May-16-22

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

May 16, 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

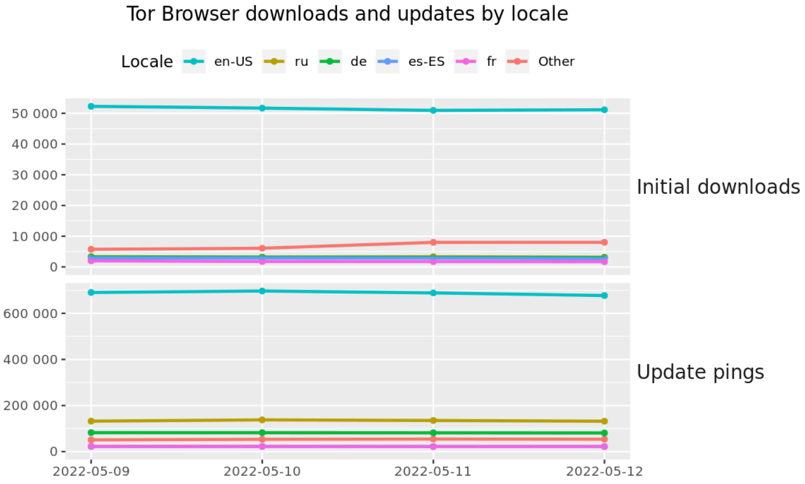
Internet Storm Center Infocon Status

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/2UulG9B

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



The Tor Project - https://metrics.torproject.org/

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* EU Governments, Lawmakers Agree On Tougher Cybersecurity Rules For Key Sectors
* Threat Actors Use Telegram To Spread Eternity Malware-As-A-Service
* Ransomware Operators Send Their Ransom Note To The Victim's Printer
* Malware Builder Leverages Discord Webhooks
* Zyxel Silently Patches Command Injection Vulnerability With 9.8 Severity Rating
* Hackers Are Exploiting WordPress Tools To Hawk Scams
* Turmoil In Crypto Market As Stablecoin Tether Breaks Dollar Peg
* Novel Nerbian Trojan Uses Advanced Anti-Detection Tricks
* Ukraine War: Don't Underestimate Russia Cyber Threat, Warns US
* APT Gang Sidewinder Goes On Two Year Attack Spree Across Asia
* Ransomware The Final Nail In Coffin For Small University
* Intel Memory Bug Poses Risk For Hundreds Of Products
* Russia Fails To Recover RuTube Access On Third Day Of Outage
* Western Governments Accuse Russia Of Hacking US Satellite Internet Provider
* Actively Exploited Zero-Day Bug Patched By Microsoft
* Fresh Ransomware Samples Indicate REvil Is Back
* Hackers Actively Exploit F5 BIG-IP Bug
* Malware Goes Regional As Attackers Change Tactics
* Crypto Assets Shed $800 Billion In Market Value In A Month
* Biden Signs Cybercrime Tracking Bill Into Law
* Conti Ransomware Attack Spurs State Of Emergency In Costa Rica
* Small Drones Are Giving Ukraine An Unprecedented Edge
* Ransomware Plows Through Farm Machinery Giant AGCO
* Colonial Pipeline Faces Nearly $1m Fine One Year After Ransomware Attack
* U.S. Sanctions Crypto Mixing Service Used By North Korea For First Time

Krebs on Security

* DEA Investigating Breach of Law Enforcement Data Portal
* Microsoft Patch Tuesday, May 2022 Edition
* Your Phone May Soon Replace Many of Your Passwords
* Russia to Rent Tech-Savvy Prisoners to Corporate IT?
* You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
* Fighting Fake EDRs With 'Credit Ratings' for Police
* Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code
* Conti's Ransomware Toll on the Healthcare Industry
* Microsoft Patch Tuesday, April 2022 Edition
* RaidForums Gets Raided, Alleged Admin Arrested

LATEST NEWS

Dark Reading

* How to Turn a Coke Can Into an Eavesdropping Device
* US Agrees to International Electronic Cybercrime Evidence Swap
* CISO Shares Top Strategies to Communicate Security's Value to the Biz
* Black Hat Asia: Democracy's Survival Depends on Taming Technology
* Linux, OpenSSF Champion Plan to Improve Open Source Security
* Log4Shell Exploit Threatens Enterprise Data Lakes, AI Poisoning
* Data Transformation: 3 Sessions to Attend at RSA 2022
* How to Avoid Falling Victim to PayOrGrief's Next Rebrand
* Transforming SQL Queries Bypasses WAF Security
* Black Hat Asia: Firmware Supply Chain Woes Plague Device Security
* 3 Predictors of Cybersecurity Startup Success
* Egnyte Enhances Program for Managed Service Providers
* StackHawk Raises $20.7 Million in Series B Funding for Developer-First Application and API Security T
* Cloud Firm Appian Awarded $2B in Trade Secret Cyber-Theft Lawsuit
* Needs Improvement: Scoring Biden's Cyber Executive Order
* How Can Your Business Defend Itself Against Fraud-as-a-Service?
* Known macOS Vulnerabilities Led Researcher to Root Out New Flaws
* 5 Years That Altered the Ransomware Landscape
* On the Air With Dark Reading News Desk at Black Hat Asia 2022
* PlainID Debuts Authorization-as-a-Service Platform

The Hacker News

* Researchers Warn of "Eternity Project" Malware Service Being Sold via Telegram
* Europe Agrees to Adopt New NIS2 Directive Aimed at Hardening Cybersecurity
* Ukrainian Hacker Jailed for 4-Years in U.S. for Selling Access to Hacked Servers
* Get Lifetime Access to 2022 Cybersecurity Certification Prep Courses @ 95% Off
* SonicWall Releases Patches for New Flaws Affecting SSLVPN SMA1000 Devices
* Google Created 'Open Source Maintenance Crew' to Help Secure Critical Projects
* New Saitama backdoor Targeted Official from Jordan's Foreign Ministry
* Zyxel Releases Patch for Critical Firewall OS Command Injection Vulnerability
* Iranian Hackers Leveraging BitLocker and DiskCryptor in Ransomware Attacks
* E.U. Proposes New Rules for Tech Companies to Combat Online Child Sexual Abuse
* Thousands of WordPress Sites Hacked to Redirect Visitors to Scam Sites
* Android and Chrome Users Can Soon Generate Virtual Credit Cards to Protect Real Ones
* Everything We Learned From the LAPSUS$ Attacks
* Government Agencies Warn of Increase in Cyberattacks Targeting MSPs
* Hackers Deploy IceApple Exploitation Framework on Hacked MS Exchange Servers

LATEST NEWS

Security Week

* Hired 'Hackers' Try, and Fail, to Invade Brazil Vote System
* Iran-Linked OilRig APT Caught Using New Backdoor
* Hackers Can Make Siemens Building Automation Controllers 'Unavailable for Days'
* devOcean Emerges From Stealth With Cloud-Native Security Operations Platform
* Critical Vulnerability Allows Remote Hacking of Zyxel Firewalls
* 'IceApple' Post-Exploitation Framework Created for Long-Running Operations
* Critical Vulnerabilities Provide Root Access to InHand Industrial Routers
* Ukrainian Sentenced to US Prison for Selling Hacked Credentials
* Organizations in Europe Targeted With New 'Nerbian' RAT
* Maryland Governor Signs Bills to Strengthen Cybersecurity
* Costa Rica Declares Emergency in Ongoing Cyberattack
* BalkanID Raises $6M for Intelligent IGA Technology
* Russia Pushes Law to Force Taxi Apps to Share Data With Spy Agency
* Size of Early Stage Cyber Deals Continues to Surge: DataTribe
* Application Security Firm StackHawk Bags $20.7 Million in Series B Funding
* Iranian Cyberspy Group Launching Ransomware Attacks Against US
* Zero Trust Firm Xage Security Adds $6 Million 'Top-up' to $30 Million Series B Funding
* HP Patches UEFI Vulnerabilities Affecting Over 200 Computers
* Hundreds of Thousands of Konica Printers Vulnerable to Hacking via &#8203;&#8203;Physical Access
* Prepare for What You Wish For: More CISOs on Boards
* Intel Patches High-Severity Vulnerabilities in BIOS, Boot Guard
* Email Security Vendors Score Billion-Dollar Valuations
* The Importance of Wellness for Security Teams
* Chrome 101 Update Patches High-Severity Vulnerabilities
* SaaS App Vanity URLs Can Be Spoofed for Phishing, Social Engineering
* Ransomware Attack a Nail in the Coffin as Lincoln College Closes After 157 Years

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Think BEC Won't Cost You Much? How Does $130 Million Sound?
* Homeland Security: U.S. Ransomware Attacks Have Doubled in the Last Year
* Trezor Crypto Wallet Attacks Results in Class Action Lawsuit Against MailChimp Owner Intuit
* Happy Credit Union Customers Become the Target of Spoofing Scams Due to a Lack of Email Security
* European Wind-Energy Sector Is the Latest Target of Russian State-Sponsored Attacks
* Beware of Spoofed Vanity URLs
* KnowBe4 Earns 2022 Top Rated Award from TrustRadius
* Another Report of SEO in Phishing
* Mustang Panda Uses Spear Phishing to Conduct Cyberespionage
* CyberheistNews Vol 12 #19 [Heads Up] There is a New Type of Phishing Campaign Using Simple Email Temp

ISC2.org Blog

* You Can Join the (ISC)&sup2; Board of Directors
* HOT CYBERSECURITY TECHNOLOGIES
* Board, (Dash)board and Bored
* CCSP Exam - Many Changes on the Way!
* (ISC)&sup2; Hellenic Chapter Wins Award for Creating Educational Materials

HackRead

* US Sentence Ukrainian to 4 Years for Brute-forcing and Selling Login Credentials
* A Guide to Using VPNs on Your Smartphone
* Misconfigured ElasticSearch Servers Exposed 579 GB of Users' Website Activity
* Top VPN Scams Revealed - Here's What to Look Out for in 2022
* Microsoft Patch Tuesday: Fixes for 0-Day and 74 Other Flaws Released
* 6 Legal and Free Streaming Services to Consider in 2022
* Fake WHO Safety Emails on COVID-19 Dropping Nerbian RAT Across Europe

Koddos

* US Sentence Ukrainian to 4 Years for Brute-forcing and Selling Login Credentials
* A Guide to Using VPNs on Your Smartphone
* Misconfigured ElasticSearch Servers Exposed 579 GB of Users' Website Activity
* Top VPN Scams Revealed - Here's What to Look Out for in 2022
* Microsoft Patch Tuesday: Fixes for 0-Day and 74 Other Flaws Released
* 6 Legal and Free Streaming Services to Consider in 2022
* Fake WHO Safety Emails on COVID-19 Dropping Nerbian RAT Across Europe

LATEST NEWS

Naked Security

* Firefox out-of-band update to 100.0.1 - just in time for Pwn2Own?
* He sold cracked passwords for a living - now he's serving 4 years in prison
* S3 Ep82: Bugs, bugs, bugs (and Colonial Pipeline again) [Podcast]
* Serious Security: Learning from curl's latest bug update
* Colonial Pipeline facing $1,000,000 fine for poor recovery plans
* RubyGems supply chain rip-and-replace bug fixed - check your logs!
* You didn't leave enough space between ROSE and AND, and AND and CROWN
* S3 Ep81: Passwords (still with us!), Github, Firefox at 100, and network worms [Podcast]
* World Password Day - the 1960s just called and gave you your passwords back
* Android monthly updates are out - critical bugs found in critical places!

Threat Post

* Threat Actors Use Telegram to Spread 'Eternity' Malware-as-a-Service
* Malware Builder Leverages Discord Webhooks
* You Can't Eliminate Cyberattacks, So Focus on Reducing the Blast Radius
* Novel 'Nerbian' Trojan Uses Advanced Anti-Detection Tricks
* Intel Memory Bug Poses Risk for Hundreds of Products
* Novel Phishing Trick Uses Weird Links to Bypass Spam Filters
* Actively Exploited Zero-Day Bug Patched by Microsoft
* Ransomware Deals Deathblow to 157-year-old College
* Hackers Actively Exploit F5 BIG-IP Bug
* Conti Ransomware Attack Spurs State of Emergency in Costa Rica

Null-Byte

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

LATEST NEWS

IBM Security Intelligence

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

InfoWorld

* Microsoft .NET 7 Preview 4 brings Regex improvements, cache metrics
* JDK 19: The features targeted for Java 19
* Cloudflare to take on AWS, Azure, Google with D1 distributed database
* What is JDBC? Introduction to Java Database Connectivity
* How to build changeable cloud solutions
* TypeScript 4.7 adds ESM support in Node.js
* Jetpack Compose 1.2 packs text improvements
* Google Flutter 3 backs macOS, Linux
* How to compress and decompress strings in C#
* 9 questions you should ask about your cloud security

C4ISRNET - Media for the Intelligence Age Military

* Pentagon technology chief pledges support for DIU following director's departure
* Space Force lays out 'Range of the Future' priorities as launches surge
* Project Convergence 22 aims to have best-positioned force shoot first
* Pentagon may rethink how it determines which space programs are classified
* Pentagon tests high-power microwave systems against drones
* War in Ukraine reinforces need for US Army network upgrades, generals say
* US and allies blame Russia for Viasat hack ahead of Ukraine invasion
* Space Force releases plan for testing satellites, ground systems
* Maxar reports $7 million loss in first quarter earnings
* Afghan-based terror groups still a year away from ability to strike US, intel leaders say

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

* Release of Technical Report into the AMD Security Processor
* The More You Know, The More You Know You Don't Know

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.

* hackrocks & HackArmour CTF
* saarCTF 2022
* Hack-A-Sat 3 Qualifiers
* Hacktrick CTF'22
* BYUCTF 2022
* HSCTF 9
* SEETF 2022
* BCACTF 3.0
* n00bzCTF
* SunshineCTF 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

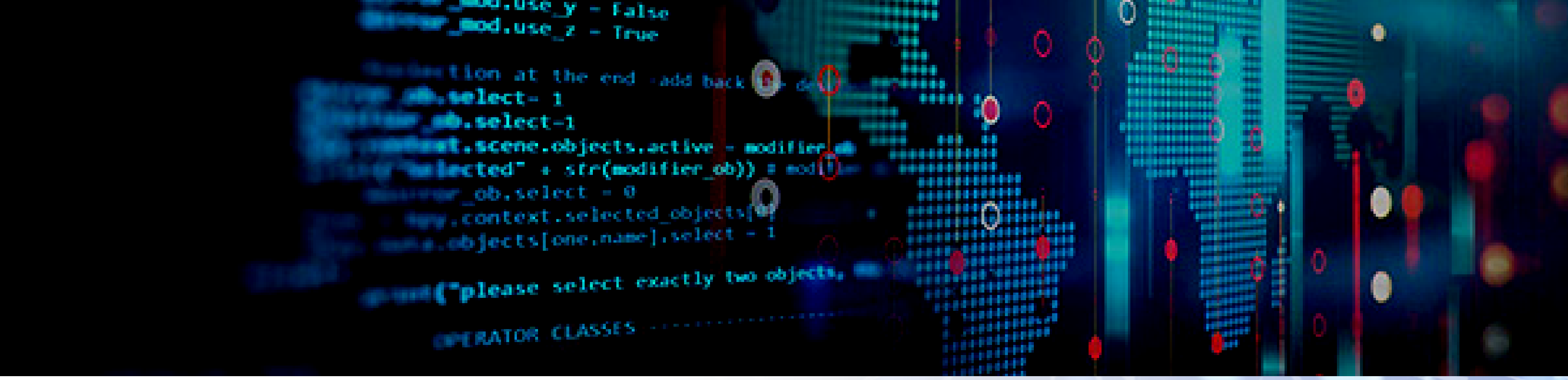
* COOPER Analysis Tool
* Aircrack-ng Wireless Network Tools 1.7
* Samhain File Integrity Checker 4.4.9
* Adversary3 2.0
* Wireshark Analyzer 3.6.5
* Clam AntiVirus Toolkit 0.105.0
* OpenSSL Toolkit 3.0.3
* OpenSSL Toolkit 1.1.1o
* Samhain File Integrity Checker 4.4.8
* TOR Virtual Network Tunneling Tool 0.4.7.7

Kali Linux Tutorials

* Zkar : A Java Serialization Protocol Analysis Tool Implement In Go
* Request_Smuggler : Http Request Smuggling Vulnerability Scanner
* Factual-Rules-Generator : An Open Source Project Which Aims To Generate YARA Rules
* SysWhispers3 : AV/EDR Evasion Via Direct System Calls
* ADExplorerSnapshot.py : An AD Explorer Snapshot Parser. It Is Made As An Ingestor For BloodHound
* Shellcode Template : An Easily Modifiable Shellcode Template For Windows X64/X86
* Vortex : VPN Overall Reconnaissance, Testing, Enumeration And exploitation Toolkit
* FastFinder : Incident Response - Fast Suspicious File Finder
* Oh365UserFinder : Python3 O365 User Enumeration Tool
* PSRansom : PowerShell Ransomware Simulator With C2 Server

GBHackers Analysis

* Multiple QNAP Flaws Let attackers to Access and Read Sensitive Data
* Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level
* Critical RCE Vulnerability in Google's VirusTotal Platform Let Attackers Scans Capabilities
* Critical Android Bug Let Attackers to Access Users' Media and Audio Conversations
* 15-Year-old Security Vulnerability In The PEAR PHP Repository Permits Supply Chain Attack



Weekly Cyber Security Video and Podcasts

SANS DFIR

* DFIR Summit 2022
* Inside FOR710 Reverse-Engineering Malware: Advanced Code Analysis
* The New GIAC MacOS and iOS Examiner Certification (GIME)
* SANS Threat Analysis Rundown | Katie Nickels

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

* Detecting WiFi Pineapples & Malicious KARMA Attacks
* Live Hacking Q&A with Kody Kinzie & Alex Lynd
* Google, Apple, and Microsoft Go Passwordless - ThreatWire

The PC Security Channel [TPSC]

* Windows Update Ransomware
* How to tell if your Wifi is hacked?

Eli the Computer Guy

* ELON MUSK FAILING to BUY TWITTER - musk is destroying twitter for the lols
* COINBASE can STEAL YOUR CRYPTOCURRENCY - crypto is a scam
* VICE MEDIA is DEAD - the economy is GREAT
* BITCOIN CRASHES - because it's tuesday

Security Now

* That "Passkeys&rdquo; Thing - White House and Quantum Computers, Android 0-day, Ransomware snapshot
* Global Privacy Control - DoD DIB-VDP, OpenSSF's Package Analysis Project, Connecticut Privacy

Troy Hunt

* Weekly Update 295

Intel Techniques: The Privacy, Security, & OSINT Show

* 261-A Client Stops By

* 260-Google's New Policy Change

Proof of Concept (PoC) & Exploits

Packet Storm Security

- Konica Minolta bizhub MFP Printer Terminal Sandbox Escape
- Ransom.REvil MVID-2022-0600 Code Execution
- Ransom.REvil MVID-2022-0599 Code Execution
- Ransom.REvil MVID-2022-0598 Code Execution
- Ransom.REvil MVID-2022-0597 Code Execution
- Ransom.REvil MVID-2022-0595 Code Execution
- F5 BIG-IP iControl Remote Code Execution
- AppleVideoDecoder CreateHeaderBuffer Out-Of-Bounds Free
- College Management System 1.0 SQL Injection
- TLR-2005KSH Arbitrary File Delete
- Ransom.REvil MVID-2022-0596 Code Execution
- Royal Event Management System 1.0 SQL Injection
- F5 BIG-IP 16.0.x Remote Code Execution
- Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
- Ruijie Reyee Mesh Router Remote Code Execution
- Joomla SexyPolling 2.1.7 SQL Injection
- WordPress Blue Admin 21.06.01 Cross Site Request Forgery
- MyBB 1.8.29 Remote Code Execution
- Beehive Forum 1.5.2 Account Takeover
- DLINK DAP-1620 A1 1.01 Directory Traversal
- PyScript 2022-05-04-Alpha Source Code Disclosure
- Google Chrome 78.0.3904.70 Remote Code Execution
- Navigate CMS 2.9.4 Server-Side Request Forgery
- Anuko Time Tracker 1.20.0.5640 SQL Injection
- UDisk Monitor Z5 Phone 2.0.3.0 Unquoted Service Path

CXSecurity

- ExifTool 12.23 Arbitrary Code Execution
- Bitrix24 Remtoe Code Execution
- Ruijie Reyee Mesh Router Remote Code Execution
- Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
- F5 BIG-IP Remote Code Execution
- VMware Workspace ONE Access Template Injection / Command Execution
- Watch Queue Out-Of-Bounds Write

Proof of Concept (PoC) & Exploits

Exploit Database

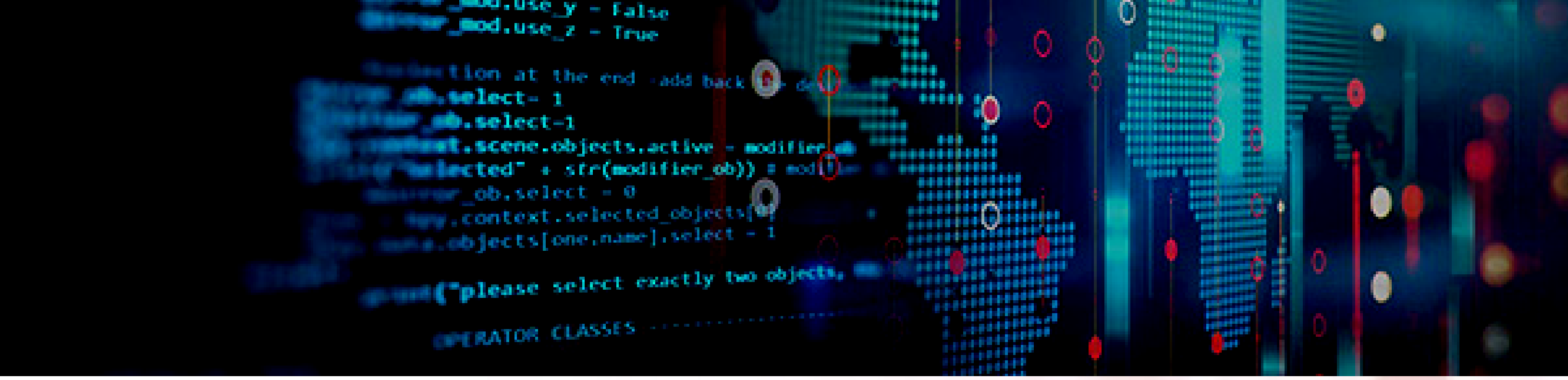
* [webapps] TLR-2005KSH - Arbitrary File Delete
* [webapps] Royal Event Management System 1.0 - 'todate' SQL Injection (Authenticated)
* [webapps] College Management System 1.0 - 'course_code' SQL Injection (Authenticated)
* [remote] F5 BIG-IP 16.0.x - Remote Code Execution (RCE)
* [webapps] TLR-2005KSH - Arbitrary File Upload
* [remote] Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)
* [webapps] Joomla Plugin SexyPolling 2.1.7 - SQLi
* [webapps] WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)
* [webapps] MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Beehive Forum - Account Takeover
* [webapps] PHProjekt PhpSimplyGest v1.3. - Stored Cross-Site Scripting (XSS)
* [webapps] Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)
* [webapps] Explore CMS 1.0 - SQL Injection
* [remote] DLINK DAP-1620 A1 v1.01 - Directory Traversal
* [remote] PyScript - Read Remote Python Source Code
* [remote] Google Chrome 78.0.3904.70 - Remote Code Execution
* [remote] Tenda HG6 v3.3.0 - Remote Command Injection
* [webapps] Anuko Time Tracker - SQLi (Authenticated)
* [remote] Apache CouchDB 3.2.1 - Remote Code Execution (RCE)
* [remote] Wondershare Dr.Fone 12.0.7 - Remote Code Execution (RCE)
* [local] Wondershare Dr.Fone 12.0.7 - Privilege Escalation (ElevationService)
* [local] ExifTool 12.23 - Arbitrary Code Execution
* [webapps] e107 CMS v3.2.1 - Multiple Vulnerabilities
* [webapps] Cyclos 4.14.7 - 'groupId' DOM Based Cross-Site Scripting (XSS)

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
```

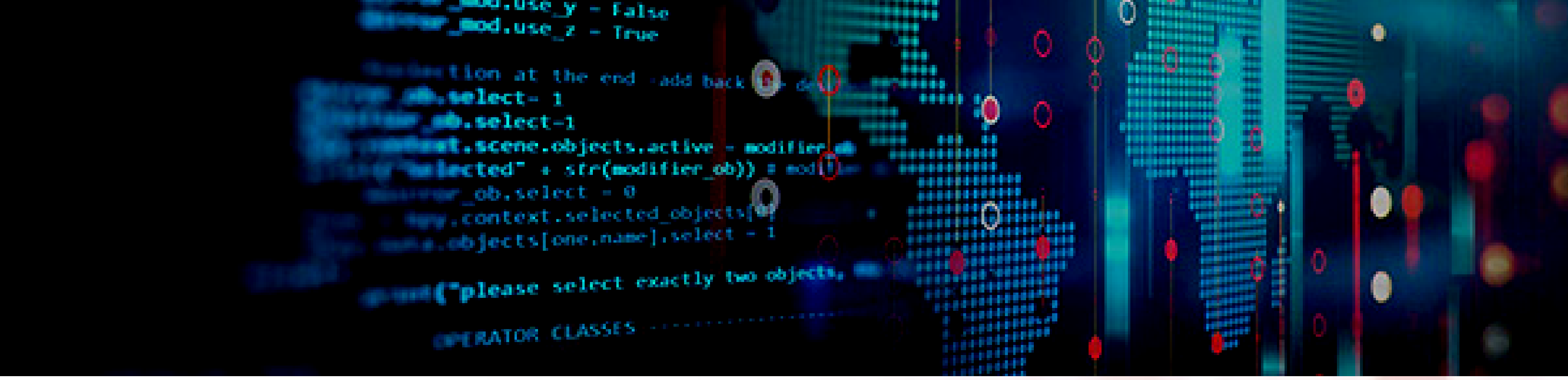
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://medpub.litbang.pertanian.go.id/index2.php
https://medpub.litbang.pertanian.go.id/index2.php notified by SanggamXploiter
http://www.pa-kediri.go.id/trkn.txt
http://www.pa-kediri.go.id/trkn.txt notified by http://www.dilmiltama.go.id/trkn.txt
https://kotawaringinbaratkab.go.id/readme.php
https://kotawaringinbaratkab.go.id/readme.php notified by Calutax07
http://www.pa-sragen.go.id/readme.htm
http://www.pa-sragen.go.id/readme.htm notified by AnonCoders
https://pn-kuningan.go.id/read.html
https://pn-kuningan.go.id/read.html notified by Mr.Rm19
https://pn-bandung.go.id/baca.html
https://pn-bandung.go.id/baca.html notified by Mr.Rm19
https://educacion.dnbc.gov.co/abcd.html
https://educacion.dnbc.gov.co/abcd.html notified by ./KeyzNet
http://agroturizem.gov.al/readme.php
http://agroturizem.gov.al/readme.php notified by AnonCoders
https://agrotourism.gov.al/readme.php
https://agrotourism.gov.al/readme.php notified by AnonCoders
http://ata.gov.al/readme.php
http://ata.gov.al/readme.php notified by AnonCoders
https://epprn.mohe.gov.my/storage/cv/2204290PrCNYETfzYr7CU.html
https://epprn.mohe.gov.my/storage/cv/2204290PrCNYETfzYr7CU.html notified by HAMMAML1F
http://appointment.mida.gov.my/hacked.html
http://appointment.mida.gov.my/hacked.html notified by HAMMAML1F
https://nmrr.gov.my/media/
https://nmrr.gov.my/media/ notified by HAMMAML1F
http://madrp.gov.dz/indexx.html
http://madrp.gov.dz/indexx.html notified by El-Harrachi
https://www.cmoriximina.pa.gov.br/datalist_mini.html
https://www.cmoriximina.pa.gov.br/datalist_mini.html notified by Hamza Anonime
https://dikbud.kalbarprov.go.id/666.html
https://dikbud.kalbarprov.go.id/666.html notified by AnonCoders
https://database-litbang.kalbarprov.go.id/666.html
https://database-litbang.kalbarprov.go.id/666.html notified by AnonCoders



Dark Web News

Darknet Live

German Allegedly Bought Kilos of Amphetamine on the Darkweb

Authorities in Lower Bavaria, Germany, arrested a man for allegedly selling drugs he had purchased on the darkweb. According to a press release from the Lower Bavaria criminal police inspectorate, police arrested a 33-year-old man from the southern district of Landshut after he had "ordered drugs for resale via the darknet.&rdquo; __ Police seized several packages of amphetamine at a post office in Landshut. Investigators in the United States had identified the suspect as part of an investigation in April 2022. The investigators in the U.S. then relayed information about the suspect to German law enforcement agencies. The 33-year-old was "already known to authorities.&rdquo; Investigations by the Landshut Criminal Police Inspectorate resulted in the interception of two drug packages addressed to the 33-year-old. The interceptions resulted in the seizure of several kilograms of amphetamine. The investigators executed a search warrant on the suspect's residence in May 2022. The search resulted in the seizure of 20 grams of amphetamine, cash, and unspecified electronic devices. After the search, police arrested the defendant. He will remain in custody as the investigation continues. (via darknetlive.com at https://darknetlive.com/post/german-allegedly-bought-kilos-of-amphetamine-on-the-darkweb/)

Woman Allegedly Tried to Hire a Hitman to Kill Her Parents

A woman who allegedly hired a hitman on the darkweb to kill her parents is planning to stand trial. On May 10, 2022, a 27-year-old woman pleaded not guilty to two counts of inciting murder at the ACT Magistrates Court. The defendant had already pleaded not guilty to attempted murder charges at a previous hearing. Magistrate James Stewart remanded the defendant into custody for a hearing on May 19 on trial-related details. __ The hitman site in question is gone. The site pictured is a nearly identical replacement. The investigation began in October 2020 after a journalist contacted Australian Capital Territory Policing about a murder-for-hire plot. The journalist provided police with evidence that someone in Canberra had agreed to pay a hitman $20,000 to kill two people. Investigators believe she had only paid $6,000 out of the agreed $20,000 contract. According to police, the defendant entered her parents' house when they were out and transferred $15,000 from her parents' bank account into a bank account they shared with the defendant. Later she moved the stolen money to her bank account. On September 24, 2020, the defendant allegedly used the stolen money to buy $6,000 in Bitcoin. She then sent $6,000 in Bitcoin to the administrator of the darkweb murder-for-hire site "The Sinaloa Cartel Marketplace.&rdquo; __ The Sinaloa Cartel Marketplace now directs visitors to this directory of hitman sites. "Having trouble using the shop function to submit job inquiry, so will do it here. Willing to pay $20,000AUD to have this done as soon as possible. 2 individuals, death by accident if at all possible,&rdquo; she wrote in a message to the site administrator, "Juan.&rdquo; Police alleged that she sent Juan the names and addresses of her parents. "I require this job to be done ASAP.&rdquo; In October 2020, police interviewed the parents. The police learned that their children would be entitled to an equal share of their 8 million dollar estate if they died. __ Conspicuously, the sites operated by the site owner are the top hitman sites. On December 7, 2020, police interviewed the defendant and searched her home. She denied knowing anything about the darkweb or Bitcoin. Police arrested her later that day. Prosecutors have charged the defendant with two counts of attempted murder, two counts of inciting murder, theft, and burglary. In her most recent hearing, which took place remotely, the defendant pleaded not guilty to the two counts of inciting murder. She already pleaded guilty to the other charges. (via darknetlive.com at https://darknetlive.com/post/woman-allegedly-tried-to-hire-a-hitman-to-kill-her-parents/)

California Meth Vendor to Be Sentenced Today

A darkweb vendor who ran his operation from behind bars is scheduled to be sentenced today. Michael Goldberg, 36, of Los Angeles, California, faces sentencing today for selling methamphetamine on the darkweb. Court documents do not officially identify the defendant's vendor username. However, an excerpt from a recorded phone call between Goldberg and one of his co-conspirators possibly identifies the username as "Drugs R Us.&rdquo; _ Goldberg may have operated the "Drugs R Us&rdquo; account on Dream and other markets. The case, which is detailed in a lengthy criminal complaint, involves three indicted co-conspirators and several unindicted co-conspirators. Donnica Rabulan, 31, Goldberg's wife, and James Caleb Kueker, 41, were also charged for their roles in the drug trafficking operation. In 2018, a shipping company identified seven suspicious packages headed to the Philippines. Federal law enforcement officers found nearly 21 kilograms of methamphetamine inside the packages. While the names on the packages were fake, Goldberg was the registered subscriber of the phone numbers associated with six of the packages. _ The classic "accidentally use your real phone number&rdquo; mistake. A Homeland Security Investigations special agent, in the criminal complaint, wrote: On May 30, 2018, I interviewed employees at the UPS Store. Based on California Driver License ("CDL&rdquo;) photographs of GOLDBERG and RABULAN, employees identified GOLDBERG as a longtime customer and the renter of Box 710 at the UPS Store and RABULAN as the person they knew as "Danica Santiago,&rdquo; the listed shipper of parcel #4. According to a UPS Store employee, on May 21, 2018, RABULAN and her friend entered the UPS Store together and mailed parcels 1 through 4. RABULAN mailed parcel #3 under the consignor name MGA Productions and parcel #4 under the consignor name Danica Santiago. RABULAN's friend, mailed parcels 1 and 2 under the consignor name "Tracy Shapoff.&rdquo; Investigators noticed a common theme with some of the packages shipped by the defendants: "On June 11, 2018 CBP officers at the IMF targeted and inspected another USPS parcel, bearing the tracking number EZ010910686US, from consignor "Jeff Stevens&rdquo; at 2700 E. Cahuenga Boulevard, Los Angeles, CA 90068 shipped to Australia and discovered approximately 72.6 grams of methamphetamine (the "AUSTRALIA PARCEL&rdquo;).&rdquo; "Jeff Stevens&rdquo; also shipped three other parcels internationally around the same time as the NEW ZEALAND PARCEL and the AUSTRALIA PARCEL. CBP seized two of the parcels, which contained a total of 176.1 grams of methamphetamine&hellip;" "On June 7, 2018, CBP Officer Lionel Andrade notified me of the POLAND PARCEL that was in transit to consignee Patryk Breczko in Piensk, Poland. The consignor of the POLAND PARCEL was "Jeff Stevens&rdquo; at 18618 Clark Street, Tarzana, California.&rdquo; Investigators identified 59 packages shipped by the defendants based on a variation of the consignor's name and the consignor's address. The defendants had shipped the packages to the Philippines, Australia, New Zealand, the United Kingdom, Italy, Poland, and France, among other places. Law enforcement officers seized 14 of the 59 packages. The seized packages contained a total of approximately 22.3 kilograms of methamphetamine and 170 grams of marijuana. Someone living at Rabulan's address tracked some of the packages. Goldberg lived at the same address until June 2018. On June 6, 2018, Goldberg surrendered to law enforcement for an outstanding warrant for mail theft and fraud. A judge sentenced Goldberg to 42 months in prison. Law enforcement officers learned that Goldberg was still running the operation while in a federal detention center. At the detention center, inmates are allotted 300 minutes to talk on the phone every month. Goldberg used all 300 of his allotted minutes and regularly used the accounts of 16 fellow inmates. While using his own line, Goldberg would tell his co-conspirators that he could not speak freely. However, he had much less of a filter when using accounts owned by other inmates. People in the outside world have to register their phone numbers with the Bureau of Prisons before an inmate can call them. As a result, officials can quickly determine when inmates place phone calls through a different inmate's account. "On June 14, 2018, at approximately 6:42 a.m.,

GOLDBERG made an MDC phone call from his own account to RABULAN. GOLDBERG and RABULAN discuss the inability to talk freely because he is on his MDC phone account. GOLDBERG states, "Hey can you answer the other phone number today? The 310 number because I'm not going to call you on this number today&hellip; Baby, answer the other phone; I can't be talking to you like this for reals.&rdquo; "Several hours later, at approximately 10:05 a.m., GOLDBERG made an MDC phone call using inmate Joseph Hill's phone account to RABULAN. The conversation begins with RABULAN, GOLDBERG, and an individual only known as "Echo&rdquo; on a three-way phone call. GOLDBERG stated that RABULAN will "handle it today or tomorrow,&rdquo; which I believe, based on the context of the exchange, is referring to the shipment of drugs and money transfers. After Echo hangs up, GOLDBERG and RABULAN continue their conversation about money an individual named "Rain&rdquo; owes them. GOLDBERG states, "Make sure you get 25% before you do anything. The rest of them make sure, especially Rain. I want 25 grand of the money he owes me.&rdquo; Based on the context of the conversation and my investigation of the case, I believe the "25 grand&rdquo; refers to the proceeds from drug sales.&rdquo; "On June 6, 2018, at approximately 9:20 a.m., GOLDBERG made an MDC phone call to RABULAN and RABULAN's older sister, Donna Mae Rabulan. In the conversation, the parties discuss getting access to the dark web, destroying evidence, and the status of drug shipments. GOLDBERG instructs RABULAN, "Tell your sister to clean out the shredder.&rdquo; RABULAN relays the message to her sister and asks, "I don't know the login for the other thing, the darkweb.&rdquo; GOLDBERG begins to respond, "It's `Drugs R Us&rdquo;' but is promptly interrupted by RABULAN and Donna Mae Rabulan from saying anything further over the phone.&rdquo; _ One of the many profiles for "Drugs R Us&rdquo; on Recon. "On June 20, 2018, in an MDC phone call between KUEKER and GOLDBERG, they discussed ordering and selling drugs. GOLDBERG says, "You guys should really look into reordering, dawg.&rdquo; KUEKER replies, "Yeah, Yeah. I just want to make sure that there's not too much in stock, you know.&rdquo; GOLDBERG also tells KUEKER that his life story would be more interesting than the drug traffickers in "Cocaine Cowboy,&rdquo; a documentary that features several Miami cocaine traffickers during the 1970s and 1980s. GOLDBERG states, "I was reading this book about this Cocaine Cowboy, and I was like this fool is fucking weak. I really want to do a movie and book when I get out. I think I'll make enough money for everybody to get out of the game.&rdquo; KUEKER responds, "I saw this from the very beginning. Man, damn, this would be a great fucking documentary.&rdquo; GOLDBERG says, "And this will be in the book too, about you calling me in the feds.&rdquo; In the criminal complaint, which I have attached to this article, there are many examples of the incriminating phone calls Goldberg made while in custody. The investigating HSI special agent wrote that they had listened to "over a hundred&rdquo; phone calls. In at least two phone calls, Goldberg tells Kueker to buy products from a Dream vendor identified as "Don Cimura.&rdquo; Later, Goldberg told Kueker to contact the vendor over Wickr because "it's the safest way.&rdquo;
_ Wells Fargo provided investigators with Goldberg's account balances. A review of records from Coinbase revealed that Goldberg had deposited more than $200,000 from Coinbase into his bank account. Rabulan and Goldberg pleaded guilty to a drug conspiracy charge. A judge sentenced Rabulan to 92 months in prison. Kueker is awaiting sentencing. Goldberg's sentencing hearing is scheduled to take place on May 10, 2022. Update May 11, 2022: Sentencing postponed for undisclosed reasons. No new sentencing date provided. complaint pdf (via darknetlive.com at
https://darknetlive.com/post/california-meth-vendor-to-be-sentenced-today/)

A Reminder Not to Take Pictures of Your Fingers

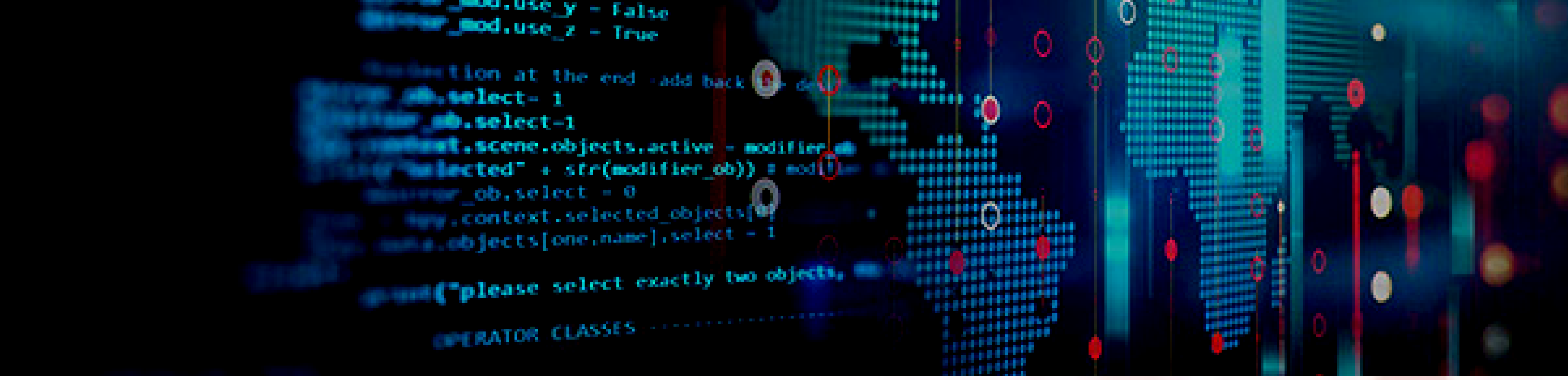
A drug dealer in the UK shared a picture of a block of cheese in one of his hands. Police analyzed the partial fingerprints in the image and identified the dealer. _ Carl Stewart One might think that people know better than to take pictures of their fingers when trying to remain anonymous. A case from 2021 would prove you wrong. When law enforcement agencies hacked Encrochat, they obtained messages sent by a drug dealer with the username "Toffeeforce.&rdquo; One of the user's messages included a picture of his hand holding a block of cheese. According to the Merseyside Police, investigators pulled palm and fingerprints from the picture. The prints matched those of Liverpool resident Carl Stewart. Det Insp Lee Wilkinson of Merseyside Police said, "Stewart was involved in supplying large amounts of class A and B drugs, but was caught out by his love of Stilton cheese, after sharing a picture of a block of it in his hand through encrochat. His palm and fingerprints were analyzed from this picture, and it was established they belonged to Stewart.&rdquo; __ A picture of the cheese picture containing Stewart's fingerprints If investigators "established&rdquo; the prints belonged to Stewart through analysis of the picture, which seems to be what the LEO is saying, law enforcement had Stewart's fingerprints on file for a different reason (such as a previous arrest). The investigation into the marijuana vendor "Canna_Bars&rdquo; provides an example of a similar scenario. Canna_Bars had uploaded pictures of their products to Imgur.com. The vendor held marijuana buds in their bare hand for the close-up images. The Imgur gallery contained shots from slightly different perspectives, giving investigators several high-definition pictures of the vendor's fingerprints. __ Pictures uploaded by Porras aka Canna_bars From a Darknetlive article about the case: "The investigator working the case sent high-quality copies of the pictures to the Homeland Security Investigations Document Laboratory (FDL). On March 20, 2018, the analysts at FDL sent the investigator a report that included their findings: the fingerprints in the pictures matched the fingerprints on file for [Jose] Porras.&rdquo; Police already had fingerprint cards on file for Porras due to a previous arrest for a possession with intent charge. One big difference is the quality of the pictures available in the Canna_bars case compared to the quality of the one picture of cheese available to the public in Stewart' case. I suspect that the only copies of the picture of Stewart's fingers have been compressed by the websites hosting the pictures, rendering it nearly impossible to see any ridgelines. The full resolution copy of Stewart's picture is available at this link. __ Left: Picture of Stewart's fingers, Right: picture of Porras' fingers This case is also less of an OPSEC failure than Porras' mistakes; police had already hacked Stewart's phone and would have likely identified him at some point, regardless of the prints. Stewart pleaded guilty to conspiracy to supply cocaine, heroin, MDMA, and ketamine and one count of transferring criminal property. In May 2021, Stewart was sentenced to 13 years and six months in prison at Liverpool Crown Court. (via darknetlive.com at https://darknetlive.com/post/reminder-about-fingerprints/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, in this article [...] The post Top Darknet Markets 2022: The Outstanding Performances To Consider Now appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

Breaking Bad Forum On The Darknet Is Revolutionary
The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

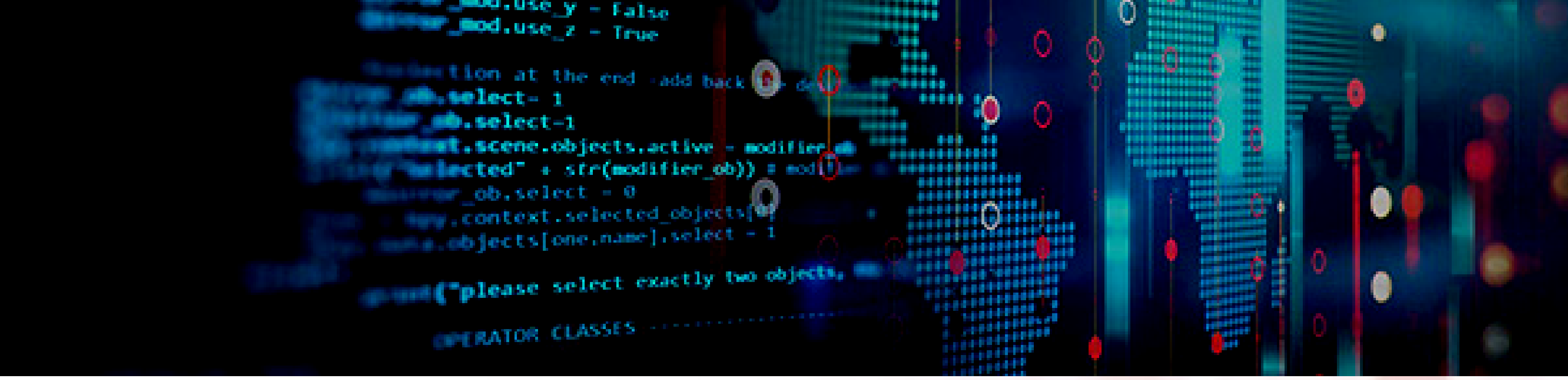
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks

FireEye

* Metasploit Weekly Wrap-Up
* Update for CIS Google Cloud Platform Foundation Benchmarks - Version 1.3.0
* CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection
* [Security Nation] Jim O'Gorman and g0tmi1k on Kali Linux
* Patch Tuesday - May 2022
* What's Changed for Cybersecurity in Banking and Finance: New Study
* Active Exploitation of F5 BIG-IP iControl REST CVE-2022-1388
* [Infographic] Cloud Misconfigurations: Don't Become a Breach Statistic
* Metasploit Wrap-Up
* Unsung Security Superheroes: You're Now Sung



Advisories

US-Cert Alerts & bulletins

* CISA Temporarily Removes CVE-2022-26925 from Known Exploited Vulnerability Catalog
* Adobe Releases Security Updates for Multiple Products
* Google Releases Security Updates for Chrome
* Microsoft Releases May 2022 Security Updates
* CISA Adds One Known Exploited Vulnerability to Catalog
* CISA Joins Partners to Release Advisory on Protecting MSPs and their Customers
* CISA Adds One Known Exploited Vulnerability to Catalog
* U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber
* AA22-131A: Protecting Against Cyber Threats to Managed Service Providers and their Customers
* AA22-117A: 2021 Top Routinely Exploited Vulnerabilities
* Vulnerability Summary for the Week of May 2, 2022
* Vulnerability Summary for the Week of April 25, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-1699-01
Red Hat Security Advisory 2022-1699-01 - 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 4.7.50.

Ubuntu Security Notice USN-5419-1
Ubuntu Security Notice 5419-1 - It was discovered that Rsyslog improperly handled certain invalid input. An attacker could use this issue to cause Rsyslog to crash.

Ubuntu Security Notice USN-5420-1
Ubuntu Security Notice 5420-1 - It was discovered that Vorbis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-2234-01
Red Hat Security Advisory 2022-2234-01 - Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes.

Red Hat Security Advisory 2022-2237-01
Red Hat Security Advisory 2022-2237-01 - Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes.

Red Hat Security Advisory 2022-2232-01
Red Hat Security Advisory 2022-2232-01 - Red Hat Data Grid is an in-memory, distributed, NoSQL datastore solution. It increases application response times and allows for dramatically improving performance while providing availability, reliability, and elastic scale. Data Grid 8.3.1 replaces Data Grid 8.3.0 and includes bug fixes and enhancements. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5417-1
Ubuntu Security Notice 5417-1 - Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. It was discovered that the MMC/SD subsystem in the Linux kernel did not properly handle read errors from SD cards in certain situations. An attacker could possibly use this to expose sensitive information.

Ubuntu Security Notice USN-5418-1
Ubuntu Security Notice 5418-1 - Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information. Demi Marie Obenour and Simon Gaiser discovered that several Xen para- virtualization device frontends did not properly restrict the access rights of device backends. An attacker could possibly use a malicious Xen backend to gain access to memory pages of a guest VM or cause a denial of service in the guest.

Ubuntu Security Notice USN-5416-1
Ubuntu Security Notice 5416-1 - Qiuhao Li, Gaoning Pan and Yongkang Jia discovered that the KVM implementation in the Linux kernel did not properly perform guest page table updates in some situations. An attacker in a guest vm could possibly use this to crash the host OS. It was discovered that the implementation of X.25 network protocols in the Linux kernel did not terminate link layer sessions properly. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-5415-1
Ubuntu Security Notice 5415-1 - Jeremy Cline discovered a use-after-free in the nouveau graphics driver of the Linux kernel during device removal. A privileged or physically proximate attacker could use this to cause a denial of service. Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele,

and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information.

Ubuntu Security Notice USN-5413-1

Ubuntu Security Notice 5413-1 - Jeremy Cline discovered a use-after-free in the nouveau graphics driver of the Linux kernel during device removal. A privileged or physically proximate attacker could use this to cause a denial of service. It was discovered that a race condition existed in the network scheduling 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.

Red Hat Security Advisory 2022-2200-01

Red Hat Security Advisory 2022-2200-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 5.0.214 and .NET Core Runtime 5.0.17. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-2216-01

Red Hat Security Advisory 2022-2216-01 - Logging Subsystem 5.4.1 - Red Hat OpenShift. Issues addressed include HTTP request smuggling and denial of service vulnerabilities.

Red Hat Security Advisory 2022-2199-01

Red Hat Security Advisory 2022-2199-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 6.0.105 and .NET Core Runtime 6.0.5. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-2218-01

Red Hat Security Advisory 2022-2218-01 - Openshift Logging Bug Fix Release. Issues addressed include HTTP request smuggling, denial of service, and man-in-the-middle vulnerabilities.

Red Hat Security Advisory 2022-2210-01

Red Hat Security Advisory 2022-2210-01 - Red Hat Directory Server is an LDAPv3-compliant directory server. The suite of packages includes the Lightweight Directory Access Protocol server, as well as command-line utilities and Web UI packages for server administration. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-2201-01

Red Hat Security Advisory 2022-2201-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

Red Hat Security Advisory 2022-2186-01

Red Hat Security Advisory 2022-2186-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-2197-01

Red Hat Security Advisory 2022-2197-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

Red Hat Security Advisory 2022-2202-01

Red Hat Security Advisory 2022-2202-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 3.1.419 and .NET Core Runtime 3.1.25. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-2214-01

Red Hat Security Advisory 2022-2214-01 - The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.

Red Hat Security Advisory 2022-2213-01

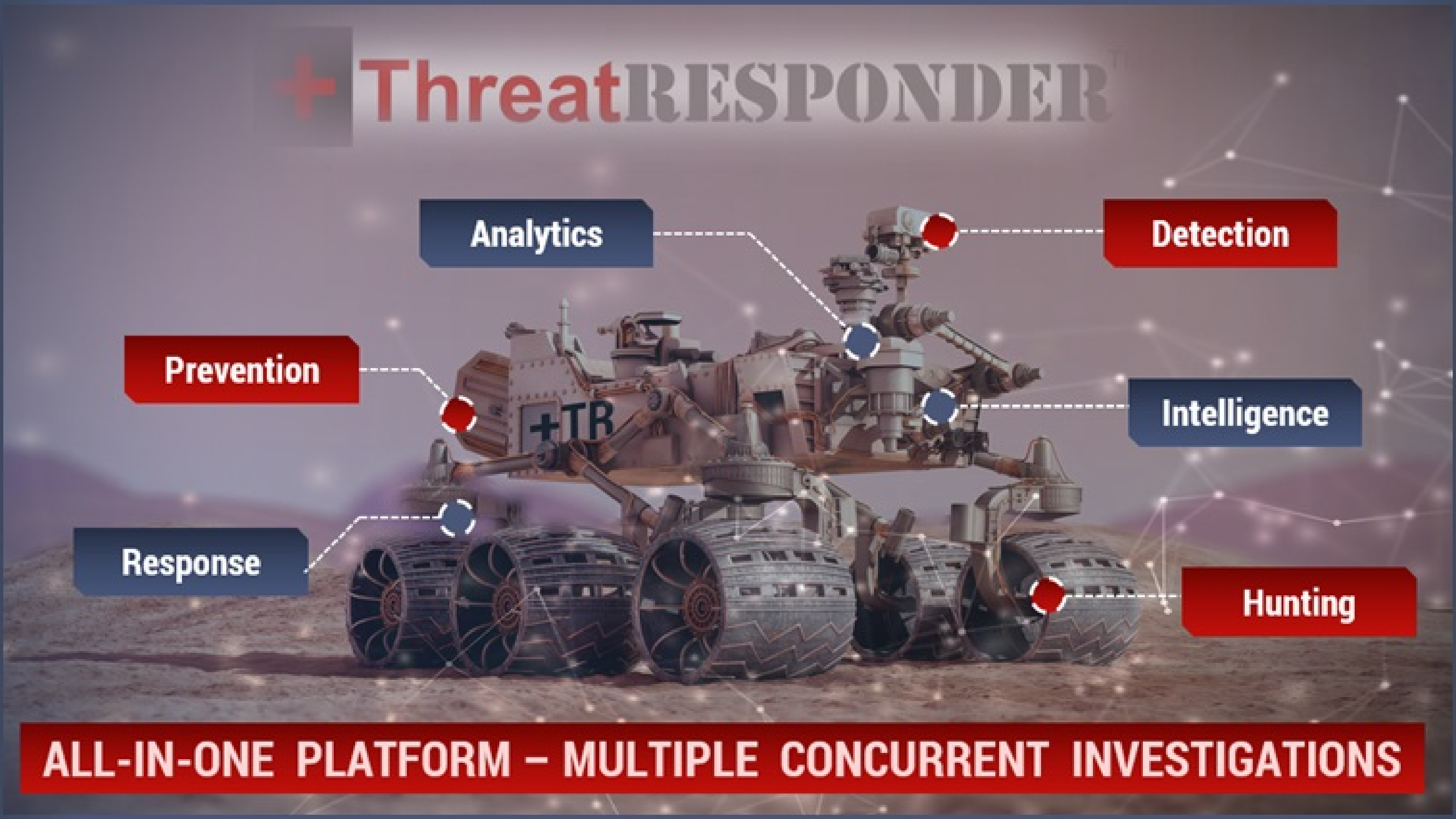
Red Hat Security Advisory 2022-2213-01 - The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.

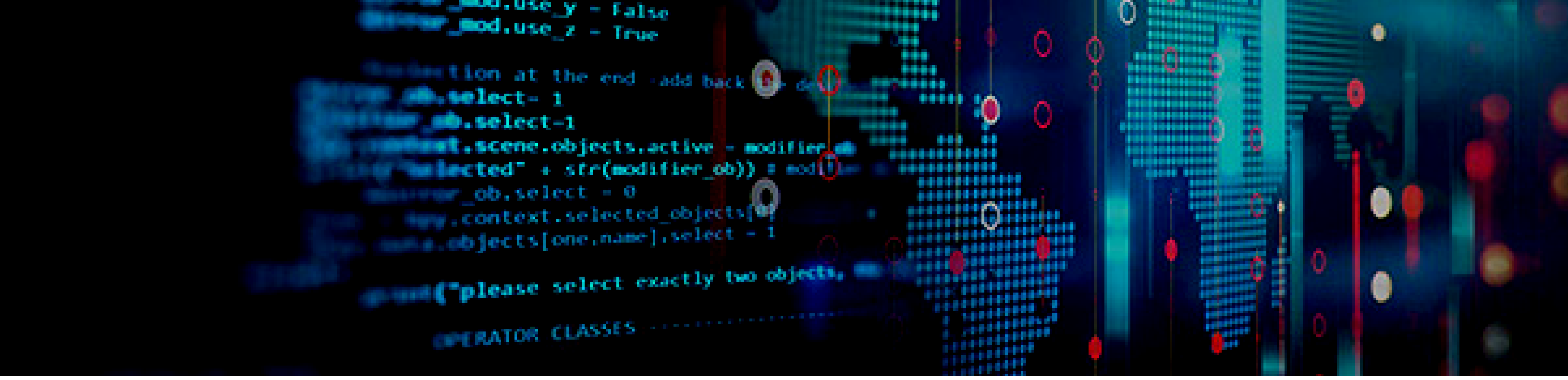
Red Hat Security Advisory 2022-2211-01

Red Hat Security Advisory 2022-2211-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-2194-01

Red Hat Security Advisory 2022-2194-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 3.1.419 and .NET Core Runtime 3.1.25. Issues addressed include a denial of service vulnerability.


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

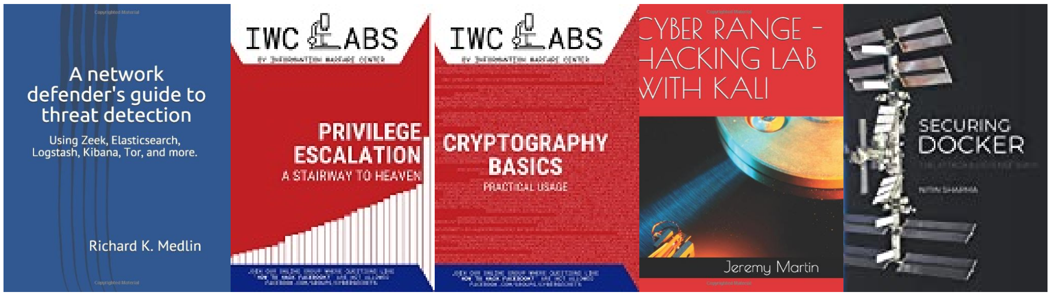


The Cyber Secrets publications on Amazon

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