Jul-18-22

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

July 18, 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

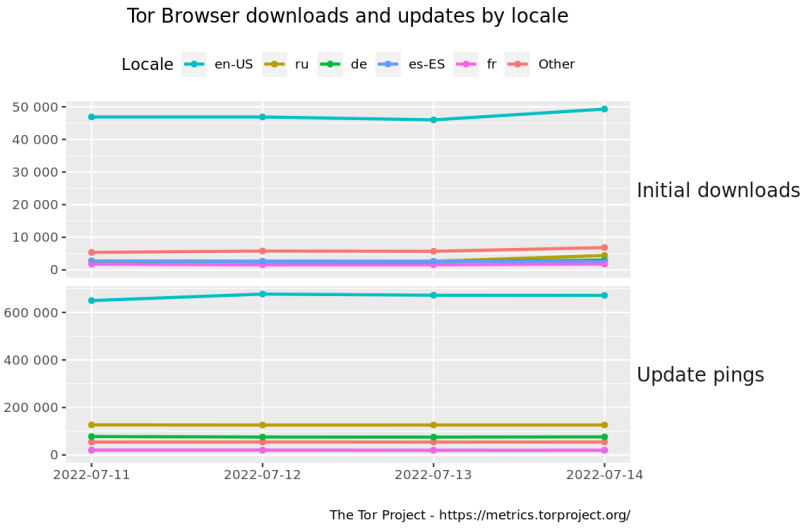
Internet Storm Center Infocon Status

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

* Windows Network File System Flaw Results In Arbitrary Code Execution As SYSTEM
* Tenet Health Sued Over Health Data Theft Impacting 1.2M
* Journalists Emerge As Favored Attack Target For APTs
* Meet Mantis, The Tiny Shrimp That Launched 3,000 DDoS Attacks
* Ex-CIA Employee Convicted Of Leaking Vault 7 Secrets To Wikileaks
* Hacking Of US Hospitals Highlights Deadly Risk Of Ransomware
* SCOTUS Judges Doxxed After Overturning Roe Versus Wade
* Amazon Handed Doorbell Cam Ring Data To US Police 11 Times So Far In 2022
* New Spectre-Type Retbleed Vulnerability Drops. Will Attackers Use It?
* Large-Scale Phishing Campaign Bypasses MFA
* Microsoft's July Patch Tuesday Fixes Actively Exploited Bug
* X.org Servers Update Closes 2 Security Holes
* Mergers And Acquisitions Put Zero Trust To The Ultimate Test
* Amazon Squashes Years-Old Authentication Bugs In AWS Kubernetes Service
* See The First Full Color Images From The Webb Space Telescope
* Who Are The Hackers Who Started A Fire In Iran?
* Apple Previews Lockdown Mode, A New Extreme Security Feature
* Hackers Say They Can Unlock And Start Honda Cars Remotely
* Microsoft Pauses Once Touted Macro Security Change
* Sneaky Orbit Malware Backdoors Linux Devices
* US Military Contractor Moves To Buy Israeli Spy-Tech Company NSO Group
* End-To-End Encryption's Central Role In Modern Self Defense
* Hack Allows Drone Takeover Via ExpressLRS Protocol
* Apple Launches Lockdown To Block Spyware
* FBI And MI5 Leaders Give Unprecedented Joint Warning On Chinese Spying

Krebs on Security

* Why 8kun Went Offline During the January 6 Hearings
* Microsoft Patch Tuesday, July 2022 Edition
* Experian, You Have Some Explaining to Do
* The Link Between AWM Proxy & the Glupteba Botnet
* Meet the Administrators of the RSOCKS Proxy Botnet
* Why Paper Receipts are Money at the Drive-Thru
* Microsoft Patch Tuesday, June 2022 Edition
* Ransomware Group Debuts Searchable Victim Data
* "Downthem" DDoS-for-Hire Boss Gets 2 Years in Prison
* Adconion Execs Plead Guilty in Federal Anti-Spam Case

Dark Reading

* Netwrix Auditor Bug Could Lead to Active Directory Domain Compromise
* What Are the Risks of Employees Going on a 'Hybrid Holiday'?
* How Attackers Could Dupe Developers into Downloading Malicious Code From GitHub
* Ex-CIA Programmer Found Guilty of Stealing Vault 7 Data, Giving It to Wikileaks
* Sandworm APT Trolls Researchers on Its Trail as It Targets Ukraine
* How Hackers Create Fake Personas for Social Engineering
* Bishop Fox Secures $75 Million in Growth Funding From Carrick Capital Partners
* DHS Review Board Deems Log4j an 'Endemic' Cyber Threat
* New Phishing Kit Hijacks WordPress Sites for PayPal Scam
* Scribe Security Releases Code Integrity Validator Alongside Github Security Open Source Project
* AEI HorizonX Ventures Joins Shift5 Series B Funding Round
* Data of Nearly 2M Patients Exposed in Ransomware Attack on Healthcare Debt Collection Firm
* Is Cryptocurrency's Crash Causing Headaches for Ransomware Gangs?
* Virtual CISOs Are the Best Defense Against Accelerating Cyber-Risks
* The Next Generation of Threat Detection Will Require Both Human and Machine Expertise
* Data Breaches Linked to Ransomware Declined in Q2 2022
* Researchers Devise New Speculative Execution Attacks Against Some Intel, AMD CPUs
* CyberRatings.org Issues AAA Rating on Forcepoint's Cloud Network Firewall
* Report: Financial Institutions Overly Complacent About Current Authentication Methods
* Mozilla: EU's eIDAS Proposal Attracts Growing Criticism

The Hacker News

* Hackers Distributing Password Cracking Tool for PLCs and HMIs to Target Industrial Systems
* Juniper Releases Patches for Critical Flaws in Junos OS and Contrail Networking
* Google Removes "App Permissions" List from Play Store for New "Data Safety" Section
* Hackers Targeting VoIP Servers By Exploiting Digium Phone Software
* New Netwrix Auditor Bug Could Let Attackers Compromise Active Directory Domain
* 5 Key Things We Learned from CISOs of Smaller Enterprises Survey
* New Cache Side Channel Attack Can De-Anonymize Targeted Online Users
* North Korean Hackers Targeting Small and Midsize Businesses with H0lyGh0st Ransomware
* Mantis Botnet Behind the Largest HTTPS DDoS Attack Targeting Cloudflare Customers
* Former CIA Engineer Convicted of Leaking 'Vault 7' Hacking Secrets to WikiLeaks
* State-Backed Hackers Targeting Journalists in Widespread Espionage Campaigns
* A Simple Formula for Getting Your IT Security Budget Approved
* Microsoft Details App Sandbox Escape Bug Impacting Apple iOS, iPadOS, macOS Devices
* Pakistani Hackers Targeting Indian Students in Latest Malware Campaign
* New 'Retbleed' Speculative Execution Attack Affects AMD and Intel CPUs

Security Week

* Supply Chain Attack Technique Spoofs GitHub Commit Metadata
* Critical Infrastructure Operators Implementing Zero Trust in OT Environments
* Powerful 'Mantis' DDoS Botnet Hits 1,000 Organizations in One Month
* Microsoft: North Korean Hackers Target SMBs With H0lyGh0st Ransomware
* Software Vendors Start Patching Retbleed CPU Vulnerabilities
* Bot Battle: The Tech That Could Decide Twitter's Musk Lawsuit
* Log4j Software Flaw 'Endemic,' New Cyber Safety Panel Says
* Two Big OT Security Concerns Related to People: Human Error and Staff Shortages
* Organizations Warned of New Lilith, RedAlert, 0mega Ransomware
* Japanese Video Game Publisher Bandai Namco Confirms Cyberattack
* Investment in IIoT/OT Security Leads to Reduced Incident Impact: Study
* Microsoft: 10,000 Organizations Targeted in Large-Scale Phishing Campaign
* Bishop Fox Lands $75 Million Series B Funding
* The Pendulum Effect and Security Automation
* CIA Coder Convicted of Massive Leak of US Hacking Tools
* Lenovo Patches UEFI Code Execution Vulnerability Affecting Many Laptops
* Retbleed: New Speculative Execution Attack Targets Intel, AMD Processors
* DLL Hijacking Flaw Fixed in Microsoft Azure Site Recovery
* Microsoft Releases Open Source Toolkit for Generating SBOMs
* Blockchain Security Startup BlockSec Raises $8 Million
* SAP Patches High-Severity Vulnerabilities in Business One Product
* Honda Admits Hackers Could Unlock Car Doors, Start Engines
* Microsoft Patch Tuesday: 84 Windows Vulns, Including Already-Exploited Zero-Day
* European Central Bank Head Targeted in Hacking Attempt
* Adobe Patch Tuesday: Critical Flaws in Acrobat, Reader, Photoshop
* ICS Patch Tuesday: Siemens, Schneider Electric Address 59 Vulnerabilities

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* New Phishing Attacks Shame, Scare Victims into Surrendering Twitter, Discord Credentials
* Ransomware Group Conti Reaches 40 Successful Attacks in a Single Month
* Phishing Attacks are the Most Prevalent Source of Identity-Related Breaches
* Facebook-Themed Scam Aims to Steal Your Credentials
* Hovering Over Links Will Protect You More Than MFA
* Watchdog Uncovers 12% of Google Ads for Student Loan Relief Could be Malicious
* QuickBooks Phishing Scam is Back
* Hacks That Bypass Multi-Factor Authentication and How to Make Your MFA Solution Phishing Resistant
* Phishing Attack Steals $8 Million Worth of Cryptocurrency
* KnowBe4's 2022 Phishing By Industry Benchmarking Report Reveals that 32.4% of Untrained End Users Wil

ISC2.org Blog

* Latest Cyberthreats and Advisories - July 15, 2022
* How I Prepared for the CISSP Exam
* CISSP Recognized as Top Cybersecurity Certification
* Hiring Managers Lead on Entry-Level Cybersecurity Job Descriptions
* #ISC2Congress: Politics, Cybersecurity & Global Issues - Ian Bremmer to Speak as (ISC)² Keynote

HackRead

* Hackers can spoof commit metadata to create false GitHub repositories
* Tiny Mantis Botnet Can Launch More Powerful DDoS Attacks Than Mirai
* CIA Whistleblower Found Guilty of Leaking Vault 7 Documents to WikiLeaks
* Uniswap V3 LPs Lose Millions in Fake Token Phishing Attack
* Ransomware attack on US healthcare debt collector exposes 1.9m patient records
* The Importance of Cybersecurity Solutions for Your Business
* Researcher Reveals How Hackers Can Remotely Unlock/Start Honda Cars

Koddos

* Hackers can spoof commit metadata to create false GitHub repositories
* Tiny Mantis Botnet Can Launch More Powerful DDoS Attacks Than Mirai
* CIA Whistleblower Found Guilty of Leaking Vault 7 Documents to WikiLeaks
* Uniswap V3 LPs Lose Millions in Fake Token Phishing Attack
* Ransomware attack on US healthcare debt collector exposes 1.9m patient records
* The Importance of Cybersecurity Solutions for Your Business
* Researcher Reveals How Hackers Can Remotely Unlock/Start Honda Cars

Naked Security

* 7 cybersecurity tips for your summer vacation!
* S3 Ep91: CodeRed, OpenSSL, Java bugs and Office macros [Podcast + Transcript]
* Facebook 2FA scammers return - this time in just 21 minutes
* Paying ransomware crooks won't reduce your legal risk, warns regulator
* That didn't last! Microsoft turns off the Office security it just turned on
* Apache "Commons Configuration" patches Log4Shell-style bug - what you need to know
* S3 Ep90: Chrome 0-day again, True Cybercrime, and a 2FA bypass [Podcast + Transcript]
* OpenSSL fixes two "one-liner" crypto bugs - what you need to know
* Google patches "in-the-wild" Chrome zero-day - update now!
* Canadian cybercriminal pleads guilty to "NetWalker" attacks in US

Threat Post

* Emerging H0lyGh0st Ransomware Tied to North Korea
* Journalists Emerge as Favored Attack Target for APTs
* Large-Scale Phishing Campaign Bypasses MFA
* How War Impacts Cyber Insurance
* 'Callback' Phishing Campaign Impersonates Security Firms
* Rethinking Vulnerability Management in a Heightened Threat Landscape
* Popular NFT Marketplace Phished for $540M
* Sneaky Orbit Malware Backdoors Linux Devices
* U.S. Healthcare Orgs Targeted with Maui Ransomware
* Hack Allows Drone Takeover Via 'ExpressLRS' Protocol

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

* Open source isn't working for AI
* 7 reasons Java is still great
* Securing data at rest and data in motion
* GitHub Copilot users feel more productive
* So why did they decide to call it Java?
* The next frontier in cloud computing
* Go language revises memory model
* What is Google JAX? NumPy on accelerators
* Rocky Linux 9.0 rocks new build system
* StarRocks launches managed DBaaS for real-time analytics

C4ISRNET - Media for the Intelligence Age Military

* General Atomics to deliver integrated ISR analytics suite to Japan this fall
* Boeing applying lessons learned from Air Force One contract, defense CEO says
* 'Space is where we need to go': US Air Force preparing networked infrastructure for new mission
* US Air Force says options limited for speeding deliveries of Wedgetail
* Lockheed working on expendable, advanced drones to team up with Air Force fighters
* US Air Force looking to Europe for commercial technologies, official says
* Pentagon goes public to fill Defense Innovation Unit post amid pressure from Congress
* Pentagon AI roadmap seen helping build warfighter, public trust
* Troops' use of TikTok may be national security threat, FCC commissioner says
* Homeland Security, Justice officials urge Congress to expand counter-drone authority

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.

* BDSec CTF 2022
* DiceCTF @ Hope
* Lexington Informatics Tournament CTF 2022
* MCH2022 CTF
* 3kCTF-2022(POSTPONED)
* RED CTF(POSTOPNDED)
* TFC CTF 2022
* UIUCTF 2022
* Aero CTF 2022
* hackrocks Cyber Summer Camp

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

* Suricata IDPE 6.0.6
* GNU Privacy Guard 2.3.7
* GNU Privacy Guard 2.2.36
* Falco 0.32.1
* Zeek 5.0.0
* OpenSSL Toolkit 3.0.5
* OpenSSL Toolkit 1.1.1q
* TripleCross Linux eBPF Rootkit
* C Language Reverse Shell Generator
* Global Socket 1.4.37

Kali Linux Tutorials

* AWS-Threat-Simulation-and-Detection : Playing Around With Stratus Red Team And SumoLogic
* Lockc : Making Containers More Secure With eBPF And Linux Security Modules (LSM)
* Puwr : SSH Pivoting Script For Expanding Attack Surfaces On Local Networks
* Atomic-Operator : A Python Package Is Used To Execute Atomic Red Team Tests
* COM-Hunter : COM Hijacking VOODOO
* CRLFsuite : Fast CRLF Injection Scanning Tool
* Cybersecurity in No-Code platforms: Key Principles
* SMB-Session-Spoofing : Tool To Create A Fake SMB Session
* Notionterm : Embed Reverse Shell In Notion Pages
* Zap-Scripts : Zed Attack Proxy Scripts For Finding CVEs And Secrets

GBHackers Analysis

* VMware vCenter Server Flaw Let Attacker Exploit to Perform Elevate Privileges Attack
* Critical Fortinet Flaws Patched - Following Products Affected
* Kids and Teens Forming Hacking Groups Online to Exchange Malware
* Critical PHP Flaws Allows Attackers to Execute Remote Code on QNAP NAS Devices
* Critical Flaws in MEGA Cloud Storage Let Attacker Decrypt User Data

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

* 5 Reasons Hackers Want Your Accounts
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* How to Track Down Hidden Cameras with Wireshark

The PC Security Channel [TPSC]

* YouTube Stealer: Hackers target gaming YouTubers
* Malwarebytes: Test vs Ransomware

Eli the Computer Guy

* eBeggar Wednesday - TWITTER SUES ELON MUSK for BEING AN ASS
* What is Networking Equipment
* What is a Firewall
* eBeggar Wednesday - Louis Rossmann YOUTUBE CHANNEL is DEAD (young man gets old)

Security Now

* The Rolling Pwn - OpenSSL patch, iOS Lockdown Mode, Yubikey's to Ukraine, Office Macros re-enabled
* The ZuoRAT - 0-Day Chrome, Firefox v102, HackerOne

Troy Hunt

* Weekly Update 304

Intel Techniques: The Privacy, Security, & OSINT Show

* 270-OSINT Tool Updates
* 269-New OSINT Tools & Breach Data Lessons

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Windows Kernel nt!MiRelocateImage Invalid Read
* Windows LSA Service LsapGetClientInfo Impersonation Level Check Privilege Escalation
* PrestaShop 1.7.6.7 Cross Site Scripting
* Sourcegraph gitserver sshCommand Remote Command Execution
* JBOSS EAP/AS 6.x Remote Code Execution
* WordPress Visual Slide Box Builder 3.2.9 SQL Injection
* Sashimi Evil OctoBot Tentacle
* Nginx 1.20.0 Denial Of Service
* Chrome PaintImage Deserialization Out-Of-Bounds Read
* Xen TLB Flush Bypass
* Mutt mutt_decode_uuencoded() Memory Disclosure
* Windows Kerberos KerbRetrieveEncodedTicketMessage AppContainer Privilege Escalation
* Windows Kerberos Redirected Logon Buffer Privilege Escalation
* Xen PV Guest Non-SELFSNOOP CPU Memory Corruption
* EQS Integrity Line Cross Site Scripting / Information Disclosure
* Magnolia CMS 6.2.19 Cross Site Scripting
* Ransom Lockbit 3.0 MVID-2022-0621 Code Execution
* Advanced Testimonials Manager 5.6 SQL Injection
* Windows Defender Remote Credential Guard Authentication Relay Privilege Escalation
* Ransom Lockbit 3.0 MVID-2022-0620 Buffer Overflow
* DouPHP 1.2 Release 20141027 SQL Injection
* Paymoney 3.3 Cross Site Scripting
* Stock Management System 2020 SQL Injection
* Packet Storm New Exploits For June, 2022
* Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal

CXSecurity

* Sourcegraph gitserver sshCommand Remote Command Execution
* JBOSS EAP/AS 6.x Remote Code Execution
* Exploit mktba 4.2 Arbitrary File Upload
* WiFi Mouse 1.7.8.5 Remote Code Execution
* Kitty 0.76.0.8 Stack Buffer Overflow
* phpIPAM 1.4.5 Remote Code Execution
* Pandora FMS 7.0NG.742 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

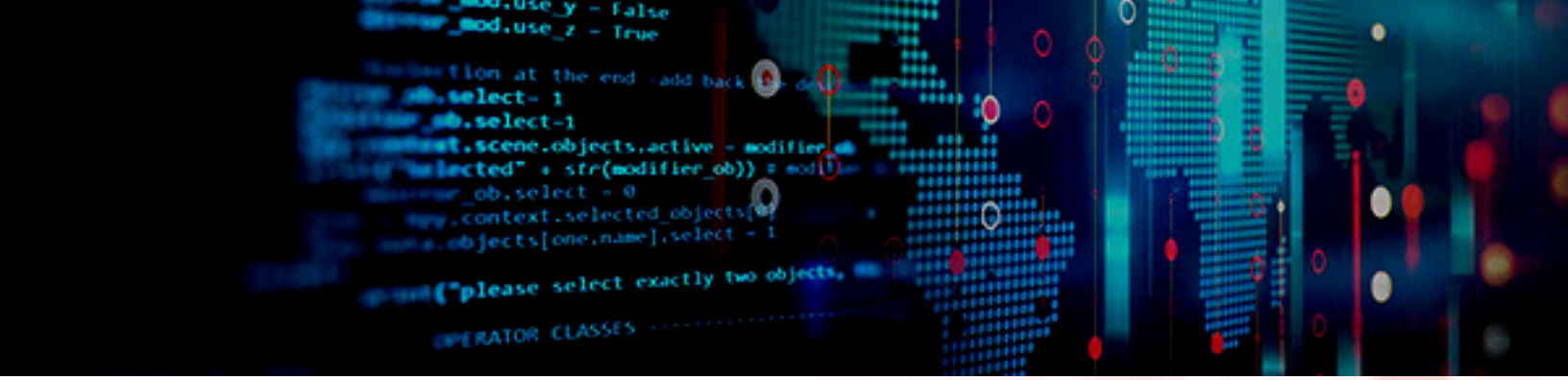
* [remote] Nginx 1.20.0 - Denial of Service (DOS)
* [remote] WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)
* [webapps] Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)
* [webapps] WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scriptin
* [webapps] WordPress Plugin Weblizar 8.9 - Backdoor
* [webapps] SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)
* [webapps] SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)
* [webapps] Old Age Home Management System 1.0 - SQLi Authentication Bypass
* [webapps] ChurchCRM 4.4.5 - SQLi
* [remote] Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)
* [webapps] phpIPAM 1.4.5 - Remote Code Execution (RCE) (Authenticated)
* [remote] TP-Link Router AX50 firmware 210730 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Pandora FMS v7.0NG.742 - Remote Code Execution (RCE) (Authenticated)
* [remote] Algo 8028 Control Panel - Remote Code Execution (RCE) (Authenticated)
* [local] HP LaserJet Professional M1210 MFP Series Receive Fax Service - Unquoted Service Path
* [remote] Virtua Software Cobranca 12S - SQLi
* [remote] Marval MSM v14.19.0.12476 - Cross-Site Request Forgery (CSRF)
* [remote] Marval MSM v14.19.0.12476 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Avantune Genialcloud ProJ 10 - Cross-Site Scripting (XSS)
* [local] Real Player 16.0.3.51 - 'external::Import()' Directory Traversal to Remote Code Execution (RC
* [local] Real Player v.20.0.8.310 G2 Control - 'DoGoToURL()' Remote Code Execution (RCE)
* [webapps] Confluence Data Center 7.18.0 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)

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*

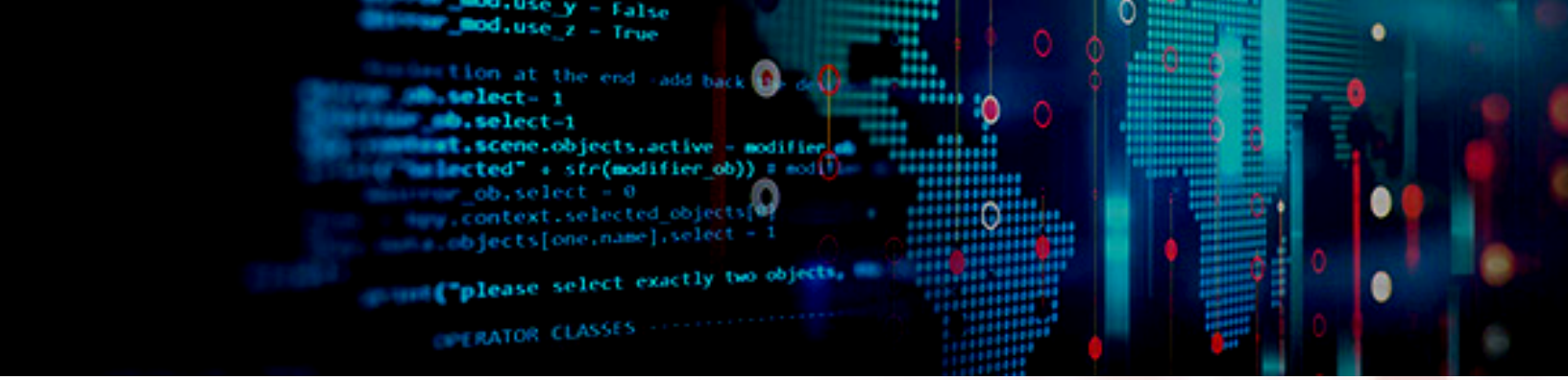
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://klongtabchan.go.th/index.php
http://klongtabchan.go.th/index.php notified by Mrj Haxcore
http://khokmamuang.go.th/index.php
http://khokmamuang.go.th/index.php notified by Mrj Haxcore
http://www.khokkung.go.th/index.php
http://www.khokkung.go.th/index.php notified by Mrj Haxcore
http://www.dontanin.go.th/index.php
http://www.dontanin.go.th/index.php notified by Mrj Haxcore
http://mamujutengahkab.go.id/readme.htm
http://mamujutengahkab.go.id/readme.htm notified by Mr.L3RB1
http://www.savarmunicipality.gov.bd/back.txt
http://www.savarmunicipality.gov.bd/back.txt notified by Illusion Silent Killer
http://www.srapra.go.th/index.php
http://www.srapra.go.th/index.php notified by ./Niz4r
http://www.sampanieng.go.th/index.php
http://www.sampanieng.go.th/index.php notified by ./Niz4r
http://www.sakot.go.th/index.php
http://www.sakot.go.th/index.php notified by ./Niz4r
http://www.soengsanglocal.go.th/index.php
http://www.soengsanglocal.go.th/index.php notified by ./Niz4r
http://sistemperencanaan.boltimkab.go.id/read.txt
http://sistemperencanaan.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://bappelitbang.boltimkab.go.id/read.txt
http://bappelitbang.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://bappeda.boltimkab.go.id/read.txt
http://bappeda.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://webdinas.boltimkab.go.id/read.txt
http://webdinas.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://testing.boltimkab.go.id/read.txt
http://testing.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://satpolppkar.boltimkab.go.id/read.txt
http://satpolppkar.boltimkab.go.id/read.txt notified by Mr.L3RB1
http://ppid.boltimkab.go.id/read.txt
http://ppid.boltimkab.go.id/read.txt notified by Mr.L3RB1



Dark Web News

Darknet Live

Chainalysis: Cryptocurrency Mixer Use at an All-Time High

Cryptocurrency mixer use has reached an all-time high in 2022, according to a report from the blockchain analysis firm Chainalysis. __ Mixers may soon become obsolete as Chainalysis continues to refine the ability to demix certain mixing transactions and see users' original source of funds. Chainalysis, a member of the World Economic Forum's (WEF) Global Innovators community, is a leader in the blockchain analytics industry. The company is an extension of governments, providing services to law enforcement agencies and hiring former feds and FinCEN employees. Mixers are receiving record amounts of cryptocurrency in 2022, according to a Chainalysis report published on July 14, 2022. On April 19, 2022, mixers received "an all-time high of $51.8 million worth of cryptocurrency.” A chart provided by Chainalysis reveals that mixers received roughly $24 million worth of cryptocurrency on the same day in 2021. __ "Are Mixers Compliant?” _ In the report, Chainalysis laments that mixers are legal "despite their utility for criminals.” FinCEN, the Financial Crimes Enforcement Network, clarified in 2020 that cryptocurrency mixers are considered money transmitters under the Bank Secrecy Act (BSA) and must comply with the same regulations as other money transmitters. These regulations include maintaining an anti-money laundering compliance program and following "Know Your Customer” (KYC) rules for Money Services Businesses (MSBs). "Given that increased privacy is the whole point of using a mixer, it seems unlikely that one could implement those compliance procedures and retain its user base. " Types of Transactions _ So far, in 2022, 23% of funds sent to mixers came from a cryptocurrency address associated with illicit activity. Illicit transactions accounted for just 12% of mixer activity in 2021. Chainalysis tracked several categories of illicit activity. Terrorism financing Stolen Funds Scam Sanctions Ransomware Cybercriminal administrator Fraud shop Darknet market Child sex abuse material "What stands out most is the huge volume of funds moving to mixers from addresses associated with sanctioned entities, especially in Q2 2022.” In April 2022 (Q2), the U.S. Treasury's Office of Foreign Assets Control (OFAC) sanctioned Hydra Market. Transactions from addresses linked to Hydra Market accounted for 50.4% of all funds moving to mixers from sanctioned entities in 2022. __ Lazarus Group is a hacking group purportedly connected to the Democratic People's Republic of Korea (DPRK). In 2022, Lazarus Group hackers stole roughly $1 billion in cryptocurrency from DeFi projects. Funds sent from addresses associated with the Lazarus Group and Blender.io accounted for nearly all of the remaining transactions in the same category. __ Blender.io is the first cryptocurrency mixer sanctioned by OFAC. OFAC sanctioned the mixer for allegedly processing $20.5 million in stolen cryptocurrency, some of which came from the Lazarus Group. "Balancing privacy with safety.” _ Chainalysis, which is a neutral source when it comes to discussions about financial privacy, believes that mixers "present a difficult question” to "members of the cryptocurrency community.” "Virtually everyone would acknowledge that financial privacy is valuable, and that in a vacuum, there's no reason services like mixers shouldn't be able to provide it. However, the data shows that mixers currently pose a significant money laundering risk…” Mixer Usage Reaches All-time Highs in 2022 With Nation State Actors and Cybercriminals Contributing Significant Volume | archive.is, archive.org, chainalysis.com (via

darknetlive.com at https://darknetlive.com/post/chainalysis-report-about-mixer-use-increasing/)

Adderall Vendor "addy4cheap" Sentenced to 52 Months in Prison

A drug dealer who sold counterfeit Adderall pills on the darkweb under the username "addy4cheap” was sentenced to 52 months in prison. According to an announcement from the U.S. Attorney's Office for the Eastern District of Virginia, a District Court judge sentenced Tyler Pham, 39, to 52 months in prison for conspiring to distribute between 15 and 45 kilograms of pills containing methamphetamine.

Tyler Pham Court documents revealed that Pham and six co-conspirators sold counterfeit Adderall pills on the darkweb from May 2019 through December 2019. Investigators linked Pham to a vendor account under the username "addy4cheap.” Addy4cheap had profiles on Empire Market and Cryptonia Market, among others. As of December 10, 2019, addy4cheap had completed 3,665 transactions on Empire and 140 transactions on Cryptonia. Based on an analysis of addy4cheap's reviews on Empire Market, investigators believe Pham received approximately $482,572.10 in sales for about 44,872 pills. Between August 2019 and December 2019, investigators conducted 20 controlled purchases from Pham's vendor accounts on Empire and Cryptonia. In total, law enforcement officers received 767 fake Adderall pills from addy4cheap. The pills weighed approximately 268 grams in total.

Feds stocked up on methamphetamine during the investigation. The investigation into addy4cheap, according to an affidavit in support of a criminal complaint and arrest warrant, began in August 2019 after law enforcement officers intercepted a package of fake Adderall pills. Investigators interviewed the intended recipient of the package. "The individual stated that he had on multiple occasions purchased Adderall through a [darknet market] known as the Empire Market from a vendor using the moniker addy4cheap. He did not think that the pills that hid were pharmaceutical grade as he had a prescription for Adderall and the tablets from addy4cheap were different from those that he had been prescribed. The individual stated that he received the tablets via U.S. Mail and that the retum address on the packages from addy4cheap was in Fairfax, Virginia. The individual provided agents with the tracking number from his most recent purchase from addy4cheap on the Empire Market.” Investigators observed several negative reviews left by addy4cheap's customers on Empire Market. Some examples of the negative reviews are as follows: "Tested positive for meth with simon a/b test”; "Not Adderall. Pressed pills. Tested positive for meth”; "Dishonest vendor. Says its authentic adderall and sends meth and sugar pressed into an "Adderall” shape. I Took this to study and ended up not sleeping for two days. It sucked. Do not buy”, and "I tested the pills, and they contain meth. I was pretty upset since he advertised them as 100% authentic. I messaged him, and he mid the most he could offer me was a 15% dimount. Just beware buyer these are Meth pills.” Law enforcement officers conducted undercover purchases from addy4cheap from late August 2019 through November 27, 2019. During the investigation, law enforcement officers observed Pham and his co-conspirators mailing packages that resembled the packages shipped by addy4cheap. After receiving the pills, analysts tested the pills and confirmed the presence of methamphetamine. In September 2019, law enforcement officers at the Ronald Reagan Washington National Airport contacted investigators about Pham. During a search of passengers, a K-9 unit purportedly hit on a piece of Pham's luggage that contained $30,000 in cash. Law enforcement seized the money. On December 9, 2019, feds raided Pham's house and the residences of Pham's co-conspirators. The search team found roughly 200 counterfeit Adderall pills in Pham's house that resembled those sold by addy4cheap. In one co-conspirator's residence, "investigators found over 6,000 peach tablets weighing approximately 2.2 kilograms which resemble those advertised on "addy4cheap” vendor pages and those received by law enforcement through controlled purchases.” In the same residence, officers found multiple envelopes, bags, raisin boxes, printers, and other materials consistent with the packaging materials used by addy4cheap" Approximately 400 grams of MDMA tablets, marijuana, vape cartridges, a money-counting machine, and U.S. currency were also found. After Pham's arrest in 2019, a judge signed off on a personal recognizance bond, allowing Pham to avoid pre-trial detention. Pham then fled to Vietnam in an attempt to avoid prosecution. The Vietnamese Ministry of Public Security returned Pham to U.S. authorities on November 16, 2021.

Pham appeared on a 'wanted by the FBI' poster. In April 2022, Pham pleaded guilty to Conspiracy to Distribute Controlled Substances. Pham's co-conspirators pleaded

guilty to charges related to the conspiracy and were sentenced to over 13 years in prison combined. A U.S. District Judge sentenced Pham to 52 months in prison on July 12, 2022. Man Sentenced for Conspiracy to Distribute Meth on the Darknet | archive.is, archive.org, justice.gov complaint pdf judgement pdf (via darknetlive.com at https://darknetlive.com/post/virginia-man-sentenced-for-selling-meth-on-darkweb/)

Bulgarian Customs Seized 200 Packages of Drugs in Ten Days

Bulgarian customs officers intercepted 198 packages of illegal drugs in ten days. According to an announcement from Bulgarian customs, customs officers intercepted 120 packages of illegal substances between June 7, 2022, and June 17, 2022. Officers seized Tramadol, Oxycodone, Fentanyl, and Diazepam, among others. The packages contained approximately 120,000 pills and 40 kilograms of Khat.

A map of the intended destinations of packages intercepted by police. The seizures were a part of a "specialized operation against drug trafficking via the darknet,” according to the announcement. Customs officers from a drug trafficking department of the Territorial Directorate (TD) Sofia Customs worked with the United States Drug Enforcement Administration during the operation. "During the operation, the customs officers carried out numerous operational and search activities, as a result of which they intercepted and prevented the dispatch of 198 shipments to various destinations abroad.” Based on the limited information in the announcement, it appears as if law enforcement officers primarily intercepted outgoing packages. Investigators determined that the contents of the packages - small quantities of pills or other substances - were "negotiated through Darknet platforms.” Suppliers in Bulgaria then prepared the drugs for shipment and mailed the packages to customers in the "USA, Europe, and Australia.”

Law enforcement officers disrupted three drug trafficking networks and dismantled one facility used by drug traffickers to prepare drugs for shipping. The Sofia City Prosecutor's Office has already initiated four pre-trial proceedings due to the interceptions. Officers have also executed search warrants at homes, offices, and warehouses in Sofia and Lovech. Four pre-trial proceedings have already been initiated in the cases, and investigations are ongoing. Numerous searches and seizures have been carried out in homes, offices, and warehouses in Sofia and Lovech.

Customs officers seized lorazepam pills during the operation. Police arrested one person and charged him with smuggling narcotics. Investigations into other suspects are ongoing. 200 пратки с наркотици, пласирани чрез Darknet, задържаха митнически служители при операция Web Thunder | archive.org, archive.is, customs.bg Pictuer quality here is so rough because the pictures are stills from this low-res YouTube video: https://www.youtube.com/watch?v=ofJHkRnqYAU&feature=youtu.be or via invidius: https://inv.riverside.rocks/watch?v=ofJHkRnqYAU (via darknetlive.com at https://darknetlive.com/post/bulgarian-customs-seized-200-darkweb-packages/)

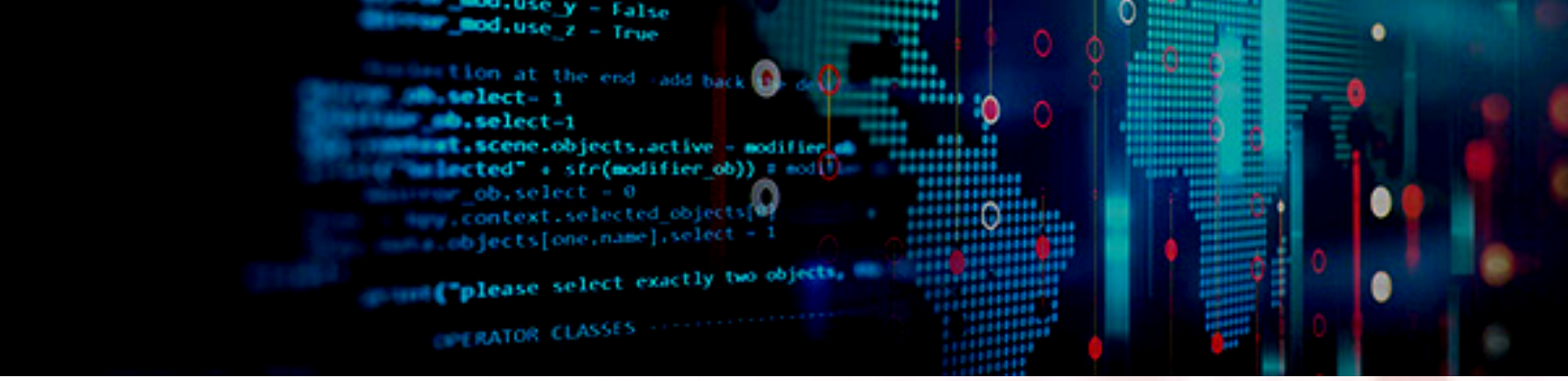
Ohio Man Sentenced for Buying Jewelry with Stolen Credit Cards

Fraudster sentenced to prison for more than six years for buying stolen credit cards on the darkweb and using them to buy jewelry. U.S. District Judge Sara Lioi sentenced Hasan Howard, 23, of Cleveland, Ohio, to more than six years in prison for various fraud charges. The judge also ordered Howard to pay $261,319.28 in restitution. In March 2022, Howard pleaded guilty to conspiracy to commit access device fraud, access device fraud, and aggravated identity theft.

Hasan Howard aka @Bigghasan on Instagram and Twitter. According to an announcement from the U.S. Attorney's Office for the Northern District of Ohio, Howard and his co-defendants, including Robert Nathaniel Andre Thomas, Tyvione Guthery, and Jaelen D. Lattimore, purchased stolen financial information on the darkweb, including credit card numbers and debit card numbers. Howard created fraudulent credit cards by embossing cards with the stolen information purchased on the darkweb. Then Howard and his co-conspirators would purchase expensive merchandise, including jewelry and watches. In a criminal complaint, an FBI Special Agent wrote that

investigators had learned that Howard had a "Joker's Stash” account. Is that a Honda Accord? In one example provided by the Attorney's Office, Howard, Guthery, and Lattimore purchased a Rolex watch for $19,062 from a jewelry store in Westlake, Ohio. They paid for the watch with a fraudulent credit card. In another example, Howard used a fraudulent credit card to purchase four diamond and gold bracelets from a jewelry store in Canton, Ohio, worth $26,463. The FBI obtained search warrants for Howard's Instagram accouts. The criminal complaint described one interaction with law enforcement and one of Howard's co-conspirators: "On or about January 6, 2021, a fraudulent transaction was reported at Sheiban Jewelers, 16938 Pearl Road, Strongsville, Ohio, belonging to victim J.M (real name known to affiant) for a total loss of $14,500. The fraudulent transaction took place on or about December 19, 2020, in which the store received a call from GUTHERY who stated that he would come to the store on the same date to make a purchase of a Rolex Yacht-Master watch.” "When GUTHERY arrived, he presented his driver's license to the employee and provided a credit card for a layaway amount of $7,000. GUTHERY then left the store but returned later with HOWARD; video surveillance shows both GUTHERY and HOWARD entering the store. When GUTHERY and HOWARD returned to the store, they paid the full amount and received the Rolex watch.” "Surveillance video also captured a Lexus G350 driven by GUTHERY, which was registered to PARRISH. On January 1, 2021, Strongsville Police Department Patrolman John Murphy spoke to GUTHERY on a phone call; the call was recorded. During the conversation, GUTHERY admitted that he was the one who drove to HOWARD in PARRISH's car to the jewelry store. GUTHERY identified the other male as his cousin HASAN (HOWARD). GUTHERY stated that HOWARD provided GUTHERY with the credit cards and billing address of the victim to GUTHERY. GUTHERY stated that HOWARD also provided PARRISH with stolen credit card information that PARRISH used at a BMW dealership to repair her vehicle in Willoughby Hills, Ohio.” On May 20, 2021, police arrested Howard and Lattimore after they had purchased more than $20,000 worth of jewelry from jewelers in Aurora, Ohio. Police found an embossing machine and three Rolex watches in Howard's possession. Howard and his co-conspirators used stolen credit card information to purchase merchandise at 30 stores, causing $261,319.28 in damages. Cleveland Man Sentenced to Prison for Leading Conspiracy that Purchased Thousands Worth of Jewelry Using Stolen Financial Information | archive.is, archive.org, justice.gov complaint pdf (via darknetlive.com at https://darknetlive.com/post/ohio-man-sentenced-for-buying-jewelry-with-stolen-cards/)

Dark Web Link



Trend Micro Anti-Malware Blog

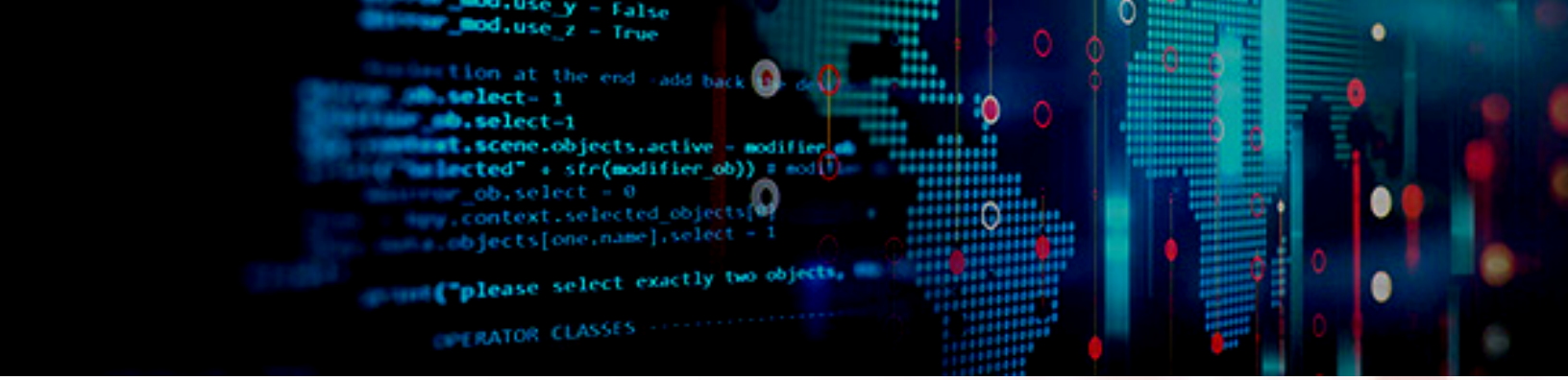
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

Unfortunately, at the time of this report, the RiskIQ resource was not availible.

FireEye

* Metasploit Weekly Wrap-Up
* InsightVM Release Update: Let's Focus on Remediation for Just a Minute
* It's the Summer of AppSec: Q2 Improvements to Our Industry-Leading DAST and WAAP
* Creating an Exceptional Workplace: Building and Expansion in a Post-COVID World
* Patch Tuesday - July 2022
* The Forecast Is Flipped: Flipping L&D to Ensure Continuous Growth
* 3 Key Challenges for Cloud Identity and Access Management
* Rapid7 MDR Reduced Breaches by 90% via Greater Efficiency to Detect, Investigate, Respond to, and Rem
* Metasploit Weekly Wrap-Up
* Today's SOC Strategies Will Soon Be Inadequate



Advisories

US-Cert Alerts & bulletins

* Juniper Networks Releases Security Updates for Multiple Products
* Adobe Releases Security Updates for Multiple Products
* Microsoft Releases July 2022 Security Updates
* SAP Releases July 2022 Security Updates
* Citrix Releases Security Updates for Hypervisor
* CISA Adds One Known Exploited Vulnerability to Catalog
* Cisco Releases Security Updates for Multiple Products
* OpenSSL Releases Security Update
* AA22-187A: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and
* AA22-181A: #StopRansomware: MedusaLocker
* Vulnerability Summary for the Week of July 4, 2022
* Vulnerability Summary for the Week of June 27, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5520-1

Ubuntu Security Notice 5520-1 - It was discovered that HTTP-Daemon incorrectly handled certain crafted requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Ubuntu Security Notice USN-5518-1

Ubuntu Security Notice 5518-1 - It was discovered that the eBPF implementation in the Linux kernel did not properly prevent writes to kernel objects in BPF_BTF_LOAD commands. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the Marvell NFC device driver implementation in the Linux kernel did not properly perform memory cleanup operations in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5517-1

Ubuntu Security Notice 5517-1 - It was discovered that the Atheros ath9k wireless device driver in the Linux kernel did not properly handle some error conditions, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the virtio RPMSG bus driver in the Linux kernel contained a double-free vulnerability in certain error conditions. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-5516-1

Ubuntu Security Notice 5516-1 - It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution.

Ubuntu Security Notice USN-5515-1

Ubuntu Security Notice 5515-1 - Eric Biederman discovered that the cgroup process migration implementation in the Linux kernel did not perform permission checks correctly in some situations. A local attacker could possibly use this to gain administrative privileges. Jann Horn discovered that the FUSE file system in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5514-1

Ubuntu Security Notice 5514-1 - It was discovered that the implementation of the 6pack and mkiss protocols in the Linux kernel did not handle detach events properly in some situations, leading to a use-after-free vulnerability. A local attacker could possibly use this to cause a denial of service. Duoming Zhou discovered that the AX.25 amateur radio protocol implementation in the Linux kernel did not handle detach events properly in some situations. A local attacker could possibly use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5513-1

Ubuntu Security Notice 5513-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Likang Luo discovered that a race condition existed in the Bluetooth subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5473-2

Ubuntu Security Notice 5473-2 - USN-5473-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 16.04 ESM. The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.50 version of the Mozilla certificate authority bundle.

Ubuntu Security Notice USN-5511-1

Ubuntu Security Notice 5511-1 - Carlo Marcelo Arenas Belon discovered that an issue related to CVE-2022-24765 still affected Git. An attacker could possibly use this issue to run arbitrary commands as administrator.

WordPress Kaswara Modern WPBakery Page Builder 3.0.1 File Upload

WordPress Kaswara Modern WPBakery Page Builder plugin versions 3.0.1 and below suffer from an arbitrary file upload vulnerability.

Ubuntu Security Notice USN-5256-1

Ubuntu Security Notice 5256-1 - It was discovered that uriparser incorrectly handled certain memory operations. An attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5510-2

Ubuntu Security Notice 5510-2 - USN-5510-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 ESM. Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Ubuntu Security Notice USN-5510-1

Ubuntu Security Notice 5510-1 - Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Ubuntu Security Notice USN-5503-2

Ubuntu Security Notice 5503-2 - USN-5503-1 fixed a vulnerability in GnuPG. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Demi Marie Obenour discovered that GnuPG incorrectly handled injection in the status message. A remote attacker could possibly use this issue to forge signatures.

Ubuntu Security Notice USN-5508-1

Ubuntu Security Notice 5508-1 - It was discovered that Python LDAP incorrectly handled certain regular expressions. An remote attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5509-1

Ubuntu Security Notice 5509-1 - Julian Brook discovered that Dovecot incorrectly handled multiple passdb configuration entries. In certain configurations, a remote attacker could possibly use this issue to escalate privileges.

VMware Security Advisory 2022-0025.2

VMware Security Advisory 2022-0025.2 - VMware vCenter Server updates address a privilege escalation vulnerability.

VMware Security Advisory 2022-0020

VMware Security Advisory 2022-0020 - VMware ESXi addresses return-stack-buffer-underflow and branch type confusion vulnerabilities.

VMware Security Advisory 2022-0018

VMware Security Advisory 2022-0018 - VMware vCenter Server updates address a server-side request forgery vulnerability.

Ubuntu Security Notice USN-5507-1

Ubuntu Security Notice 5507-1 - It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the program to crash, use unexpected values, or execute arbitrary code. It was discovered that Vim incorrectly handled memory access. An attacker could potentially use this issue to cause the corruption of sensitive information, a crash, or arbitrary code execution.

Ubuntu Security Notice USN-5479-3

Ubuntu Security Notice 5479-3 - USN-5479-1 fixed vulnerabilities in PHP. Unfortunately that update for CVE-2022-31625 was incomplete for Ubuntu 18.04 LTS. This update fixes the problem. Charles Fol discovered that PHP incorrectly handled initializing certain arrays when handling the pg_query_params function. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code. Charles Fol discovered that PHP incorrectly handled passwords in mysqlnd. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5506-1

Ubuntu Security Notice 5506-1 - Tavis Ormandy discovered that NSS incorrectly handled an empty pkcs7 sequence. A remote attacker could possibly use this issue to cause NSS to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10. Ronald Crane discovered that NSS incorrectly handled certain memory operations. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Dovecot IMAP Server 2.2 Improper Access Control

Dovecot IMAP server version 2.2 suffers from a privilege escalation vulnerability. When two passdb configuration entries exist in the Dovecot configuration, which have the same driver and args settings, the incorrect username_filter and mechanism settings can be applied to passdb definitions. These incorrectly applied settings can lead to an unintended security configuration and can permit privilege escalation with certain configurations involving master user authentication.

Ubuntu Security Notice USN-5505-1

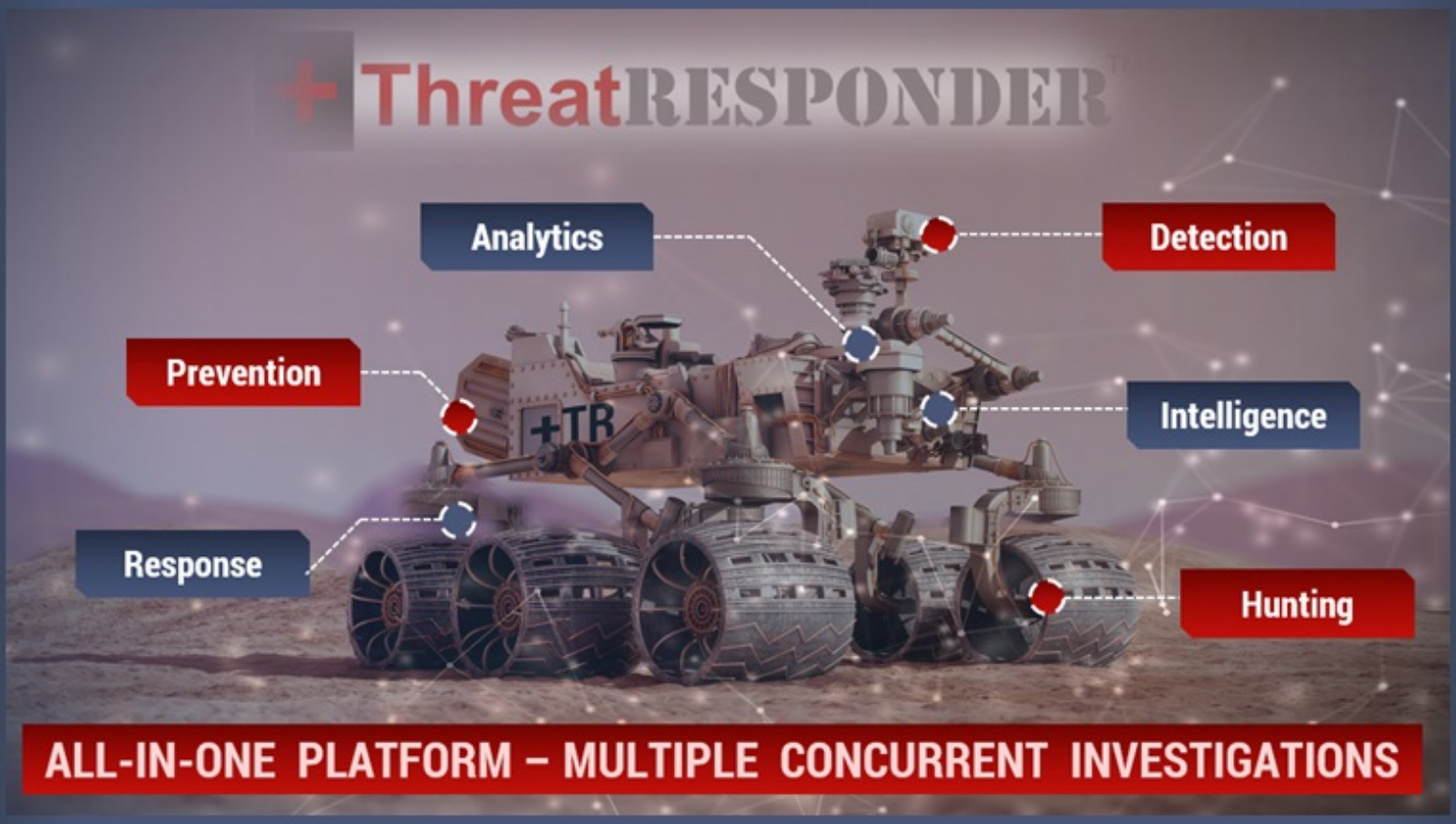
Ubuntu Security Notice 5505-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Likang Luo discovered that a race condition existed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

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



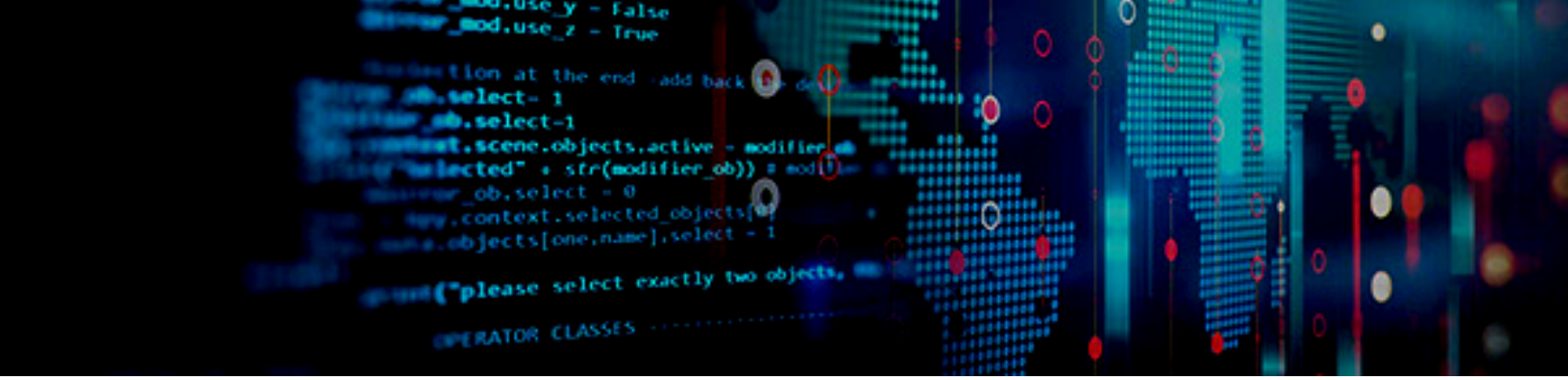
The Solution – ThreatResponder® Platform

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

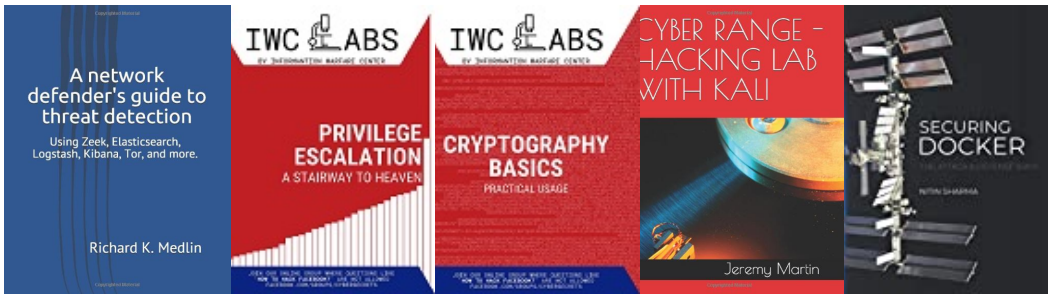


The Cyber Secrets publications on Amazon

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