May-30-22

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

May 30, 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

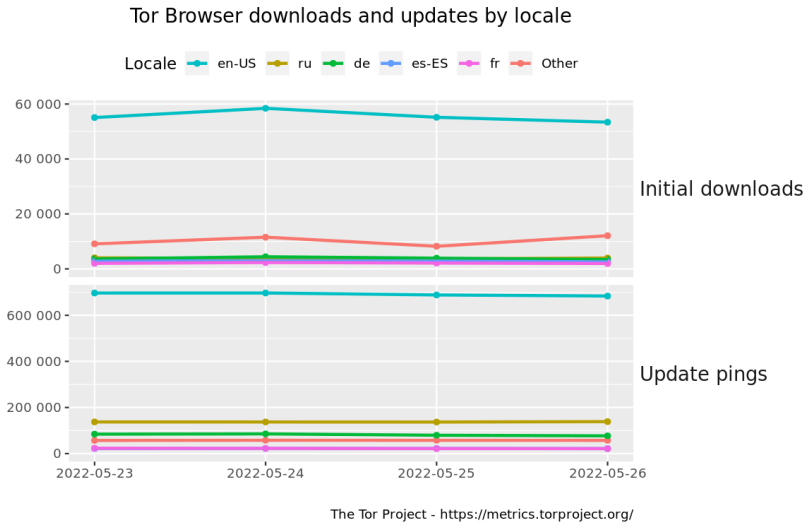
Internet Storm Center Infocon Status

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

* Surveillance Tech Didn't Stop The Uvalde Massacre
* Critical Flaws In Popular ICS Platform Can Trigger RCE
* GitHub Saved Plaintext Passwords Of npm Users In Log Files, Post Mortem Reveals
* Malware Uses PowerShell To Inject Malicious Extension Into Chrome
* Hacker Steals $1.4 Million In NFTs From Collector In One Sweep
* Suspected Phishing Email Crime Boss Cuffed In Nigeria
* Twitter Fined $150m For Handing Users' Contact Details To Advertisers
* Some QCT Servers Vulnerable To Pantsdown Flaw
* Hacker Steals Database Of Hundreds Of Verizon Employees
* Web App Attacks On The Rise In Healthcare
* Beijing Needs The Ability To Destroy Starlink, Say Chinese Researchers
* Quad Nations Pledge Deeper Collaboration On Infosec And More
* Zoom Patches XMPP Vulnerability Chain That Could Lead To Remote Code Execution
* Zuckerberg Sued By DC Attorney General Over Cambridge Analytica Data Scandal
* Fronton IOT Botnet Packs Disinformation Punch
* Cyber Feud Between Anonymous And Killnet Unlikely To Affect Others
* Hacker Leaks Mountain Of Files From Inside Xinjiang Camps
* These Are The Flaws That Let Hackers Attack Blockchain And DeFi Projects
* Snake Keylogger Spreads Through Malicious PDFs
* How To Find NPM Dependencies Vulnerable To Account Hijacking
* Clearview AI Fined In UK For Illegally Storing Facial Images
* Researchers Find Backdoor Lurking In WP Plugin Used By Schools
* Global Food Supply Chain At Risk From Malicious Hackers
* Strapi Exposed Data, Password Reset To Unprivileged Users
* 380K Kubernetes API Servers Exposed To Public Internet

Krebs on Security

* Senators Urge FTC to Probe ID.me Over Selfie Data
* When Your Smart ID Card Reader Comes With Malware
* 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

Dark Reading

* Critical OAS Bugs Open Industrial Systems to Takeover
* Exposed Kubernetes Clusters, Kubelet Ports Can Be Abused in Cyberattacks
* Space Force Expands Cyber Defense Operations
* Scammer Behind $568M International Cybercrime Syndicate Gets 4 Years
* New Chaos Malware Variant Ditches Wiper for Encryption
* ChromeLoader Malware Hijacks Browsers With ISO Files
* Physical Security Teams' Impact Is Far-Reaching
* Taking the Danger Out of IT/OT Convergence
* Microsoft Unveils Dev Box, a Workstation-as-a-Service
* Broadcom Snaps Up VMware in $61B Deal
* Lacework Announces Layoffs, Restructuring
* Third-Party Scripts on Websites Present a 'Broad & Open' Attack Vector
* Twitter Fined $150M for Security Data Misuse
* The FDA's New Cybersecurity Guidance for Medical Devices Reminds Us That Safety & Security Go Hand in
* VMware, Airline Targeted as Ransomware Chaos Reigns
* Big Cyber Hits on GM, Chicago Public Schools, & Zola Showcase the Password Problem
* Act Now: Leveraging PCI Compliance to Improve Security
* Quanta Servers Caught With 'Pantsdown' BMC Vulnerability
* Most Common Threats in DBIR
* Forescout Launches Forescout Frontline to Help Organizations Tackle Ransomware and Real Time Threats

The Hacker News

* Watch Out! Researchers Spot New Microsoft Office Zero-Day Exploit in the Wild
* New 'GoodWill' Ransomware Forces Victims to Donate Money and Clothes to the Poor
* FBI Warns About Hackers Selling VPN Credentials for U.S. College Networks
* New York Man Sentenced to 4 Years in Transnational Cybercrime Scheme
* Microsoft Finds Critical Bugs in Pre-Installed Apps on Millions of Android Devices
* Experts Detail New RCE Vulnerability Affecting Google Chrome Dev Channel
* Nearly 100,000 NPM Users' Credentials Stolen in GitHub OAuth Breach
* The Myths of Ransomware Attacks and How To Mitigate Risk
* Attackers Can Use Electromagnetic Signals to Control Touchscreens Remotely
* Zyxel Issues Patches for 4 New Flaws Affecting AP, API Controller, and Firewall Devices
* Critical 'Pantsdown' BMC Vulnerability Affects QCT Servers Used in Data Centers
* Experts Warn of Rise in ChromeLoader Malware Hijacking Users' Browsers
* Hackers Increasingly Using Browser Automation Frameworks for Malicious Activities
* The Added Dangers Privileged Accounts Pose to Your Active Directory
* Tails OS Users Advised Not to Use Tor Browser Until Critical Firefox Bugs are Patched

Security Week

* Exploitation of VMware Vulnerability Imminent Following Release of PoC
* Microsoft Finds Major Security Flaws in Pre-Installed Android Apps
* FBI: Higher Education Credentials Sold on Cybercrime Forums
* Google Announces New Chrome and Chrome OS Security Features for Enterprises
* Hundreds Stranded After Ransomware Attack on Indian Airline
* Spain to Tighten Control Over Secret Services After Spying Scandal
* SYN Ventures Closes $300M Fund for Cybersecurity Bets
* Cloud Security Firm Lacework Lays Off 20% of Workforce
* VMware to Absorb Broadcom Security Solutions Following $61 Billion Deal
* Greg Johnson to Take Reins as McAfee CEO
* QCT Servers Affected by 'Pantsdown' BMC Vulnerability
* Critical Vulnerabilities Found in Open Automation Software Platform
* Twitter to Pay $150M Penalty Over Privacy of Users' Data
* OT Remote Access Firm Xona Raises $7.2 Million in Series A Funding
* Alleged Cybercrime Ringleader Arrested in Nigeria
* Webinar Today: Missing Links for Managing OT Cyber Risk
* Tapping Neurodiverse Candidates Can Address Cybersecurity Skills Shortage
* Tidelift Raises $27 Million to Tackle Open Source Supply Chain Security
* WhiteSource Becomes Mend, Adds Automatic Code Remediation
* Two Cybersecurity Companies Offering Free Risk Assessments
* Notorious Vietnamese Hacker Turns Government Cyber Agent
* Chrome 102 Patches 32 Vulnerabilities
* Google Discloses Details of Zoom Zero-Click Remote Code Execution Exploit
* Trend Micro Patches Vulnerability Exploited by Chinese Cyberspies
* Video: Fireside Chat With Shane Huntley, Director at Google's Threat Analysis Group
* PyPI Served Malicious Version of Popular 'Ctx' Python Package

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* We Do Not Talk Enough About Social Engineering and It's Hurting Us
* The $44 Billion Smishing Problem and How to Not Be a Victim
* Collaring the (Alleged) Leader of a BEC Gang
* Verizon: Ransomware Involved in 25% of Data Breaches as Credentials and Phishing are Seen as "Key Pat
* That's Not Actually Elon Musk
* New Scam Uses Fraud Support Social Engineering to Take Victims for Thousands of Dollars
* Phishing Scammers Benefit from Shady SEO Practices to Rank Better Than Legitimate Domains
* New IRS Phishing Scam Uses Fake Notices to Steal Microsoft 365 Credentials
* FBI Director Warns of "Unprecedented" Cyberespionage Attacks Originating in China
* New Phishing Attack Uses Malicious Chatbot For Real Time Social Engineering

ISC2.org Blog

* (ISC)2 Supports Members with Thoughtful Response to SEC Proposed Rule on Cybersecurity Reporting
* Journey Into Cybersecurity - Conversations with Cyber Newcomers, Part 1
* (ISC)² Entry-Level Cybersecurity Certification Pilot Exam Reaches 1,000 Exam Milestone
* How to Prevent Burnout Among Cybersecurity Professionals Before, During and After a Breach
* (ISC)² Advocates for Membership - Shares Opinions on Proposed UK Standards and Pathway

HackRead

* 10 Application Security Best Practices To Follow In 2022
* How To Screencast on Windows 10
* ChromeLoader Browser Malware Spreading Via Pirated Games and QR Codes
* Cybercrime Syndicate Leader Behind Phishing and BEC Scams Arrested in Nigeria
* How Software Architects Can Manage Technical Debt in a Microservice Architecture
* Food For Files: GoodWill Ransomware demands food for the poor to decrypt locked files
* DuckDuckGo Allows Microsoft Trackers Despite No Tracking Policy - Researcher

Koddos

* 10 Application Security Best Practices To Follow In 2022
* How To Screencast on Windows 10
* ChromeLoader Browser Malware Spreading Via Pirated Games and QR Codes
* Cybercrime Syndicate Leader Behind Phishing and BEC Scams Arrested in Nigeria
* How Software Architects Can Manage Technical Debt in a Microservice Architecture
* Food For Files: GoodWill Ransomware demands food for the poor to decrypt locked files
* DuckDuckGo Allows Microsoft Trackers Despite No Tracking Policy - Researcher

Naked Security

* S3 Ep84: Government demand, Mozilla velocity, and Clearview fine [Podcast]
* Who's watching your webcam? The Screencastify Chrome extension story…
* Poisoned Python and PHP packages purloin passwords for AWS access
* Clearview AI face-matching service fined a lot less than expected
* Mozilla patches Wednesday's Pwn2Own double-exploit… on Friday!
* Microsoft patches the Patch Tuesday patch that broke authentication
* US Government says: Patch VMware right now, or get off our network
* S3 Ep83: Cracking passwords, patching Firefox, and Apple vulns [Podcast]
* Pwn2Own hacking schedule released - Windows and Linux are top targets
* Apple patches zero-day kernel hole and much more - update now!

Threat Post

* Critical Flaws in Popular ICS Platform Can Trigger RCE
* Cybergang Claims REvil is Back, Executes DDoS Attacks
* Link Found Connecting Chaos, Onyx and Yashma Ransomware
* Zoom Patches 'Zero-Click' RCE Bug
* Verizon Report: Ransomware, Human Error Among Top Security Risks
* Fronton IOT Botnet Packs Disinformation Punch
* Zero Trust for Data Helps Enterprises Detect, Respond and Recover from Breaches
* Snake Keylogger Spreads Through Malicious PDFs
* Closing the Gap Between Application Security and Observability
* 380K Kubernetes API Servers Exposed to Public Internet

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

* Multicloud complexity is a major operational challenge
* What is WebAssembly? The next-generation web platform explained
* Eclipse unveils Java binaries marketplace
* Reactive JavaScript: The evolution of front-end architecture
* How to work with String.Create in C#
* TypeScript 4.7 crosses the finish line
* Broadcom targets enterprise infrastructure with $61B VMware acquisition
* Microsoft .NET MAUI framework arrives
* Google gets serious about Gitops
* CockroachDB's 22.1 update aims to help prototype faster, scale on demand

C4ISRNET - Media for the Intelligence Age Military

* Army aviation exercise focuses on communicating with allies
* Air Force's Haugh confirmed as US Cyber Command deputy
* Government analysis of facial recognition tech must extend beyond privacy
* AI less about 'killer robots,' more about Pentagon transformation, Groen says
* National Reconnaissance Office expands use of commercial satellite imagery
* Marine Corps seeks 'information command' in Force Design 2030 update
* Military commands spent pandemic money on space analytics, IT upgrades
* Pentagon making progress on cybersecurity amid challenges, watchdog says
* Putin complains about barrage of cyberattacks
* Why Latin American partners need a better way to share intel than WhatsApp

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.

* Security Fest 2022
* SEETF 2022
* XeroCTF 2022 - Teaser
* BCACTF 3.0
* BSidesSF 2022 CTF
* n00bzCTF
* SunshineCTF 2022
* Grey Cat The Flag 2022
* Tenable CTF 2022
* Access Denied CTF 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

* I2P 1.8.0
* Deliverance 0.018-daf9452 File Descriptor Fuzzer
* TP-Link Backup Decryption Utility
* Lynis Auditing Tool 3.0.8
* 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

Kali Linux Tutorials

* Shhhloader : SysWhispers Shellcode Loader
* modifyCertTemplate : ADCS Cert Template Modification And ACL Enumeration
* Melody : A Transparent Internet Sensor Built For Threat Intelligence
* Maat : Open-source Symbolic Execution Framework
* Presshell : Quick And Dirty WordPress Command Execution Shell
* NimPackt-v1 : Nim-based Assembly Packer And Shellcode Loader For Opsec And Profit
* Wholeaked : A File-Sharing Tool That Allows You To Find The Responsible Person In Case Of A Leakage
* EvilSelenium : A Tool That Weaponizes Selenium To Attack Chromium Based Browsers
* LDAP shell : AD ACL Abuse
* Poro : Scan Publicly Accessible Assets On Your AWS Cloud Environment

GBHackers Analysis

* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3
* Pwn2Own - Windows 11, Microsoft Teams Hacked & Exploiting 16 Zero-day Bugs
* Hackers Exploiting a Critical Vulnerability in Zyxel Firewall & VPN Devices
* Multiple QNAP Flaws Let attackers to Access and Read Sensitive Data
* Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Learning to Combat Ransomware
* FOR509: Cloud Forensics & Incident Response Course - What to Expect
* Hunting Is Sacred, But We Never Do It for Sport! - SANS THIR Summit 2019

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

* Can Linux Aliases Steal Your Password? (Bash Bunny Demo)
* Live Hacking Q&A with Kody and Alex
* Protecting Ethical Hacking With The CFAA? Plus: Hacking Teslas With BLE - ThreatWire

The PC Security Channel [TPSC]

* Android Malware: SharkBot
* Windows Update Ransomware

Eli the Computer Guy

* ELON MUSK SUED by TWITTER SHAREHOLDERS
* GOOGLE TRACKING ILLEGAL ABORTIONS
* ELON MUSK accused of SEXUAL HARASSMENT
* BUMPY RIDE for Silicon Derby Robot Car

Security Now

* Dis-CONTI-nued: The End of Conti? - Clearview AI in Ukraine, Vancouver Pwn2Own, Voyager 1
* The New EU Surveillance State - Eventful Patch Tuesday, Open Source Maintenance Crew, BIG-IP Boxes

Troy Hunt

* Weekly Update 297

Intel Techniques: The Privacy, Security, & OSINT Show

* 263-Proton Changes & New Breach Lessons
* 262-Brief Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Tigase XMPP Server Stanza Smuggling
* ChromeOS usbguard Bypass
* qdPM 9.1 Remote Code Execution
* Print Spooler Remote DLL Injection
* Online Fire Reporting System 1.0 SQL Injection
* CLink Office 2.0 SQL Injection
* Zoom XMPP Stanza Smuggling Remote Code Execution
* iTop Remote Command Execution
* m1k1o's Blog 1.3 Remote Code Execution
* Blockchain FiatExchanger 2.2.1 SQL Injection
* Blockchain AltExchanger 1.2.1 SQL Injection
* OpenCart Newsletter 3.0.2.0 SQL Injection
* Linux USB Use-After-Free
* SAP Application Server ABAP / ABAP Platform Code Injection / SQL Injection / Missing Authorization
* LiquidFiles 3.4.15 Cross Site Scripting
* PHPIPAM 1.4.4 Cross Site Request Forgery / Cross Site Scripting
* Emby Media Server 4.7.0.60 Cross Site Scripting
* Trojan-Ransom.Thanos MVID-2022-0607 Code Execution
* SDT-CW3B1 1.1.0 Command Injection
* Online Discussion Forum Site 1.0 SQL Injection
* Showdoc 2.10.3 Cross Site Scripting
* OpenCart So Listing Tabs 2.2.0 Unsafe Deserialization
* T-Soft E-Commerce 4 SQL Injection
* T-Soft E-Commerce 4 Cross Site Scripting
* Survey Sparrow Enterprise Survey Software 2022 Cross Site Scripting

CXSecurity

* qdPM 9.1 Remote Code Execution (RCE) (Authenticated) (v2)
* Print Spooler Remote DLL Injection
* iTop Remote Command Execution
* 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

Proof of Concept (PoC) & Exploits

Exploit Database

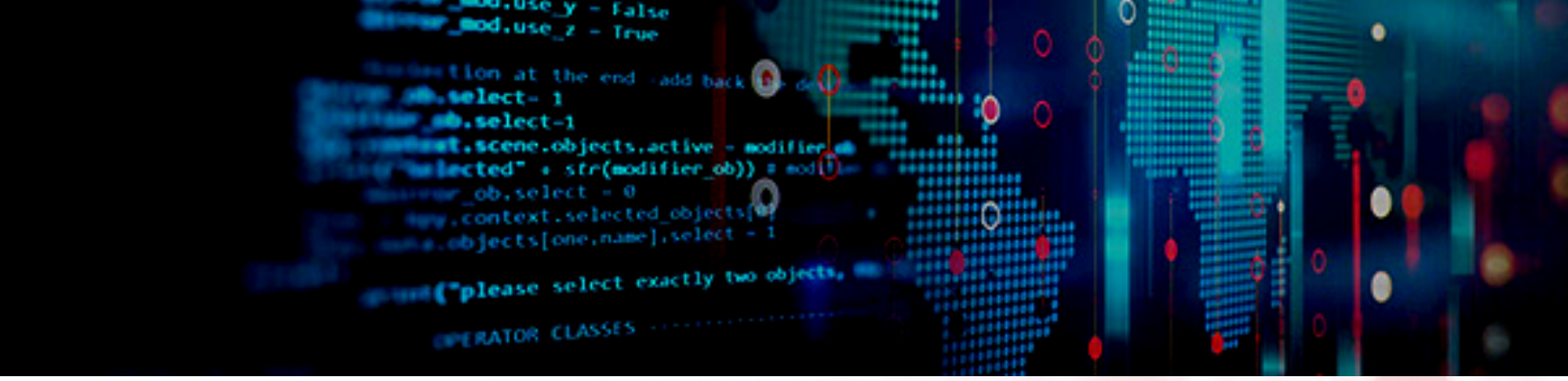
* [webapps] qdPM 9.1 - Remote Code Execution (RCE) (Authenticated) (v2)
* [webapps] m1k1o's Blog v.10 - Remote Code Execution (RCE) (Authenticated)
* [webapps] OpenCart v3.x Newsletter Module - Blind SQLi
* [webapps] Showdoc 2.10.3 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.0 - OS Command Injection
* [webapps] T-Soft E-Commerce 4 - SQLi (Authenticated)
* [webapps] T-Soft E-Commerce 4 - 'UrunAdi' Stored Cross-Site Scripting (XSS)
* [webapps] Survey Sparrow Enterprise Survey Software 2022 - Stored Cross-Site Scripting (XSS)
* [remote] SDT-CW3B1 1.1.0 - OS Command Injection
* [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

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

user@yourlinux:~$ *searchsploit keyword1 keyword2*

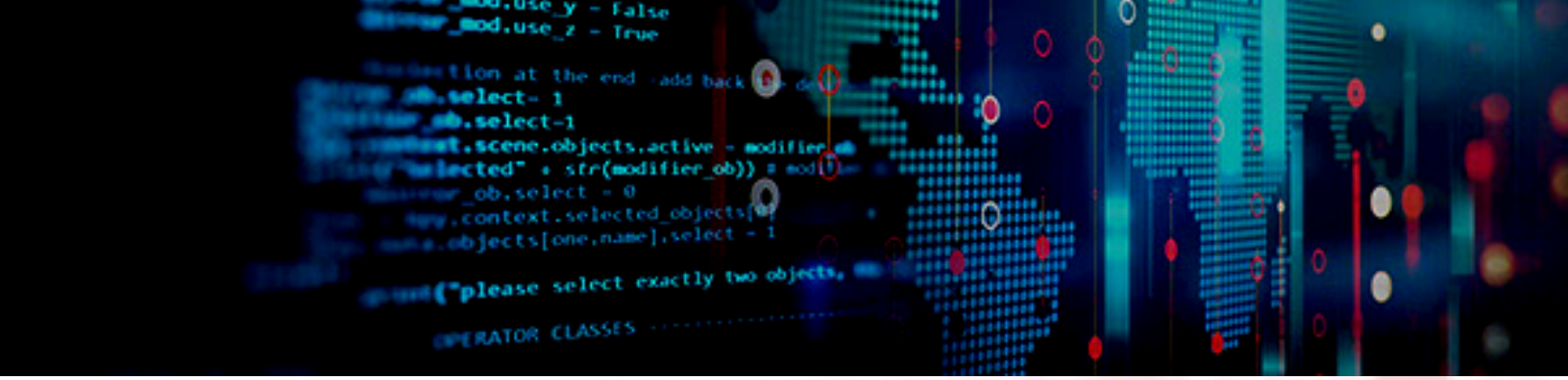
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.armstrong.gov.ar
https://www.armstrong.gov.ar notified by 1877
https://langsakota.go.id/lah.html
https://langsakota.go.id/lah.html notified by KatakBeracun
https://loei2.go.th/1975.html
https://loei2.go.th/1975.html notified by 1975 Team
https://nphl.gov.np/1975.html
https://nphl.gov.np/1975.html notified by 1975 Team
https://apnp.gov.ir/1337.php
https://apnp.gov.ir/1337.php notified by Matigan1337
https://amnat-ed.go.th/1975.html
https://amnat-ed.go.th/1975.html notified by 1975 Team
http://kuis.kpu-tangerangkab.go.id/idolsec.html
http://kuis.kpu-tangerangkab.go.id/idolsec.html notified by Melody-x48
http://rpp.kpu-tangerangkab.go.id/idolsec.html
http://rpp.kpu-tangerangkab.go.id/idolsec.html notified by Melody-x48
http://www.siproh.kpu-tangerangkab.go.id/idolsec.html
http://www.siproh.kpu-tangerangkab.go.id/idolsec.html notified by Melody-x48
http://aplikasi.kpu-tangerangkab.go.id/idolsec.html
http://aplikasi.kpu-tangerangkab.go.id/idolsec.html notified by Melody-x48
http://www.ppid.kpu-tangerangkab.go.id/idolsec.html
http://www.ppid.kpu-tangerangkab.go.id/idolsec.html notified by Melody-x48
http://www.northshoa.gov.et
http://www.northshoa.gov.et notified by 0xEv1lS0UL
http://rumahpintar.kpu-tangerangkab.go.id/407.php
http://rumahpintar.kpu-tangerangkab.go.id/407.php notified by Melody-x48
http://www.mhs-pao.go.th/zil.php
http://www.mhs-pao.go.th/zil.php notified by AnonCoders
https://pdpb.kpu-tangerangkab.go.id/idolsec.html
https://pdpb.kpu-tangerangkab.go.id/idolsec.html notified by PikunPe0ple
https://kpu-tangerangkab.go.id/README.html
https://kpu-tangerangkab.go.id/README.html notified by PikunPeople
http://cems.diw.go.th/sadme.htm
http://cems.diw.go.th/sadme.htm notified by typicalsadboy



Dark Web News

Darknet Live

[No Prison for Woman Who Received Four Kilos of Cocaine]

U.S. Senior District Court Judge Douglas P. Woodlock [sentenced] Michel Saredi-Munoz Moronta, 22, to time served (roughly 21 months) and four years of supervised release for her role in a drug trafficking conspiracy. In August 2020, law enforcement officers identified several USPS Priority Mail envelopes that contained cocaine. When law enforcement officers conducted surveillance at the delivery addresses in Lawrence, they saw a woman, later identified as Munoz Moronta, get out of her car and take possession of the packages. Police arrested her after she had collected all of the suspicious packages. The packages contained a total of four kilograms of cocaine. Cocaine trafficking sentences often involve incarceration. In December 2021, the defendant "pleaded guilty to one count of conspiracy to distribute and to possess with intent to distribute 500 grams or more of cocaine.” This fairly straightforward case involved the Federal Bureau of Investigation, U.S. Postal Inspection Service, and the Lawrence Police Department. United States Attorney Rachael S. Rollins' Narcotics & Money Laundering Unit prosecuted the case. United States Attorney Rachael S. Rollins announced the sentence. (via darknetlive.com at https://darknetlive.com/post/woman-avoids-prison-in-cocaine-case/)

[FBI: Academic Credentials for Sale on the Darkweb]

An alert from the FBI warns that compromised US academic credentials are being sold on the darkweb. A Private Industry Notification (PIN) from the Federal Bureau of Investigation (FBI) warns that investigators have identified compromised US academic credentials on forums, including at least one on the darkweb. Summary "The FBI is informing academic partners of identified US college and university credentials advertised for sale on online criminal marketplaces and publically accessible forums. This exposure of sensitive credential and network access information, especially privileged user accounts, could lead to subsequent cyber attacks against individual users or affiliated organizations.” Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums Threat "Cyber actors continue to conduct attacks against US colleges and universities, leading to the exposure of user information on public and cyber criminal forums. Credential harvesting against an organization is often a byproduct of spear-phishing, ransomware, or other cyber intrusion tactics. For example, in 2017, cyber criminals targeted universities to hack .edu accounts by cloning university login pages and embedding a credential harvester link in phishing emails. Successfully harvested credentials were then sent to the cyber criminals in an automated email from their servers. Such tactics have continued to prevail and ramped up with COVID-themed phishing attacks to steal university login credentials, according to security researchers from a US-based company in December 2021.” "The FBI has observed incidents of stolen higher education credential information posted on publically accessible online forums or listed for sale on criminal marketplaces. The exposure of usernames and passwords can lead to brute force credential stuffing computer network attacks, whereby attackers attempt logins across various internet sites or exploit them for subsequent cyber attacks as criminal actors take advantage of users recycling the same credentials across multiple accounts, internet sites, and services. If attackers are successful in compromising a victim account, they may attempt to drain the account of

stored value, leverage or re-sell credit card numbers and other personally identifiable information, submit fraudulent transactions, exploit for other criminal activity against the account holder, or use for subsequent attacks against affiliated organizations.” Examples _ As of January 2022, Russian cyber criminal forums offered for sale or posted for public access the network credentials and virtual private network accesses to a multitude of identified US-based universities and colleges across the country, some of which included screenshots as proof of access. Sites posting credentials for sale typically listed prices varying from a few to multiple thousands of US dollars. In May 2021, over 36,000 email and password combinations (some of which may have been duplicates) for email accounts ending in .edu were identified on a publically available instant messaging platform. The group posting the compromised data appeared to be involved in the trafficking of stolen login credentials and other cyber criminal activities. In late 2020, US territory-based university account usernames and passwords with the domain .edu were found for sale on the dark web. The seller listed approximately 2,000 unique usernames with accompanying passwords and asked for donations be made to an identified bitcoin wallet. As of early 2022, the site containing the credentials was no longer accessible. It surprises me that something as mundane as compromised academic credentials meets the threshold for a PIN. Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums pdf (via darknetlive.com at https://darknetlive.com/post/fbi-warns-of-hacked-edu-accounts-for-sale/)

ToRReZ Vendor "OnlyTheFinest" Enters Guilty Plea

A man with an address in Tampa, Florida, pleaded guilty to selling counterfeit Oxycodone pills on ToRReZ and Dark0de Reborn. Akshay Ram Kancharla, 26, pleaded guilty to a single count of distribution of fentanyl. According to court documents, Kancharla sold counterfeit Oxycodone pills containing fentanyl, counterfeit Xanax, counterfeit Adderall, and THC resin on ToRReZ and Dark0de Reborn. The defendant opened a vendor account on ToRReZ under the username "OnlyTheFinest” in August 2021. On October 7, 2021, an undercover FBI employee ordered ten counterfeit Oxycodone pills from OnlyTheFinest. Several days later, the feds received a package at the address they had provided to OnlyTheFinest. The return address on the envelope was an address in Tampa, Florida, and had a business name of "SKIN NUTRIENTS & ESSENTIALS, LLC.” Employees of the United States Postal Inspection Service (USPIS) reviewed USPS records for the package's tracking number. Records indicated that someone with an I.P. address in Tampa, Florida, had tracked the package. USPIS employees then searched for other packages tracked by the same I.P. address. They found that someone with the same I.P. address had tracked several packages addressed to an address on the 16000 block of Colchester Palms Drive in Tampa, Florida. This is stealth?

On October 22, 2021, Coinbase provided the investigators with the information on two accounts associated with the address on Colchester Palms Drive. Both accounts belonged to Kancharla. Kancharla had sent Coinbase a picture of himself and a picture of his driver's license. Investigators matched the pictures, confirming that the operator of the Coinbase account was Kancharla. On October 30, 2021, an undercover fed messaged OnlyTheFinest on ToRReZ and asked if the vendor would "conduct a direct deal off of the D.M.” The vendor provided the fed with the Wickr username "farmgod1.” When the fed contacted the vendor through Wickr, the vendor wrote, "hello there, onlythefinest here!” The same day, the undercover fed purchased 50 pressed Oxycodone pills and 20 Adderall pills from the vendor on Wickr. The vendor provided the fed with a Bitcoin address where he would receive payment. Several days later, feds received a package at the address sent through Wickr. The package had the same business name of "SKIN NUTRIENTS & ESSENTIALS, LLC.” "When law enforcement conducts investigations involving virtual currency, they sometimes use commercial services offered by several different blockchain-analysis companies. These companies analyze the Bitcoin blockchain and attempt to identify the individuals or groups involved in transactions. Specifically, these companies have developed proprietary software that analyzes all the data underlying each Bitcoin transaction on the Bitcoin blockchain and then groups related Bitcoin transactions into "clusters” based on that analysis. The methods employed by these blockchain analysis companies have been independently validated by computer scientists, who have shown that these "clustering” techniques provide accurate results. Additionally, through numerous, unrelated investigations, law enforcement has been able to corroborate the accuracy of the information provided via these third-party services.”

Analysis of the Bitcoin address provided by farmgod1 for payment in connection with the October 30, 2021, controlled purchase revealed that the Bitcoin address was associated with Square. Investigators obtained records from Square, which indicated Kancharla had registered the account. On November 3, 2021, law enforcement conducted surveillance at Kancharla's residence. They watched him leave his house and drive to a UPS store. After he had left the store, law enforcement officers entered the store and asked the employee behind the counter if they could see any packages dropped off by Kancharla. The employee showed the police six packages, each with the sender name "SKIN NUTRIENTS & ESSENTIALS LLC” or "Akshay Kancharla.” Between the November 3, 2021, trip to the UPS store and ToRReZ Market's retirement in December, investigators conducted several controlled purchases through Wickr. In some instances, police intercepted the package they had ordered by following the defendant to the UPS store and watching him drop off packages. On January 27, 2022, investigators conducted a review on DarkOde Reborn for the vendor profile OnlyTheFinest. On the market, OnlyTheFinest had completed 73 transactions and received 26 reviews. On ToRRez market, Kancharla sold over $73,096 in controlled substances and completed over 264 transactions by December 21, 2021, including sales of 7,375 pressed Oxycodone pills. On Dark0de Reborn, he sold over $39,793 in controlled substances, including rated orders for 3,975 pressed Oxycodone pills sold. Investigators compared the PGP listed by OnlyTheFinest on DarkOde Reborn with the PGP listed on ToRReZ, which revealed they were the same. On February 17, 2022, police executed a search warrant at the defendant's residence. During the search, officers found pressed Oxycodone pills weighing approximately 2.38 kilograms, pressed Xanax bars weighing 437.5 grams, marijuana, $30,140 in U.S. currency, and approximately 2.444 in Bitcoin. Kancharla's sentencing hearing is scheduled for August 4. He faces a maximum penalty of 20 years in prison. Darknet Vendor of Fentanyl-Laced Pills Pleads Guilty archive.is, archive.org, justice.gov Complaint pdf Plea Agreement pdf Recon appears to be down, otherwise I would pull up the vendor's profile. (via darknetlive.com at https://darknetlive.com/post/darkweb-vendor-admits-selling-fake-oxys/)

PSA: Serious Security Vulnerability in Tor Browser

HugBunter, who is apparently alive, posted a PSA on Dread about a vulnerability in all FireFox versions HugBunter: _ "Upgrade Tor Browser to the latest release (11.0.13) immediately where possible and ensure you have JavaScript Disabled in Tor Browser at all times, as always. This vulnerability is present in Firefox, and so affects all previous Tor Browser versions Source: dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/4313ca4ac715d83505c0

__ Update to Tor Browser version 11.0.13 as soon as possible. Tails: _ Tor Browser in Tails 5.0 and earlier is unsafe to use for sensitive information. We recommend that you stop using Tails until the release of 5.1 (May 31) if you use Tor Browser for sensitive information (passwords, private messages, personal information, etc.). A security vulnerability was discovered in the JavaScript engine of Firefox and Tor Browser. See the Mozilla Foundation Security Advisory 2022-19 This vulnerability allows a malicious website to bypass some of the security built in Tor Browser and access information from other websites. For example, after you visit a malicious website, an attacker controlling this website might access the password or other sensitive information that you send to other websites afterwards during the same Tails session. This vulnerability doesn't break the anonymity and encryption of Tor connections. For example, it is still safe and anonymous to access websites from Tails if you don't share sensitive information with them. After Tor Browser has been compromised, the only reliable solution is to restart Tails. Other applications in Tails are not vulnerable. Thunderbird in Tails is not vulnerable because JavaScript is disabled. The Safest security level of Tor Browser is not affected because JavaScript is disabled at this security level. Mozilla is aware of websites exploiting this vulnerability already. This vulnerability will be fixed in Tails 5.1 (May 31), but our team doesn't have the capacity to publish an emergency release earlier. Source: tails.boum.org/security/prototype_pollution/index.en.html The Tor Project's Blog: _ Tor Browser 11.0.13 is now available from the Tor Browser download page and also from our distribution directory. This version includes important security updates to Firefox. We also updated Tor to 0.4.7.7 (the first stable Tor release with support for congestion control). Note: the Android version 11.0.13 will be available later during the week. The full changelog since Tor Browser 11.0.12 is: Android Bug fenix#40212: Tor Browser crashing on launch All

Platforms Update Tor to 0.4.7.7 Bug tor-browser#40967: Integrate Mozilla fix for Bug 1770137 Bug tor-browser#40968: Integrate Mozilla fix for Bug 1770048 Build System All Platforms Update Go to 1.17.10 Bug tor-browser-build#40319: Add build tag to downloads.json Bug tor-browser-build#40486: Add tools/signing/do-all-signing script, and other signing scripts improvements Source: pzhdfe7jraknpj2qgu5cz2u3i4deuyfwmonvzu5i3nyw4t4bmg7o5pad.onion/new-release-tor-browser-11013/index.html CVE-2022-1802: Prototype pollution in Top-Level Await implementation _ Reporter: Manfred Paul via Trend Micro's Zero Day Initiative Impact: critical Description _ If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. References _ Bug 1770137 Source: www.mozilla.org/en-US/security/advisories/mfsa2022-19/ CVE-2022-1529: Untrusted input used in JavaScript object indexing, leading to prototype pollution _ Reporter: Manfred Paul via Trend Micro's Zero Day Initiative Impact: critical Description _ An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. References _ Bug 1770048 Source: www.mozilla.org/en-US/security/advisories/mfsa2022-19/ __ ???? (via darknetlive.com at https://darknetlive.com/post/psa-security-vuln-in-tor-browser/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now

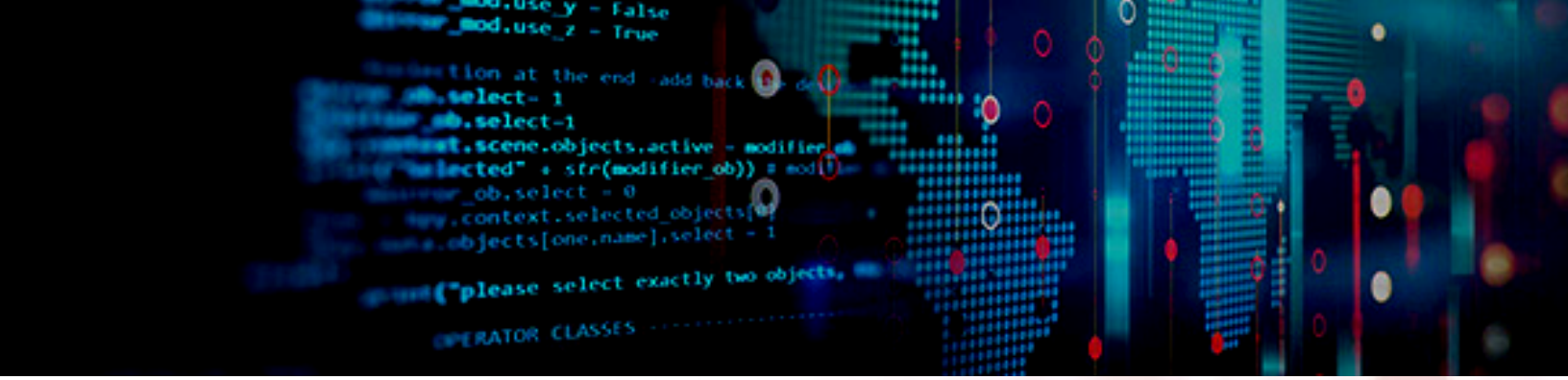
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, 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

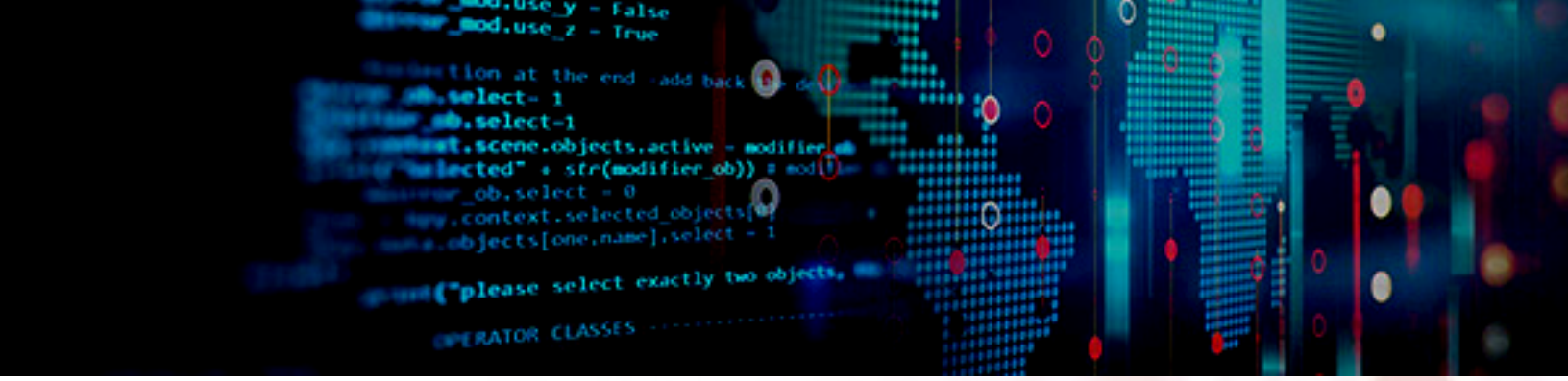
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-Up
* The Forecast Is Flipped: Flipping L&D Enables Managers to Be Impact Multipliers
* The Rapid7 Sales Culture and Experience: An Inside Look From 2 VPs
* [Security Nation] Omer Akgul and Richard Roberts on YouTube VPN Ads
* What It Takes to Securely Scale Cloud Environments at Tech Companies Today
* CVE-2022-22977: VMware Guest Authentication Service LPE (FIXED)
* A Year on from the Ransomware Task Force Report
* DFIR Without Limits: Moving Beyond the "Sucker's Choice" of Today's Breach Response Services
* Metasploit Weekly Wrap-Up
* Are You in the 2.5% Who Meet This Cybersecurity Job Requirement?



Advisories

US-Cert Alerts & bulletins

* Drupal Releases Security Updates
* Citrix Releases Security Updates for ADC and Gateway
* CISA and DoD Release 5G Security Evaluation Process Investigation Study
* Google Releases Security Updates for Chrome
* CISA Adds 34 Known Exploited Vulnerabilities to Catalog
* CISA Adds 20 Known Exploited Vulnerabilities to Catalog
* Mozilla Releases Security Products for Multiple Firefox Products
* CISA Adds 21 Known Exploited Vulnerabilities to Catalog
* AA22-138B: Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control
* AA22-138A: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388
* Vulnerability Summary for the Week of May 16, 2022
* Vulnerability Summary for the Week of May 9, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-4774-01

Red Hat Security Advisory 2022-4774-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.1.

Red Hat Security Advisory 2022-4773-01

Red Hat Security Advisory 2022-4773-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.1.

Red Hat Security Advisory 2022-2263-01

Red Hat Security Advisory 2022-2263-01 - 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 4.6.58. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2022-2265-01

Red Hat Security Advisory 2022-2265-01 - 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 4.6.58.

Red Hat Security Advisory 2022-4764-01

Red Hat Security Advisory 2022-4764-01 - The ovirt-host package consolidates host package requirements into a single meta package. Issues addressed include a Bugzilla fix for vdsm where there was a disclosure of sensitive values in log files.

Ubuntu Security Notice USN-5450-1

Ubuntu Security Notice 5450-1 - Evgeny Kotkov discovered that subversion servers did not properly follow path-based authorization rules in certain cases. An attacker could potentially use this issue to retrieve information about private paths. Thomas Weißschuh discovered that subversion servers did not properly handle memory in certain configurations. A remote attacker could potentially use this issue to cause a denial of service or other unspecified impact.

Red Hat Security Advisory 2022-4711-01

Red Hat Security Advisory 2022-4711-01 - The ovirt-engine package provides the Red Hat Virtualization Manager, a centralized management platform that allows system administrators to view and manage virtual machines. The Manager provides a comprehensive range of features including search capabilities, resource management, live migrations, and virtual infrastructure provisioning. Issues addressed include cross site scripting and denial of service vulnerabilities.

Red Hat Security Advisory 2022-2264-01

Red Hat Security Advisory 2022-2264-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.6.58.

Red Hat Security Advisory 2022-4712-01

Red Hat Security Advisory 2022-4712-01 - The ovirt-engine package provides the Red Hat Virtualization Manager, a centralized management platform that allows system administrators to view and manage virtual machines. The Manager provides a comprehensive range of features including search capabilities, resource management, live migrations, and virtual infrastructure provisioning. The ovirt-ansible-hosted-engine-setup package provides an Ansible role for deploying Red Hat Virtualization Hosted-Engine.

Ubuntu Security Notice USN-5449-1

Ubuntu Security Notice 5449-1 - It was discovered that libXv incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5448-1

Ubuntu Security Notice 5448-1 - It was discovered that ncurses was not properly checking array bounds when executing the fmt_entry function, which could result in an out-of-bounds write. An attacker could possibly use this issue to execute arbitrary code. It was discovered that ncurses was not properly checking user input, which

could result in it being treated as a format argument. An attacker could possibly use this issue to expose sensitive information or to execute arbitrary code.

Ubuntu Security Notice USN-5402-2

Ubuntu Security Notice 5402-2 - USN-5402-1 fixed several vulnerabilities in OpenSSL. This update provides the corresponding update for Ubuntu 16.04 ESM. Elison Niven discovered that OpenSSL incorrectly handled the c_rehash script. A local attacker could possibly use this issue to execute arbitrary commands when c_rehash is run. Aliaksei Levin discovered that OpenSSL incorrectly handled resources when decoding certificates and keys. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS.

Ubuntu Security Notice USN-5447-1

Ubuntu Security Notice 5447-1 - It was discovered that logrotate incorrectly handled the state file. A local attacker could possibly use this issue to keep a lock on the state file and cause logrotate to stop working, leading to a denial of service.

Red Hat Security Advisory 2022-2272-01

Red Hat Security Advisory 2022-2272-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.8.41.

Ubuntu Security Notice USN-5446-1

Ubuntu Security Notice 5446-1 - Max Justicz discovered that dpkg incorrectly handled unpacking certain source packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could modify files outside the target unpack directory, leading to a denial of service or potentially gaining access to the system.

Red Hat Security Advisory 2022-2268-01

Red Hat Security Advisory 2022-2268-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.7.51.

Ubuntu Security Notice USN-5445-1

Ubuntu Security Notice 5445-1 - Ace Olszowka discovered that Subversion incorrectly handled certain svnserve requests. A remote attacker could possibly use this issue to cause svnserver to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. Tomas Bortoli discovered that Subversion incorrectly handled certain svnserve requests. A remote attacker could possibly use this issue to cause svnserver to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS.

Red Hat Security Advisory 2022-4745-01

Red Hat Security Advisory 2022-4745-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-2283-01

Red Hat Security Advisory 2022-2283-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.9.35.

Ubuntu Security Notice USN-5404-2

Ubuntu Security Notice 5404-2 - USN-5404-1 addressed a vulnerability in Rsyslog. This update provides the corresponding update for Ubuntu 16.04 ESM. Pieter Agten discovered that Rsyslog incorrectly handled certain requests. An attacker could possibly use this issue to cause a crash.

Red Hat Security Advisory 2022-4729-01

Red Hat Security Advisory 2022-4729-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.9.1 ESR.

Red Hat Security Advisory 2022-4730-01

Red Hat Security Advisory 2022-4730-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This

update upgrades Thunderbird to version 91.9.1.

Red Hat Security Advisory 2022-4721-01

Red Hat Security Advisory 2022-4721-01 - 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 a privilege escalation vulnerability.

Ubuntu Security Notice USN-5439-1

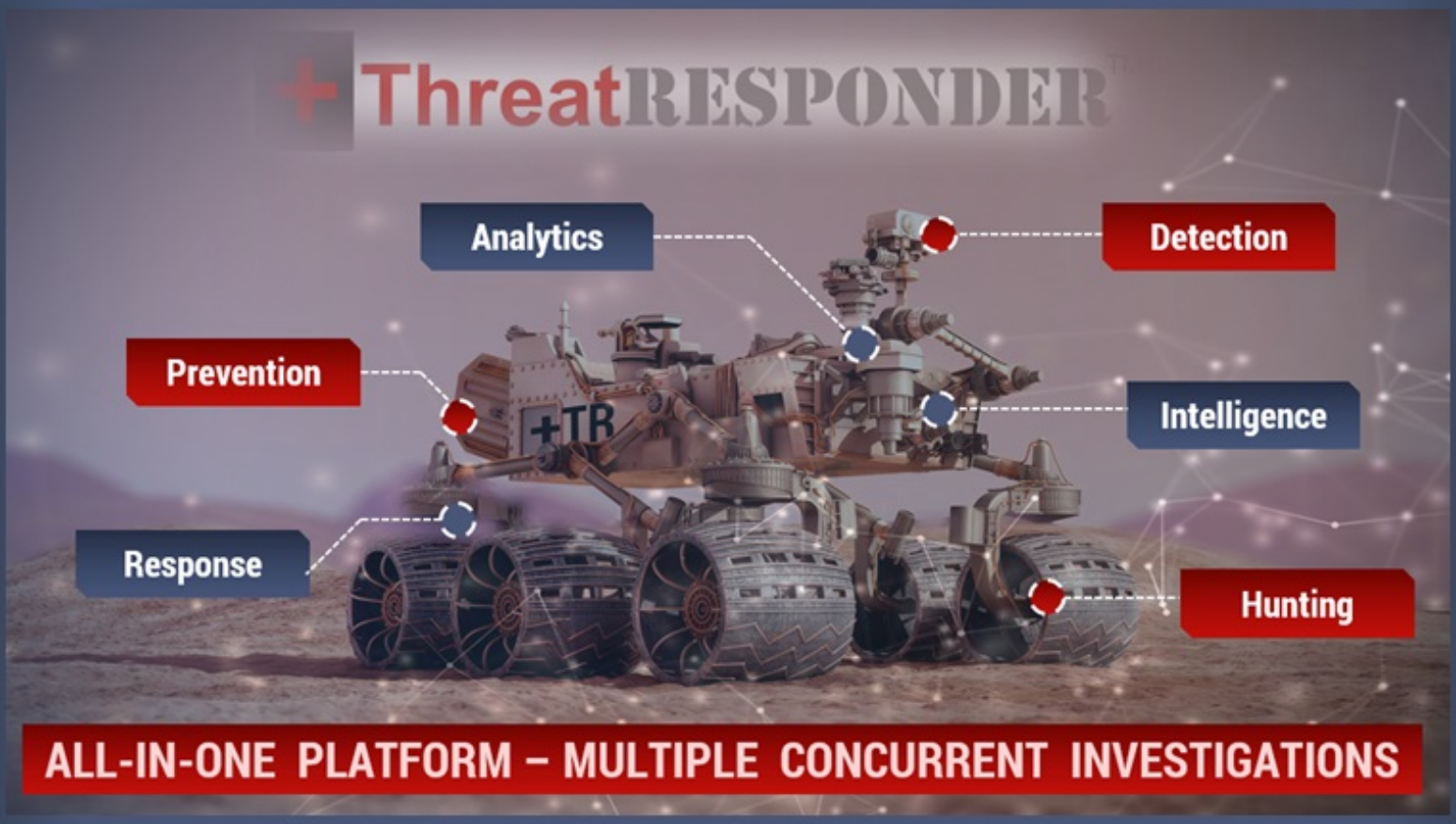
Ubuntu Security Notice 5439-1 - Gunnar Hjalmarsson discovered that AccountsService incorrectly dropped privileges. A local user could possibly use this issue to cause AccountsService to crash or stop responding, resulting in a denial of service.

Are You...

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

Do DFIR Investigations Better

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



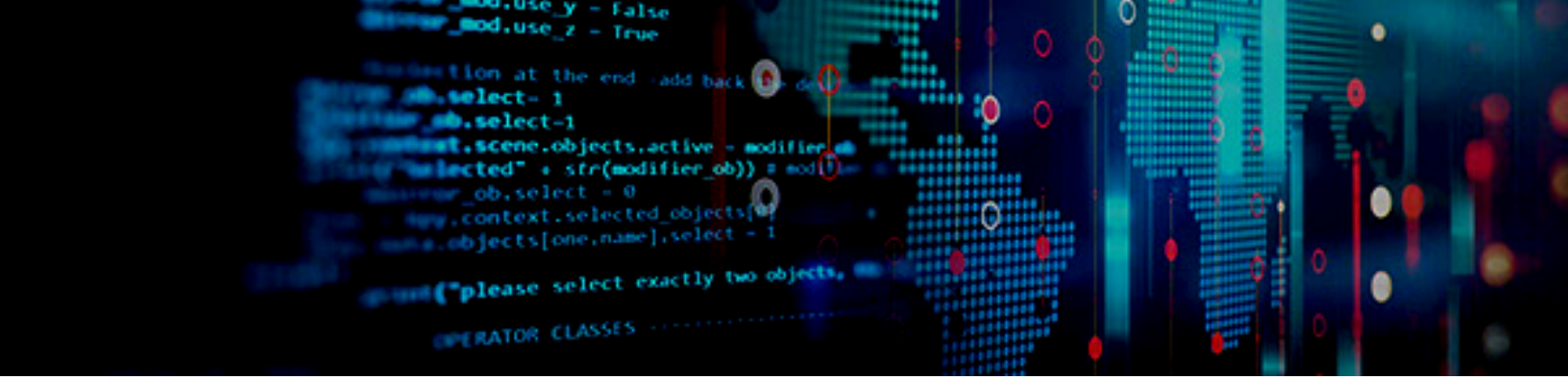
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

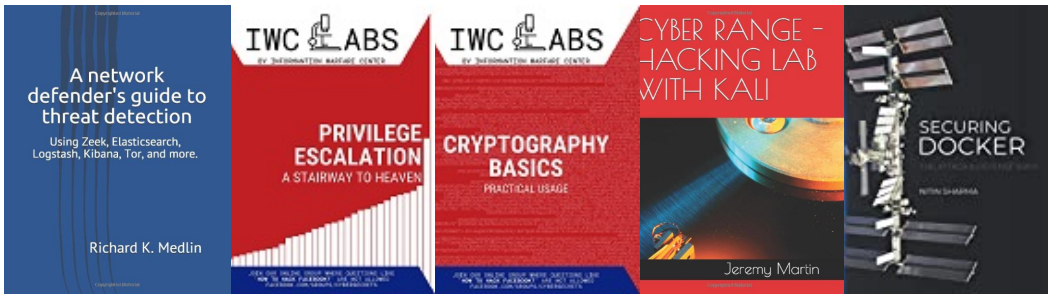


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP