawahiri
* Post-Quantum Encryption Contender Is Taken Out By Single-Core PC And 1 Hour
* Spyware Developer Charged By Australian Police After 14,500 Sales
* Akamai: We Stopped Record DDoS Attack In Europe
* Founder Of Pro Russian Hacktivist Killnet Quitting Group
* Malicious Npm Packages Tapped Again To Target Discord Users
* Threat Actors Pivot Around Microsoft's Macro-Blocking In Office
* JPMorgan, UBS Among Trio Accused Of Shoddy ID Theft Protection
* Ransomware Hit The American Dental Association
* BreachForums Booms On The Back Of Billion Record Chinese Data Leak

Krebs on Security

* 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
* Massive Losses Define Epidemic of 'Pig Butchering'
* A Deep Dive Into the Residential Proxy Service '911'
* Why 8kun Went Offline During the January 6 Hearings
* Microsoft Patch Tuesday, July 2022 Edition

Dark Reading

* What Worries Security Teams About the Cloud?
* Genesis IAB Market Brings Polish to the Dark Web
* A Ransomware Explosion Fosters Thriving Dark Web Ecosystem
* Stolen Data Gives Attackers Advantage Against Text-Based 2FA
* Fresh RapperBot Malware Variant Brute-Forces Its Way Into SSH Servers
* How to Resolve Permission Issues in CI/CD Pipelines
* A Digital Home Has Many Open Doors
* Cyberattackers Increasingly Target Cloud IAM as a Weak Link
* Amazon, IBM Move Swiftly on Post-Quantum Cryptographic Algorithms Selected by NIST
* Time to Patch VMware Products Against a Critical New Vulnerability
* High-Severity Bug in Kaspersky VPN Client Opens Door to PC Takeover
* How Email Security Is Evolving
* Massive China-Linked Disinformation Campaign Taps PR Firm for Help
* Phylum Releases a Free Community Edition to Make Software Supply Chain Security More Accessible
* The Myth of Protection Online - and What Comes Next
* Deep Instinct Pioneers Deep-Learning Malware Prevention to Protect Mission-Critical Business Applicat
* 35K Malicious Code Insertions in GitHub: Attack or Bug-Bounty Effort?
* Ping Identity to Go Private After $2.8B Acquisition
* Startup Footprint Tackles Identity Verification
* How IT Teams Can Use 'Harm Reduction' for Better Cybersecurity Outcomes

The Hacker News

* Meta Cracks Down on Cyber Espionage Operations in South Asia Abusing Facebook
* New IoT RapperBot Malware Targeting Linux Servers via SSH Brute-Forcing Attack
* Hackers Exploit Twitter Vulnerability to Exposes 5.4 Million Accounts
* Slack Resets Passwords After a Bug Exposed Hashed Passwords for Some Users
* Iranian Hackers Likely Behind Disruptive Cyberattacks Against Albanian Government
* Emergency Alert System Flaws Could Let Attackers Transmit Fake Messages
* Resolving Availability vs. Security, a Constant Conflict in IT
* A Growing Number of Malware Attacks Leveraging Dark Utilities 'C2-as-a-Service'
* CISA Adds Zimbra Email Vulnerability to its Exploited Vulnerabilities Catalog
* Who Has Control: The SaaS App Admin Paradox
* Critical RCE Bug Could Let Hackers Remotely Take Over DrayTek Vigor Routers
* New Woody RAT Malware Being Used to Target Russian Organizations
* Hackers Exploited Atlassian Confluence Bug to Deploy Ljl Backdoor for Espionage
* Three Common Mistakes That May Sabotage Your Security Training
* Cisco Business Routers Found Vulnerable to Critical Remote Hacking Flaws

Security Week

* Twitter Breach Exposed Anonymous Account Owners
* Ghost Security Snags $15M Investment for API Security Tech
* Slack Forces Password Resets After Discovering Software Flaw
* FEMA Urges Patching of Emergency Alert Systems, But Some Flaws Remain Unfixed
* F5 Fixes 21 Vulnerabilities With Quarterly Security Patches
* Traffic Light Protocol 2.0 Brings Wording Improvements, Label Changes
* Zimbra Credential Theft Vulnerability Exploited in Attacks
* Disruptive Cyberattacks on NATO Member Albania Linked to Iran
* SMBs Exposed to Attacks by Critical Vulnerability in DrayTek Vigor Routers
* The Secret to Automation? Eat the Elephant in Chunks.
* Cybersecurity Firm ZeroFox Begins Trading on Nasdaq via SPAC Deal
* Critical Vulnerabilities Allow Hacking of Cisco Small Business Routers
* Secure Enterprise Browser Startup Talon Raises $100 Million
* Cyber Readiness Measurement Firm Axio Raises $23 Million
* Taiwan Govt Websites Attacked During Pelosi Visit
* VirusTotal Data Shows How Malware Distribution Leverages Legitimate Sites, Apps
* Compliance Automation Startup RegScale Scores $20 Million Investment
* Robinhood Crypto Penalized $30M for Violating NY Cybersecurity Regulations
* Power Electronics Manufacturer Semikron Targeted in Ransomware Attack
* Thoma Bravo to Acquire Ping Identity for $2.8 Billion
* Cybersecurity Financing Declined in Q2 2022, But Investors Optimistic
* Cybersecurity M&A Roundup: 39 Deals Announced in July 2022
* Google Paid Out $90,000 for Vulnerabilities Patched by Chrome 104
* The Ever-Increasing Issue of Cyber Threats - and the Zero Trust Answer
* Nearly $200 Million Stolen From Cryptocurrency Bridge Nomad
* UK Clears Norton's $8B Avast Cyber Security Takeover

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* LinkedIn Continues its Reign as the Most-Impersonated Brand in Phishing Attacks
* Ransomware Attack Downtime Costs in the U.S. Rise to Nearly $160 Billion
* Open Redirects Exploited for Phishing
* KnowBe4 Wins Multiple Summer 2022 "Best of" Awards From TrustRadius
* On-Demand Webinar: New 2022 Phishing By Industry Benchmarking Report: How Does Your Organization Meas
* Labor Market Social Engineering: Supply-Side and Demand-Side
* New Data Breach Extortion Attack Begins with a Fake Duolingo or MasterClass Subscription Scam
* Security and Gender: The Gaps Are Not Where You Expect
* CyberheistNews Vol 12 #31 [Heads Up] Crafty Microsoft USB Scam Shows the Importance of Security Aware
* Cyber Insurance Expected to Continue to Rise as Sophistication and Cost of Ransomware Attacks Increas

ISC2.org Blog

* Latest Cyberthreats and Advisories - August 5, 2022
* #ISC2CONGRESS - Why you won't want to miss it!
* #ISC2Congress: From National Security to Cartel Infiltration - Ciaran Martin and Robert Mazur to Keyn
* State Policymakers Tackling Cyber Issues Including Ransomware
* SSCP Exam - Changes on the Way!

HackRead

* Twitter Confirms Data Breach as 5.4M Accounts Sold on Hacker Forum
* Microsoft bars Tutanota users from registering MS Teams accounts
* Machine Learning: How To Become A Machine Learning Engineer?
* Chinese Adult Site Leaking 14 Million User Details - and It's Increasing!
* Hackers Can Exploit US Emergency Alert System Flaws to Fake Warnings
* Anonymous Source Leaks 4TB of Cellebrite Data After Cyberattack
* Thousands of GitHub Repositories Cloned in Supply Chain Attack

Koddos

* Twitter Confirms Data Breach as 5.4M Accounts Sold on Hacker Forum
* Microsoft bars Tutanota users from registering MS Teams accounts
* Machine Learning: How To Become A Machine Learning Engineer?
* Chinese Adult Site Leaking 14 Million User Details - and It's Increasing!
* Hackers Can Exploit US Emergency Alert System Flaws to Fake Warnings
* Anonymous Source Leaks 4TB of Cellebrite Data After Cyberattack
* Thousands of GitHub Repositories Cloned in Supply Chain Attack

Naked Security

* 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!
* S3 Ep93: Office security, breach costs, and leisurely patches [Audio + Text]
* Critical Samba bug could let anyone become Domain Admin - patch now!
* Mild monthly security update from Firefox - but update anyway

Threat Post

* Open Redirect Flaw Snags Amex, Snapchat User Data
* VMWare Urges Users to Patch Critical Authentication Bypass Bug
* Universities Put Email Users at Cyber Risk
* Securing Your Move to the Hybrid Cloud
* Malicious Npm Packages Tapped Again to Target Discord Users
* Threat Actors Pivot Around Microsoft's Macro-Blocking in Office
* Messaging Apps Tapped as Platform for Cybercriminal Activity
* Novel Malware Hijacks Facebook Business Accounts
* Phishing Attacks Skyrocket with Microsoft and Facebook as Most Abused Brands
* IoT Botnets Fuels DDoS Attacks - Are You Prepared?

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

* The cloud ate my database
* 9 platforms that improve employee digital experiences
* Visual Studio vs. Visual Studio Code: How to choose
* Microsoft launches .NET Community Toolkit
* iPaaS, low-code platform sales to hit double-digit growth in 2022: Gartner
* Django 4.1 adds async handlers
* Some cloud-based AI systems are returning to on-premises data centers
* What is Tomcat? The original Java servlet container
* BrandPost: A Climbing Crane Helps Energy Harvesting Reach New Heights
* BrandPost: Accelerating Azure Databricks Runtime for Machine Learning

C4ISRNET - Media for the Intelligence Age Military

* Raytheon's Blue Canyon opens expanded small satellite production facility
* Operation Cyber Dragon turning US Navy reservists into digital defenders
* Pentagon reminds everyone not to wipe their phones
* Machinist union votes to approve new Boeing contract, averting strike
* US spy agency sends another satellite to space in show of rapid launch capability
* Space-Based Infrared satellite launch to complete missile warning system
* Remember 5G? Pentagon backs 6G hub tied to Army Research Lab
* Which drone was used in Al-Zawahiri strike? Experts point to General Atomics' Reaper
* A look at the 'knife bomb' that may have killed al-Qaida leader
* US, Ukraine agree to more cyber cooperation amid Russian threat

The Hacker Corner

Conferences

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

Google Zero Day Project

* 2022 0-day In-the-Wild Exploitation…so far
* The curious tale of a fake Carrier.app

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* T3N4CI0US CTF - Escape
* DEF CON CTF 2022
* SHELLCTF 2022
* nullcon Goa HackIM CTF 2022
* WMCTF2022
* Midnight Sun CTF 2022 Finals
* Hacker's Playground 2022
* CTFZone 2022
* HITB SECCONF CTF 2022
* MapleCTF 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 0.17.3
* 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
* Global Socket 1.4.38
* Suricata IDPE 6.0.6
* GNU Privacy Guard 2.3.7

Kali Linux Tutorials

* 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
* Kubeaudit : Tool To Audit Your Kubernetes Clusters Against Common Security Controls
* Dumpscan : Tool To Extract And Dump Secrets From Kernel And Windows Minidump Formats
* Trufflehog : Find Credentials All Over The Place
* Bypass-Url-Parser : Tool That Tests Many URL Bypasses To Reach A 40X Protected Page
* WebView2-Cookie-Stealer : Attacking With WebView2 Applications
* Tofu : Windows Offline Filesystem Hacking Tool For Linux

GBHackers Analysis

* 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
* Cisco Nexus Dashboard Flaw Let Remote Attacker Execute Arbitrary Commands
* VMware vCenter Server Flaw Let Attacker Exploit to Perform Elevate Privileges Attack

Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

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

Hak5

* Major Release Announcement
* Advanced Windows Recon Using the OMG Cable | HakByte
* UEFI Rootkit Spotted In The Wild - ThreatWire

The PC Security Channel [TPSC]

* Kaspersky Plus Review: First Impressions
* How to know if your PC is hacked? Suspicious Network Activity 101

Eli the Computer Guy

* Silicon Dojo #1 - Tour of Hatch Coworking
* Testing Streamlabs
* eBeggar Wednesday - DOCTOR STRANGE 2 SUCKED
* Be a YOUTUBE CREATOR for Business and Career Development (Silicon Dojo)

Security Now

* Rowhammer's Nine Lives - TLS-Anvil, Chrome cookies stick around, Atlassian Confluence under attack
* The MV720 - MS Office VBA macros, Win 11 security changes, start button failure

Troy Hunt

* Weekly Update 307

Intel Techniques: The Privacy, Security, & OSINT Show

* 273-Credential Exposure Removal
* 272-Processor Attacks Explained

Proof of Concept (PoC) & Exploits

Packet Storm Security

* 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
* Online Admission System 1.0 SQL Injection
* WordPress Testimonial Slider And Showcase 2.2.6 Cross Site Scripting
* VMware Workspace ONE Access Privilege Escalation
* Chrome WebGL Uniform Integer Overflows
* Backdoor.Win32.Jokerdoor MVID-2022-0628 Buffer Overflow
* WordPress Download Manager 3.2.50 Arbitrary File Deletion
* WordPress Duplicator 1.4.7 Unauthenticated Backup Download
* Zoho Password Manager Pro XML-RPC Java Deserialization
* MobileIron Log4Shell Remote Command Execution
* Multi-Language Hotel Management 2022 1.0 SQL Injection
* IObit Malware Fighter 9.2 Tampering / Privilege Escalation
* uftpd 2.10 Directory Traversal
* Packet Storm New Exploits For July, 2022
* Backdoor.Win32.Destrukor.20 MVID-2022-0627 Remote Command Execution
* Omnia MPX 1.5.0+r1 Path Traversal
* NanoCMS 0.4 Remote Code Execution
* CuteEditor For PHP 6.6 Directory Traversal
* Backdoor.Win32.Destrukor.20 MVID-2022-0626 Authentication Bypass / Code Execution
* mPDF 7.0 Local File Inclusion
* WordPress Duplicator 1.4.6 Backup Disclosure
* WordPress Duplicator 1.4.7 Information Disclosure

CXSecurity

* VMware Workspace ONE Access Privilege Escalation
* NanoCMS 0.4 Remote Code Execution
* MobileIron Log4Shell Remote Command Execution
* mPDF 7.0 Local File Inclusion
* Easy Chat Server 3.1 Buffer Overflow
* Roxy-WI Remote Command Execution
* Sourcegraph gitserver sshCommand Remote Command Execution

Proof of Concept (PoC) & Exploits

Exploit Database

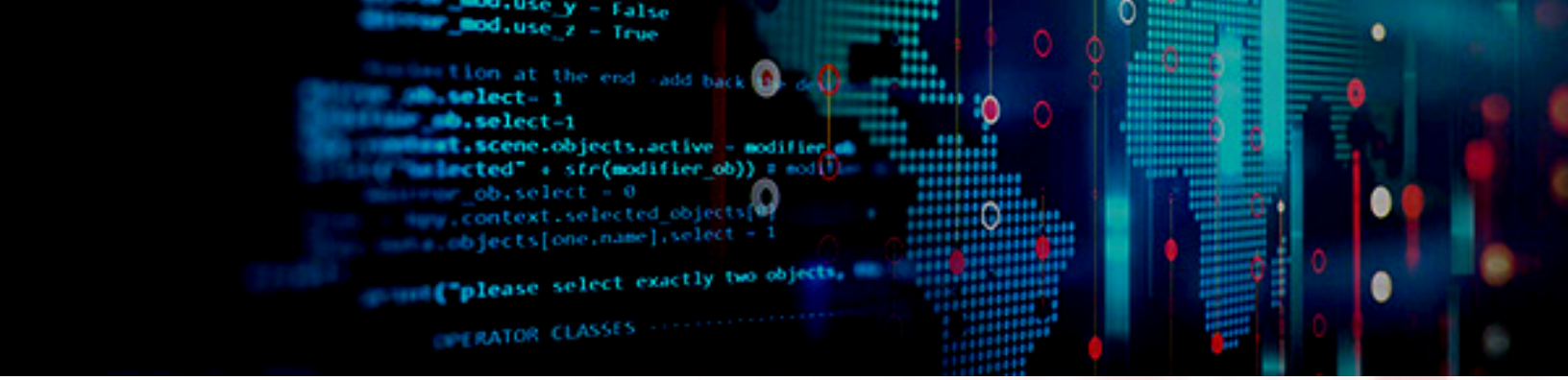
* [remote] uftpd 2.10 - Directory Traversal (Authenticated)
* [remote] Easy Chat Server 3.1 - Remote Stack Buffer Overflow (SEH)
* [webapps] Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)
* [webapps] NanoCMS v0.4 - Remote Code Execution (RCE) (Authenticated)
* [remote] Omnia MPX 1.5.0+r1 - 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
* [webapps] OctoBot WebInterface 0.4.3 - Remote Code Execution (RCE)
* [webapps] CodoForum v5.1 - Remote Code Execution (RCE)
* [local] Dr. Fone 4.0.8 - 'net_updater32.exe' Unquoted Service Path
* [webapps] Magnolia CMS 6.2.19 - Stored Cross-Site Scripting (XSS)
* [local] Kite 1.2021.610.0 - Unquoted Service Path

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*

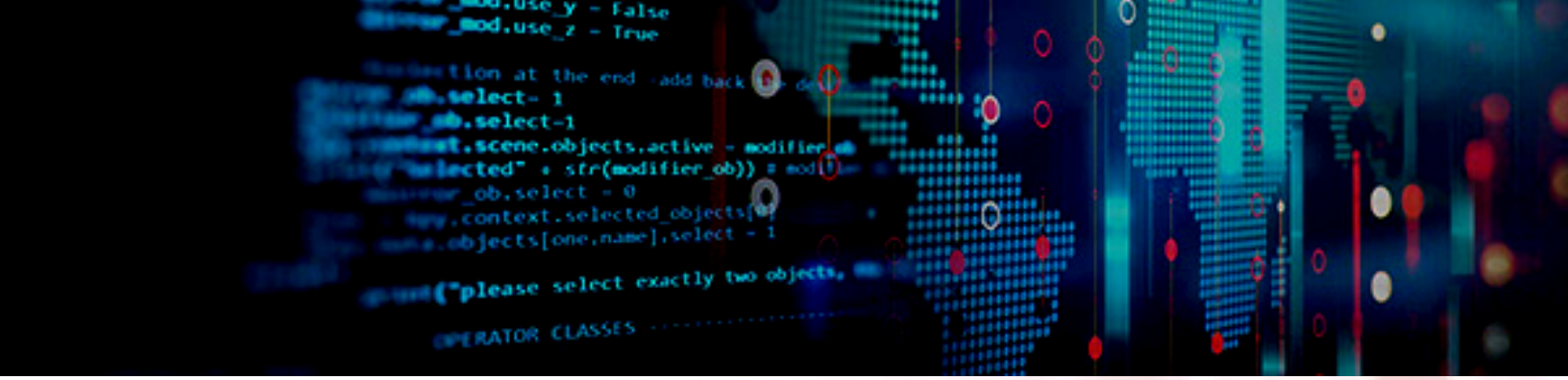
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.oicfiscaliamorelos.gob.mx/fake.php
https://www.oicfiscaliamorelos.gob.mx/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://satpolpp.sukabumikab.go.id/fake.php
https://satpolpp.sukabumikab.go.id/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://ffh.gov.mz/fake.php
https://ffh.gov.mz/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://www.municipalidadpjc.gov.py/fake.php
https://www.municipalidadpjc.gov.py/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://hsdp.gov.co/mf4tn.html
https://hsdp.gov.co/mf4tn.html notified by Mf4 Team
https://loon.gov.ph/sad.php
https://loon.gov.ph/sad.php notified by ./BarBarKing
http://inhukab.go.id
http://inhukab.go.id notified by ./MungielL
https://abiico.gov.et/404.html
https://abiico.gov.et/404.html notified by AnonSec Team
https://amharatrade.gov.et/404.html
https://amharatrade.gov.et/404.html notified by AnonSec Team
http://sindhhec.gov.pk/Sec.html
http://sindhhec.gov.pk/Sec.html notified by Mr.Kro0oz.305
https://nonyor.go.th/Sec.html
https://nonyor.go.th/Sec.html notified by Mr.Kro0oz.305
https://kangplu.go.th/Sec.html
https://kangplu.go.th/Sec.html notified by Mr.Kro0oz.305
https://naimeung.go.th/Sec.html
https://naimeung.go.th/Sec.html notified by Mr.Kro0oz.305
https://khamtalayso.go.th/Sec.html
https://khamtalayso.go.th/Sec.html notified by Mr.Kro0oz.305
https://samrong.go.th/Sec.html
https://samrong.go.th/Sec.html notified by Mr.Kro0oz.305
https://congchung.gov.vn/0.htm
https://congchung.gov.vn/0.htm notified by ./Cyber00t
http://dindik.lumajangkab.go.id/read.txt
http://dindik.lumajangkab.go.id/read.txt notified by Mr.L3RB1



Dark Web News

Darknet Live

Counterfeit Euro Use in Germany Is on the Decline

The number of counterfeit banknotes in circulation in Germany fell to the lowest since 2013. According to Germany's central bank, the Deutsche Bundesbank, law enforcement officers, bank employees, and retailers pulled 19,789 counterfeit euro notes out of circulation in the first six months of 2022. The number of counterfeit notes decreased by 3.9% since the second half of 2021. __ The European Central Bank unveiled a new 50-euro note in 2016 to combat counterfeiting The number of notes pulled from circulation is the lowest since the second half of 2013, when authorities recorded 19,350 fake euros. "The trend in counterfeit money has been declining since 2016,” said Bundesbank board member Johannes Beermann. However, the damage caused by counterfeit euros increased by 11% to â‚¬991,690 since the second half of 2021. Counterfeit â‚¬20 and â‚¬50 banknotes account for 77% of the counterfeit euros seized There are five fake euro notes per 10,000 inhabitants in Germany There are ten fake euros per 10,000 across Europe Beerman suggested that the government's lockdowns made it more difficult for criminals to pass counterfeit notes. Fake euros seized during an investigation into Europe's second-largest counterfeit currency network The Federal Criminal Police Office (BKA) reported that more than half of the counterfeit notes in circulation came from vendors on the darknet or "via encrypted messenger services.” Counterfeit Figures At Lowest Level Since 2013 | archive.is, archive.org, globeecho.com (via darknetlive.com at https://darknetlive.com/post/counterfeit-use-in-germany-is-declining/)

Washington Doctor Might Plead Guilty in Murder For Hire Case

A neonatologist who allegedly tried to hire a hitman on the darkweb to kidnap his wife and assault a colleague might enter a guilty plea. Dr. Ronald Ilg, 55, of Spokane, Washington, allegedly contacted murder-for-hire sites on the darkweb with two jobs. In his first request, the doctor asked for someone to injure a colleague. In his messages to the murder-for-hire sites, Ilg allegedly used the username "Scar215.” __ Ronald Ilg | Linkedin Victim 1 _ Scar215: "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.” In subsequent messages, Scar215 provided the name and address of the intended victim (Victim #1). Victim 2 _ In the the request, Scar215 wanted someone to kidnap, assault, drug, and extort his wife (Victim #2). Transcripts of Scar215's messages are provided in the criminal complaint. __ Redacted Screenshot from DARK WEBSITE #1 - A fraudulent murder-for-hire website Scar215 : "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. Also, 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.” The user offered a bonus if the hitman or employee of the murder-for-hire site could get the victim to do certain things. Scar215: "First, let's ensure the goals are correct. I think you accidently wrote 'not go back' when in fact she MUST go back. This is the absolute goal that she must do for a good bonus. Goals Stop all court proceedings Do go back to her husband weather she wants to or not Keep her mouth shut, and tell no one about the kidnapping Plant drugs in her home and used needles a day or so after collecting her. So, if people start looking for her while she is detained, they will find them. Inject her with heroin 2 times per day. Teach her to inject herself. Send pics and videos of her injecting herself for bribery later. Her schedule I have described. I have been told she has kids every other week starting on Friday. She has kids starting this Friday. She works week days from about 8 to 4. When she does NOT have kids she works at the spa on Saturday and then Wednesday after work. I will use an external escrow. Hidden WiKi, where I first discovered your link, suggests the following: 'Bitcoin Escrow - Best escrow service on the dark web, low fees, ensures that both vendor and customers are safe by keeping the funds in a secure account until goods or services are delivered' Can you please encourage your guy to start now. I have $40k in a wallet right now. I tried to send a pic of it but I cant get this email to select that file. I will start moving the Bitcoin as soon as we agreed on an escrow. But it will take a couple days to get there. I dont want to loose much more time. If he collects her when she has kids it will be immediately publisized. If she doesnt have kids AND she is forced to send texts out to work and any nosey friends , she could say she has COVID and is quarantined. So, please have him start now and send me updates and pics as soon as you have her. AND is the Bitcoin Escrow gonna work for us? Thanks” Redacted Screenshot from DARK WEBSITE #2 Scar215: "I am moving Bitcoin around for the independent escrow. I think being very clear about the bonus will avoid a dispute. So, I will propose the following: To earn the additional associated bonus, within two weeks of the target being released, she will have completed the specific goal. permanently withdraw all court motions and all mediated agreements. Bonus $10k Return to your husband by asking to move back home AND fucking him at least three times within the 2 week time frame.” "Bonus: $10k Keep her mouth shut and tell no one ever about the kidnapping Bonus $10k Inject her daily with heroin and teach her to do it AND supply pics and videos of her injecting herself. $5k Plant drugs and used needles with her DNA in the needles through her home. Provide some pics of drugs and needles scattered around $5k It is important to note that the husband does NOT know this is happening. He had a similar experience though to make sure he will take her back, which he agreed to do. She is strong for a woman. And she is stubborn and will need lots of persuasion. And she will say yes when she is thinking "fuck no,” so after she is released a way to continue to encourage her would be a good idea. Let me know soon if the escrow I named is acceptable. If so, I will put $40k in there. I will put $20k today once we agree to the escrow and the terms of the goals.” 'Redacted Screenshot from DARK WEBSITE #3' which appears to depict an escrow website. In April 2020, journalists with a British news organization (BBC) forwarded transcripts of Scar215's messages to investigators with the Federal Bureau of Investigation (FBI). The transcripts included Bitcoin transaction hashes sent from Scar215 to at least one of the murder-for-hire site operators. The transactions referenced by Scar215 originated from Coinbase. The FBI Virtual Currency Response Team conducted Bitcoin blockchain analysis on the Bitcoin transaction hashes and addresses included in the messages sent by Scar215. They found that most of the payments received by the murder-for-hire site(s) originated from Coinbase. Records provided by Coinbase indicated that "Ron Ilg” had opened the Coinbase account responsible for sending the Bitcoin to the murder-for-hire site. The account was also associated with Ilg's phone number, email address, and social security number. Coinbase also provided investigators with a list of transactions initiated by Ilg. Included in the list are transactions related to those involving Scar215.
Coinbase provided feds with a list of transactions initiated by Ilg. "Notably, the highlighted transactions

indicate that ILG used Coinbase.com to transfer approximately $56,308.12 into escrow to pay for the assault of VICTIM 1 and for the plan to kidnap, assault, extort, and drug VICTIM 2. The timing and value of these transactions also corresponds with the messages obtained from the News Organization and later confirmed by the FBI.” On April 11, 2021, the FBI executed a search warrant at Ilg's house in Spokane, Washington. In the house, the FBI found the username "Scar215” and an associated password written on a sticky note inside a safe. Ilg opened the safe using his fingerprint at the FBI's request. Later, the FBI used the credentials found in the safe to access the "Scar215” account on three onion services. In an interview with the FBI, Ilg admitted using the onion services in question but said he had intended on employing their services on himself (in an assisted suicide, of sorts). The doctor has pleaded not guilty to the charges. However, Ilg's attorney, Carl Oreskovtich, asked the court about setting up a hearing in the event the defense and prosecution came to an agreement. Less than a week later, the court scheduled a change of plea hearing, indicating that Ilg would plead guilty to at least some of the charges. Background on Victim 1 _ One of the doctor's former coworkers at Pediatrix claimed the doctor had harassed her at work. As a result, according to a civil lawsuit filed by the doctor, the company forced him to resign. Ilg claims the harassment claims are false. The Spokesman-Review: "In the civil lawsuit, Ilg alleges that he'd served as Pediatrix's corporate medical director through November 2019, when the company eliminated the position following allegations of harassment against Ilg that he claims were false. A year later, he was forced to resign from the company, according to the lawsuit.” "Ilg alleges that the termination was without cause and that Pediatrix and its parent company, Mednax, did not give him an opportunity to participate in a human resources investigation against him.” "The lawsuit states that Ilg entered the Physician Health Program, a confidential treatment program for doctors who face challenges that might impair their work, following a meeting with Sacred Heart Medical Center Children's Hospital's chief administrator in 2019. The doctor treating Ilg would not allow him to return to work at Sacred Heart during his treatment, according to the lawsuit.” "Ilg was forced to resign by Pediatrix in December 2020, according to the lawsuit.” Victim 1 is apparently the former coworker who made the harassment claims against Ilg. Complaint pdf (via darknetlive.com at https://darknetlive.com/post/washington-dr-to-plead-guilty-in-murder-for-hire-case/)

Jersey Teen Sentenced for Buying Amphetamine on Darkweb

A Jersey teenager who bought amphetamine on the darkweb was sentenced to 150 hours of community service and 12 months of probation. According to information heard in court, the defendant purchased drugs on the darkweb to use and sell to his friends. In November 2020, customs officers executed a search warrant at the then 16-year-old's residence. During the search, officers found MDMA pills, amphetamine powder, and LSD. They also seized a laptop computer, USB drive, and other electronic devices. According to the Jersey Evening Post, investigators found the USB drive plugged into the laptop. It was "discovered to have a browser open on a dark web marketplace selling controlled drugs. The USB stick was later found to hold a program designed to anonymise computer use relating to the internet and emails.” Tails!

Out of all the fictional dystopian art styles that exist, THIS is the dystopian art style we get? FML A search of the defendant's phone resulted in the discovery of messages discussing drug dealing, internet searches related to drug use, and cryptocurrency exchange accounts. Investigators found evidence the defendant had purchased marijuana online, "pictures depicting drug use, large amounts of cash, evidence of the purchase of hundreds of clear plastic zip-lock bags, and a suspected Instagram and Snapchat advert for MDMA.” The defendant also had a text document on his phone outlining plans for drug importation and trafficking. Womp womp "An expert witness valued the seized drugs seized at: two MDMA tablets with with a total value between Â£40 and Â£60, as well as 25.45 grams of amphetamine totalling between Â£1,500 and Â£2,000, 0.610 grams of amphetamine totalling between Â£30 and Â£40, 0.653 grams amphetamine totalling between Â£30 to Â£40 and half a tab of LSD worth between Â£10 and Â£15.” At an earlier hearing, the defendant pleaded guilty to possession charges and later admitted arranging to import 35 grams of amphetamine to a friend's house. The defendant's attorney told the court that her client struggled with undiagnosed autism and ADHD and that he primarily used the drugs for "medical purposes.” Edited 3 Aug 2022 to revise introductory paragraph with no material changes to content. (via

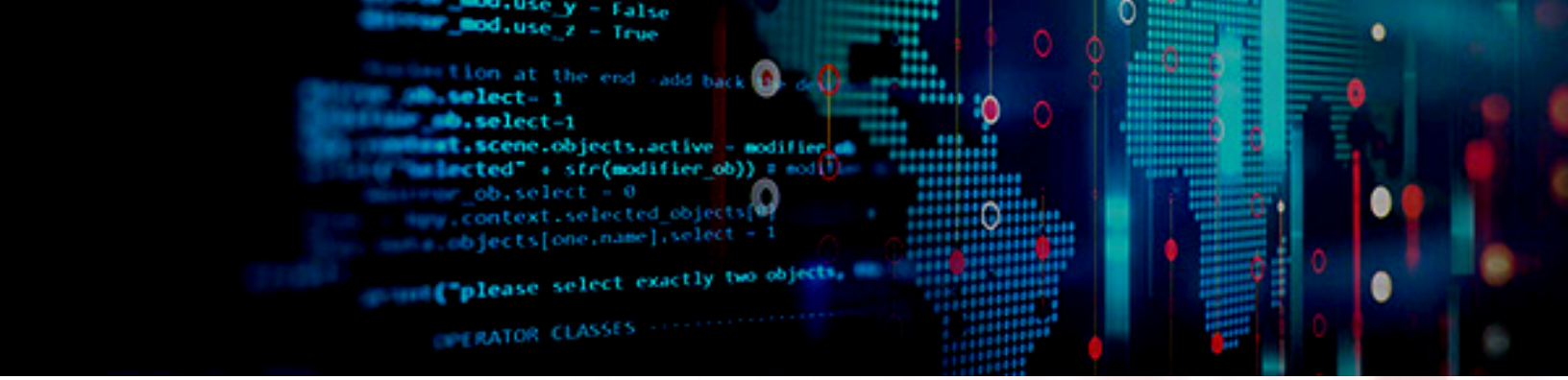
darknetlive.com at https://darknetlive.com/post/jersey-teen-sentenced-for-buying-drugs-on-darkweb/)

Ohio Man Sentenced for Buying Jewelry with Stolen Credit Cards

A Cleveland man was sentenced to probation for purchasing jewelry with stolen credit card information purchased on the darkweb. U.S. District Judge Sara Lioi sentenced Jaelen D. Lattimore, 23, to three years probation for purchasing $20,000 worth of jewelry from two Jewelry stores in Aurora, Ohio. In March, Lattimore pleaded guilty to conspiracy to commit access device fraud. He admitted to conspiring with Hasan J. Howard Jr., 23, to purchase jewelry using stolen credit card information. According to information revealed in court, Howard and Lattimore bought stolen credit and bank card information on the darkweb. Specifically, investigators learned that the conspirators purchased the stolen information on "Joker's Stash,” one of the most successful markets for buying and selling stolen data. A tweet from one of Lattimore's co-conspirators. From the criminal complaint: "On or about May 19, 2021, HASAN and LATTIMORE were arrested after conducting thefts at Kay and Zales Jewelers in Aurora, Ohio, for purchases exceeding $20,000. At the time of their arrest, HOWARD and LATTIMORE had a credit card embossing machine, three Rolex watches, and a .38 caliber pistol.” In most cases, the defendants purchased jewelry from jewelry stores over the phone or online. The criminal complaint provides numerous examples, including the following incidents from May 2021: "On or about May 10, 2021, a fraudulent transaction was reported at Jared Jewelers, 16760 Royalton Road, Strongsville, Ohio, for a diamond earring, using a fraudulent credit card ending in 5437, for a loss of $8,261. The order was placed over the phone using XXX-XXX-9656 under the name ALEXANDER JOHNSON believed to be HOWARD. Later that same day, another purchase was attempted using the same credit card for $9,179 but was declined. "On May 11, 2021, a fraudulent transaction was reported at Jared Jewelers, 16760 Royalton Road, Strongsville, Ohio, for two diamond bracelets, using fraudulent credit card ending in 0192, for a total loss of $18,359. The order was placed over the phone using XXXXXX-9656 under the name ALEXANDER JOHNSON believed to be HOWARD. On the same date, 17 minutes later, an attempted purchase using XXX-XXX-9656, under ALEXANDER JOHNSON was placed using the same credit card but was declined for the attempted $17,279.99.”

Hasan J. Howard Jr. Prosecutors say the defendants used stolen payment information to purchase jewelry from 30 jewelry stores in Ohio. On Howard's publicly viewable Instagram account, investigators found pictures of jewelry and electronics stolen from businesses in Ohio. "On or about December 28, 2020, a fraudulent transaction was reported at Big Sandy Superstore, Reynoldsburg, Ohio, using a fraudulent credit card ending in 3922 to purchase an 8K television for $5,159. No video surveillance was available at the pickup location of the television. The name used on the invoice was ADRIAN BERRY. It was later discovered during the search warrant for Instagram account belonging to HOWARD, that HOWARD posted pictures of the fraudulently purchased television on or about December 28, 2020 with quote "8K tv for ps5 ya know”. This same television was discovered at HOWARD's residence during the execution of a search warrant on May 20, 2021.” Howard often sold solen jewelry through Instagram and paid his co-conspirators with the proceeds of the sales. Judge Lioi sentenced Hasan Howard, 23, of Cleveland, Ohio, to more than six years in prison for various fraud charges. In March 2022, Howard pleaded guilty to conspiracy to commit access device fraud, access device fraud, and aggravated identity theft. The judge also ordered Howard to pay $261,319.28 in restitution. Other co-conspirators are awaiting sentencing. Criminal Complaint pdf Judgement pdf (via darknetlive.com at https://darknetlive.com/post/ohio-man-sentenced-to-prison-for-using-stolen-cards-to-buy-jewelry/)

Dark Web Link



Trend Micro Anti-Malware Blog

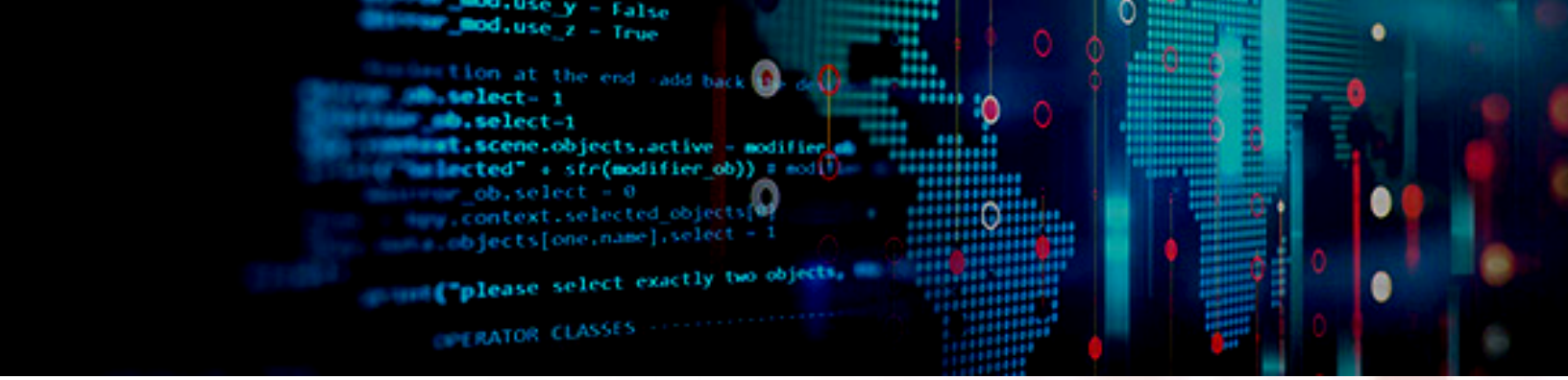
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* CVE-2022-31660 and CVE-2022-31661 (FIXED): VMware Workspace ONE Access, Identity Manager, and vRealiz
* Building Cybersecurity KPIs for Business Leaders and Stakeholders
* What We're Looking Forward to at Black Hat, DEF CON, and BSidesLV 2022
* QNAP Poisoned XML Command Injection (Silently Patched)
* [Security Nation] Curt Barnard on Defaultinator (Black Hat Arsenal Preview)
* The Future of the SOC Is XDR
* Primary Arms PII Disclosure via IDOR (FIXED)
* Collaboration Drives Secure Cloud Innovation: Insights From AWS re:Inforce
* Shift Left: Secure Your Innovation Pipeline



Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* Cisco Releases Security Updates for RV Series Routers
* F5 Releases Security Updates
* VMware Releases Security Updates
* CISA and ACSC Release Top 2021 Malware Strains
* CISA Adds One Known Exploited Vulnerability to Catalog
* CISA Releases Log4Shell-Related MAR
* Samba Releases Security Updates
* AA22-216A: 2021 Top Malware Strains
* AA22-187A: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and
* Vulnerability Summary for the Week of July 25, 2022
* Vulnerability Summary for the Week of July 18, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-5905-01

Red Hat Security Advisory 2022-5905-01 - X.Org is an open-source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon. Issues addressed include an out of bounds access vulnerability.

Red Hat Security Advisory 2022-5909-01

Red Hat Security Advisory 2022-5909-01 - Openshift Logging Bug Fix Release. Issues addressed include denial of service and out of bounds read vulnerabilities.

Red Hat Security Advisory 2022-5908-01

Red Hat Security Advisory 2022-5908-01 - Openshift Logging Bug Fix Release. Issues addressed include denial of service and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-5551-1

Ubuntu Security Notice 5551-1 - It was discovered that mod-wsgi did not correctly remove the X-Client-IP header when processing requests from untrusted proxies. A remote attacker could use this issue to pass the header to WSGI applications, contrary to expectations.

Ubuntu Security Notice USN-5550-1

Ubuntu Security Notice 5550-1 - It was discovered that GnuTLS incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. It was discovered that GnuTLS incorrectly handled the verification of certain pkcs7 signatures. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5549-1

Ubuntu Security Notice 5549-1 - It was discovered that Django incorrectly handled certain FileResponse. An attacker could possibly use this issue to expose sensitive information or gain access over user machine.

Ubuntu Security Notice USN-5546-1

Ubuntu Security Notice 5546-1 - Neil Madden discovered that OpenJDK did not properly verify ECDSA signatures. A remote attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 17 and OpenJDK 18. It was discovered that OpenJDK incorrectly limited memory when compiling a specially crafted XPath expression. An attacker could possibly use this issue to cause a denial of service. This issue was fixed in OpenJDK 8 and OpenJDK 18. USN-5388-1 and USN-5388-2 addressed this issue in OpenJDK 11 and OpenJDK 17.

Ubuntu Security Notice USN-5546-2

Ubuntu Security Notice 5546-2 - USN-5546-1 fixed vulnerabilities in OpenJDK. This update provides the corresponding updates for Ubuntu 16.04 ESM. Neil Madden discovered that OpenJDK did not properly verify ECDSA signatures. A remote attacker could possibly use this issue to insert, edit or obtain sensitive information. This issue only affected OpenJDK 17 and OpenJDK 18.

Gentoo Linux Security Advisory 202208-01

Gentoo Linux Security Advisory 202208-1 - A vulnerability in lib3mf could lead to remote code execution. Versions less than 2.1.1 are affected.

Gentoo Linux Security Advisory 202208-05

Gentoo Linux Security Advisory 202208-5 - Multiple vulnerabilities have been found in Icinga Web 2, the worst of which could result in remote code execution. Versions less than 2.9.6 are affected.

Gentoo Linux Security Advisory 202208-04

Gentoo Linux Security Advisory 202208-4 - Multiple vulnerabilities in libmcpp could result in a denial of service condition. Versions less than 2.7.2_p5 are affected.

Gentoo Linux Security Advisory 202208-03

Gentoo Linux Security Advisory 202208-3 - A vulnerability in Babel could result in remote code execution. Versions less than 2.9.1 are affected.

Gentoo Linux Security Advisory 202208-02

Gentoo Linux Security Advisory 202208-2 - Multiple vulnerabilities have been found in Go, the worst of which could result in remote code execution. Versions less than 1.18.5 are affected.

Red Hat Security Advisory 2022-5904-01

Red Hat Security Advisory 2022-5904-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2022-5903-01

Red Hat Security Advisory 2022-5903-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This asynchronous security patch is an update to Red Hat Process Automation Manager 7. Issues addressed include HTTP request smuggling, denial of service, and deserialization vulnerabilities.

Red Hat Security Advisory 2022-5892-01

Red Hat Security Advisory 2022-5892-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2022-5893-01

Red Hat Security Advisory 2022-5893-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2022-5894-01

Red Hat Security Advisory 2022-5894-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.6 is a first release for Red Hat JBoss Enterprise Application Platform 7.4 on Red Hat Enterprise Linux 9, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a deserialization vulnerability.

Ubuntu Security Notice USN-5547-1

Ubuntu Security Notice 5547-1 - Le Wu discovered that the NVIDIA graphics drivers did not properly perform input validation in some situations. A local user could use this to cause a denial of service or possibly execute arbitrary code. Tal Lossos discovered that the NVIDIA graphics drivers incorrectly handled certain memory operations, leading to a null-pointer dereference. A local attacker could use this to cause a denial of service. Artem S. Tashkinov discovered that the NVIDIA graphics drivers Dynamic Boost D-Bus component did not properly restrict access to its endpoint. When enabled in non-default configurations, a local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2022-5766-01

Red Hat Security Advisory 2022-5766-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.12.0 ESR. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-5778-01

Red Hat Security Advisory 2022-5778-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.12.0. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-5765-01

Red Hat Security Advisory 2022-5765-01 - Mozilla Firefox is an open-source web browser, designed for

standards compliance, performance, and portability. This update upgrades Firefox to version 91.12.0 ESR. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-5840-01

Red Hat Security Advisory 2022-5840-01 - The Migration Toolkit for Containers enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API.

Red Hat Security Advisory 2022-5729-01

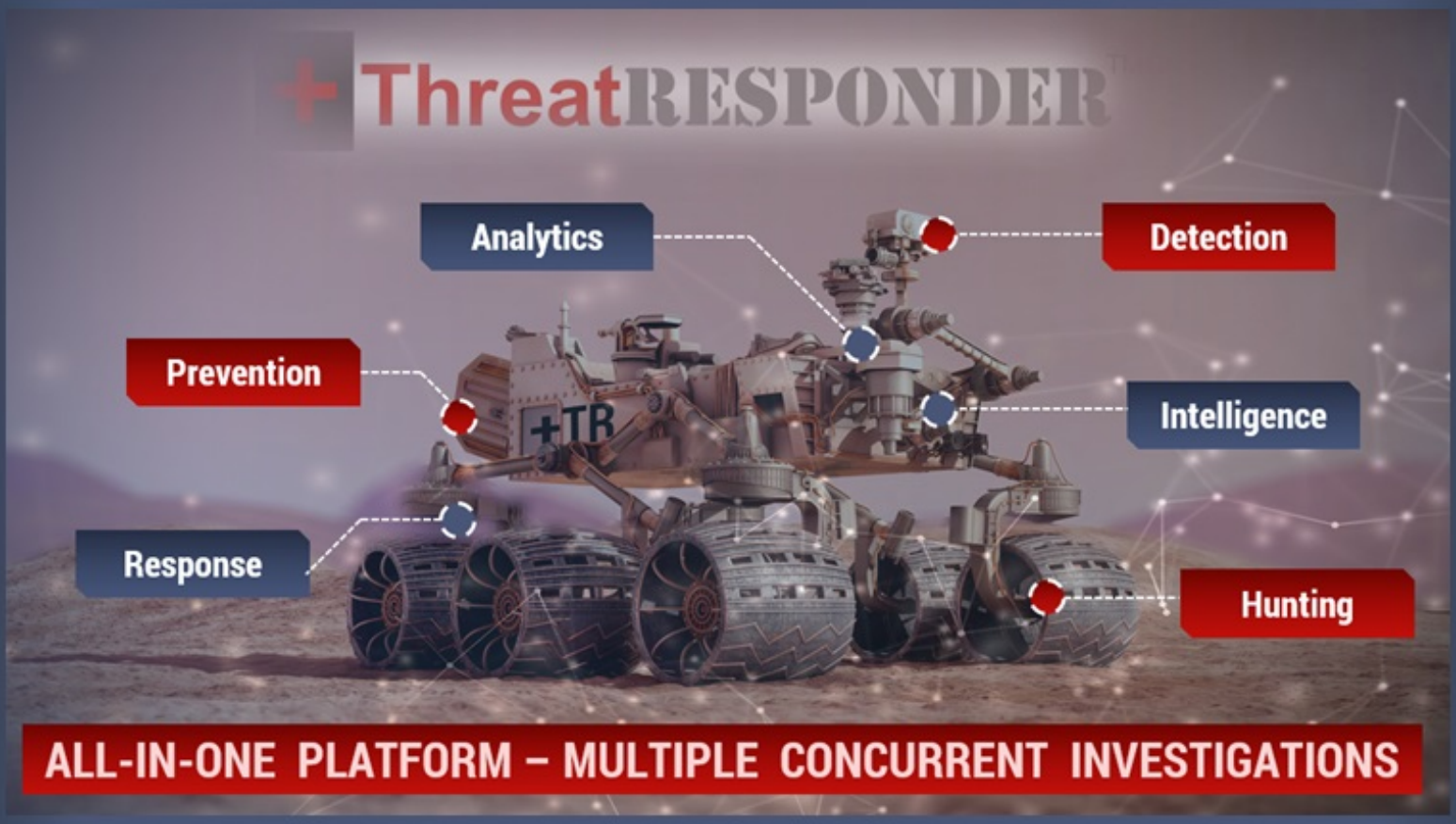
Red Hat Security Advisory 2022-5729-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.25.

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



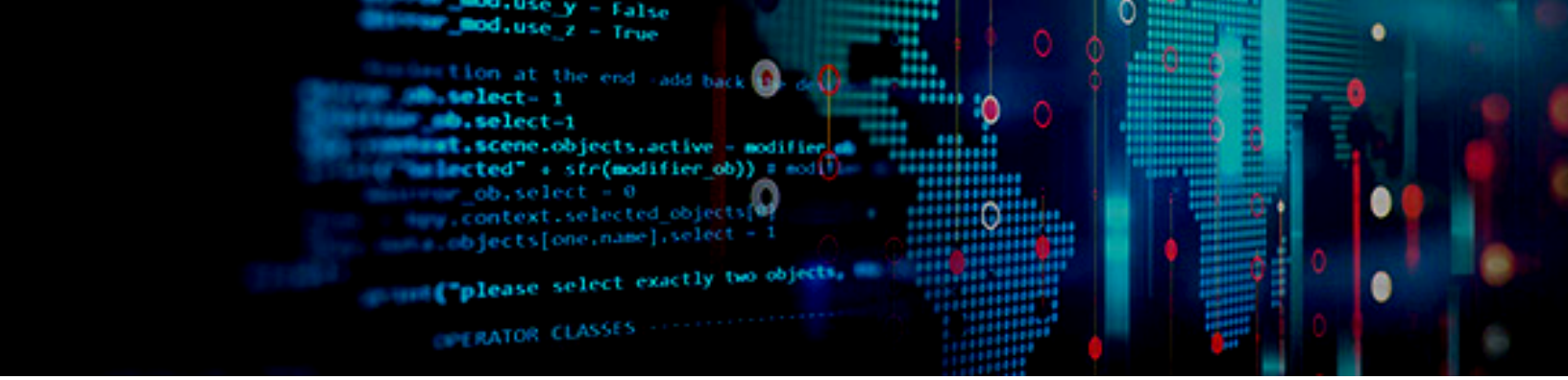
The Solution – ThreatResponder® Platform

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

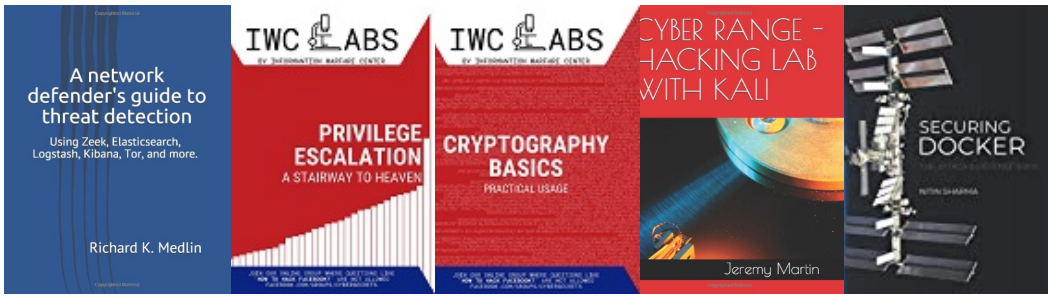


The Cyber Secrets publications on Amazon

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