Jan-03-22

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

January 3, 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

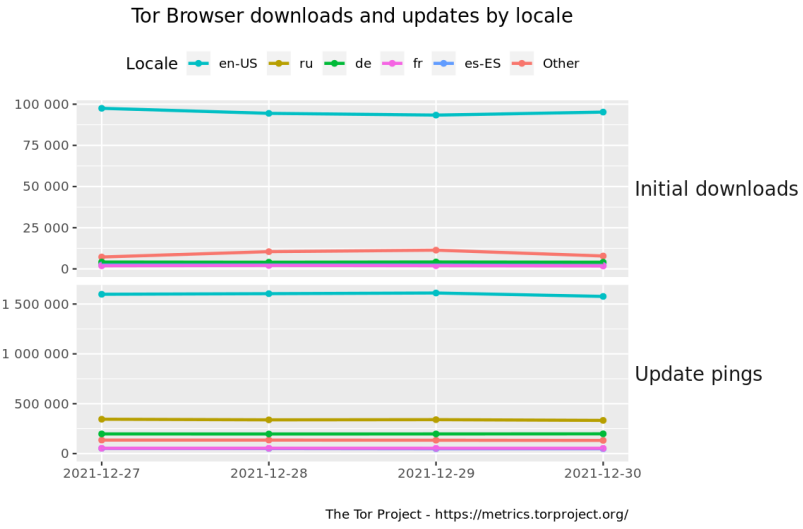
Internet Storm Center Infocon Status

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

* Chinese Espionage Group Leveraged Log4j Bug In VMware
* Polish Prosecutors Decline To Investigate Phone Hacking Allegation
* Cryptomining Attack Exploits Docker API Misconfig Since 2019
* That Toy You Got For Christmas Could Be Spying On You
* T-Mobile Reportedly Suffers Another Data Breach
* Nation State Actors Are Posing Greater Threats
* The 5 Most Wanted Threatpost Stories Of 2021
* Polish Senator Says Prosecutors Dragging Feet Over Phone Hacking
* Shutterfly Reports Ransomware Incident
* Apache's New Security Update For HTTPD Server Fixes Two Flaws
* Log4j Makes Waves In The US Financial Industry
* Four Bugs In Microsoft Teams Left Platform Vulnerable Since March
* US Intel And Satellite Images Show Saudi Arabia Is Now Building Its Own Ballistic Missiles With Help
* Ubisoft Confirms Just Dance Data Breach
* The Secret Uganda Deal That Has Brought NSO To The Brink of Collapse
* Walk-Through Metal Detectors Can Be Hacked, New Research Finds
* The Cybersecurity Stories Vice Was Jealous Of In 2021
* FBI: Hackers Are Actively Exploiting This Flaw On ManageEngine Desktop Central Servers
* Conti Ransomware Gang Has Full Log4Shell Attack Chain
* Evil Corp Is Dodging Sanctions By Dressing Up As REvil
* How The Matrix Inspired A New Generation Of Hackers
* Scammers Stole $7.7 Billion In Crypto In 2021
* Bad Things Come In Threes: Apache Reveals Another Log4j Bug
* Google Warns That NSO Hacking Is On Par WIth Elite Nation-State Spies
* BBC Bitcoin Mining Report Used In Crypto-Scam

Krebs on Security

* Happy 12th Birthday, KrebsOnSecurity.com!
* NY Man Pleads Guilty in $20 Million SIM Swap Theft
* Microsoft Patch Tuesday, December 2021 Edition
* Inside Ireland's Public Healthcare Ransomware Scare
* Canada Charges Its "Most Prolific Cybercriminal"
* Who Is the Network Access Broker 'Babam'?
* Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach"
* The Internet is Held Together With Spit & Baling Wire
* Arrest in 'Ransom Your Employer' Email Scheme
* The 'Zelle Fraud' Scam: How it Works, How to Fight Back

Dark Reading

* Name That Edge Toon: In Your Face!
* Creating the Next Generation of Secure Developers
* Adding Resiliency to BGP Avoids Network Outages, Data Loss
* Getting Started With Threat-Informed Security Programs
* Zero Trust and Access: Protecting the Keys to the Kingdom
* In the Fight Against Cybercrime, Takedowns Are Only Temporary
* Why Cyber Due Diligence Is Essential to the M&A Process
* 7 Steps for Navigating a Zero-Trust Journey
* The Log4j Flaw Will Take Years to be Fully Addressed
* After Google's Landmark Settlement, How Ad Networks Should Tackle Child Privacy
* AV-Comparatives Reveals Results of Long-Term Tests of 19 Leading Endpoint Security Solutions
* An Adaptive Security Strategy Is Critical for Stopping Advanced Attacks
* A Year in Microsoft Bugs: The Most Critical, Overlooked & Hard to Patch
* How Do I Reduce the Risk of an Insider Threat?
* The CISO as Sustaining Force: Helping Infosec Staff Beat Burnout
* 6 Security-Tech Innovations We're Excited to See in 2022
* Log4j: A CISO's Practical Advice
* The Future of Work Has Changed, and Your Security Mindset Needs to Follow
* 7 of the Most Impactful Cybersecurity Incidents of 2021
* Microsoft Customer Source Code Exposed via Azure App Service Bug

The Hacker News

* Detecting Evasive Malware on IoT Devices Using Electromagnetic Emanations
* Are Medical Devices at Risk of Ransomware Attacks?
* Microsoft Issues Fix for Exchange Y2K22 Bug That Crippled Email Delivery Service
* New iLOBleed Rootkit Targeting HP Enterprise Servers with Data Wiping Attacks
* Chinese APT Hackers Used Log4Shell Exploit to Target Academic Institution
* Ongoing Autom Cryptomining Malware Attacks Using Upgraded Evasion Tactics
* New Apache Log4j Update Released to Patch Newly Discovered Vulnerability
* Experts Detail Logging Tool of DanderSpritz Framework Used by Equation Group Hackers
* Garrett Walk-Through Metal Detectors Can Be Hacked Remotely
* PECB Certified Lead Ethical Hacker: Take Your Career to the Next Level
* 'Spider-Man: No Way Home' Pirated Downloads Contain Crypto-Mining Malware
* New Android Malware Targeting Brazil's Itaú Unibanco Bank Customers
* Expert Details macOS Bug That Could Let Malware Bypass Gatekeeper Security
* New Ransomware Variants Flourish Amid Law Enforcement Actions
* New BLISTER Malware Using Code Signing Certificates to Evade Detection

Security Week

* Shopping Platform PulseTV Discloses Potential Breach Impacting 200,000 People
* Sophisticated iLOBleed Rootkit Targets HP Servers
* Quantum Computing Is for Tomorrow, But Quantum-Related Risk Is Here Today
* Multiple Vulnerabilities Impact Netgear Nighthawk R6700 Routers
* Israeli Media Outlets Hacked on Soleimani Killing Anniversary
* ACLU Demands Answers About Transit Agency Data Breach
* Cybersecurity M&A Roundup: 35 Deals Announced in December 2021
* A New Year Will Bring New Targets: What to Look for in 2022
* What to Expect in 2022: Microservices Will Bring Macro Threats
* LastPass Automated Warnings Linked to 'Credential Stuffing' Attack
* Chinese Spies Exploit Log4Shell to Hack Major Academic Institution
* The Right to Work and Non-Competes in the Security Industry
* Storage Devices of Major Vendors Impacted by Encryption Software Flaws
* Another Remote Code Execution Vulnerability Patched in Log4j
* Norwegian Media Firm Amedia Suffers Disruption Due to Cyberattack
* Poland's Tusk Calls Spyware Use 'Crisis for Democracy'
* Researchers Dive Into Equation Group Tool 'DoubleFeature'
* The Human Connection: A Mindset for the Coming Year
* Threat Actors Abuse MSBuild for Cobalt Strike Beacon Execution
* State Workers to Be Paid on Time Despite Ransomware Attack
* Shutterfly Says Ransomware Attack Impacted Manufacturing
* DuckDuckGo Signals Entry Into Desktop Browser Market
* High-Risk Flaw Haunts Apache Server
* IT Services Firm Inetum Discloses Ransomware Attack
* Jackson Public Schools Ups Cybersecurity After Hacker Attack

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* 2022 Resolution: "I'll Be A Certified Security Awareness and Culture Professional (SACP)â„¢"
* Amazon Token Crypto "Presale" Scam Takes Advantage of News Hype and Steals Your Real Cryptocurrency
* New "Karakurt" Threat Group is Gaining Attention Through Multiple and Frequent Extortion Attacks
* Omicron-Themed Phishing Campaign is Running Rampant
* Organizations Worldwide Experience Over 722 Million Attacks in the Last 30 Days!
* 5 Notable Obscure Phishing Scams
* Conti Ransomware Affiliate Attacks Australian Utilities Giant's Corporate Network
* Google Takes a Step Towards Reducing the Use of Calendar Invitations as Phishing Tools
* CyberheistNews Vol 11 #51 [Heads Up] Phishing Attacks Remain the Top Type of Cybersecurity Breach Thi
* West Virginia Healthcare Breach Traced to Phishing

ISC2.org Blog

* What's Next for Cybersecurity in 2022?
* What Were the Best Cybersecurity Webinars of 2021?
* Looking Back at 2021 and Forward to 2022
* 2021 (ISC)² Leadership Webinars On-Demand
* What do cybersecurity experts predict in 2022?

HackRead

* N Korean hackers stole $1.7 billion from cryptocurrency exchanges
* Research claims Samsung Galaxy Store apps are spreading malware
* Error prompted LastPass to send false breach alerts to users
* MSP vs MSSP: What's The Difference?
* T-Mobile's latest data breach exposed users to SIM swapping attacks
* How to Develop Complex Marketing Operations with "No Code" Tools
* Logistics giant D.W. Morgan exposed 100 GB worth of clients' data

Koddos

* N Korean hackers stole $1.7 billion from cryptocurrency exchanges
* Research claims Samsung Galaxy Store apps are spreading malware
* Error prompted LastPass to send false breach alerts to users
* MSP vs MSSP: What's The Difference?
* T-Mobile's latest data breach exposed users to SIM swapping attacks
* How to Develop Complex Marketing Operations with "No Code" Tools
* Logistics giant D.W. Morgan exposed 100 GB worth of clients' data

Naked Security

* Instagram copyright infringment scams - don't get sucked in!
* Log4Shell vulnerability Number Four: "Much ado about something"
* SFW! The Top N Cybersecurity Stories of 2021 (for small positive integer values of N)
* The cool retro phone with a REAL DIAL… plus plenty of IoT problems
* Plundered bitcoins recovered by FBI - all 3,879-and-one-sixth of them!
* Apache's other product: Critical bugs in 'httpd' web server, patch now!
* Log4Shell: The Movie… a short, safe visual tour for work and home
* Serious Security: OpenSSL fixes "error conflation" bugs - how mixing up mistakes can lead to trouble
* S3 Ep63: Log4Shell (what else?) and Apple kernel bugs [Podcast+Transcript]
* Apple security updates are out - and not a Log4Shell mention in sight

Threat Post

* What the Rise in Cyber-Recon Means for Your Security Strategy
* APT 'Aquatic Panda' Targets Universities with Log4Shell Exploit Tools
* Threat Advisory: E-commerce Bots Use Domain Registration Services for Mass Account Fraud
* Cryptomining Attack Exploits Docker API Misconfiguration Since 2019
* 5 Cybersecurity Trends to Watch in 2022
* That Toy You Got for Christmas Could Be Spying on You
* 2021 Wants Another Chance (A Lighter-Side Year in Review)
* Global Cyberattacks from Nation-State Actors Posing Greater Threats
* The 5 Most-Wanted Threatpost Stories of 2021
* 4-Year-Old Microsoft Azure Zero-Day Exposes Web App Source Code

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

* Everything You Need To Know About Ransomware Attacks and Gangs In 2022
* Intelligent Adversary Engagement: Deceiving the Attacker
* Changing the Conversation with Risk Quantification
* 2021 Zero Trust Security Intelligence Roundup
* 2021 Manufacturing and Supply Chain Security Roundup
* Ransomware Attackers' New Tactic: Double Extortion
* Cyber Warfare: What To Expect in 2022
* Why CISOs Shouldn't Report to CIOs in the C-Suite
* What Cybersecurity Professionals Are Wishing for This Holiday Season
* A Journey in Organizational Resilience: Survive the Disruption and Become Stronger

InfoWorld

* 8 steps to better DNS
* Is Amazon Alexa a success?
* Virtual whiteboards prove vital for remote developer teams
* What most cloud-using CIOs want in 2022
* How no-code, reusable AI will bridge the AI divide
* What app developers need to do now to fight Log4j exploits
* How digital twins improve physical systems
* GitLab 14.6 shines on distributed deployments
* Hands-on with Dropwizard REST APIs
* Visual Studio feedback upgrade snubs older versions

C4ISRNET - Media for the Intelligence Age Military

* New in 2022: Marines are finally leveling up their drone game
* Army hopes to recover from IT modernization missteps
* New US Army cyber unit is building concepts for tactical cyber operations
* How are the US Army's tactical network upgrades coming along? We put the question to several military
* This company's drone set flight-time records. But what it really wants is more work with the Pentagon
* Space Force issues $32 million contract for prototype space-based sensor
* The US military wants to plug commercial satellites into its orbital networks
* Air Force Research Laboratory is one step closer to beaming solar energy from space to Earth
* US Army conducts first tactical cyber exercise readying teams for operations
* New hypersonic missile-tracking satellites pass critical design review

The Hacker Corner

Conferences

* Marketing Cybersecurity In 2021
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution
* This shouldn't have happened: A vulnerability postmortem

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.

* WASTC Winter ICT Educator's Conference
* #kksctf open / 5th anniversary edition
* BSides Algiers 2021 Finals
* KnightCTF 2022
* Real World CTF 4th
* Insomni'hack teaser 2022
* DiceCTF 2022
* STAY ~/ CTF 2022
* VU CYBERTHON 2022
* Codegate CTF 2022 Preliminary

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

* Wapiti Web Application Vulnerability Scanner 3.0.9
* TOR Virtual Network Tunneling Tool 0.4.6.9
* Google OSS Fuzz
* Log4j Recognizer
* OpenSSL Toolkit 1.1.1m
* Zed Attack Proxy 2.11.1 Cross Platform Package
* nfstream 6.4.0
* ETS5 Password Recovery Tool
* I2P 1.6.1
* Wapiti Web Application Vulnerability Scanner 3.0.8

Kali Linux Tutorials

* JVMXRay : Make Java Security Events Of Interest Visible For Analysis
* Hyenae Ng : An Advanced Cross-Platform Network Packet Generator And The Successor Of Hyenae
* Gotanda : Browser Web Extension For OSINT
* Fhex : A Full-Featured HexEditor
* Cumulus : Web Application Weakness Monitoring, It Would Be Working By Add Just 3 Codelines
* EXOCET : AV-evading, Undetectable, Payload Delivery Tool
* What is Crypto Margin Trading & How it Works?
* Clash : A Rule-Based Tunnel In Go
* ChopChop : ChopChop Is A CLI To Help Developers Scanning Endpoints And Identifying Exposition Of Sens
* Canadian Furious Beaver : A Tool For Monitoring IRP Handler In Windows Drivers, And Facilitating The

GBHackers Analysis

* Critical Security Flaws with Apache HTTP Server Let Hackers Execute Arbitrary Code Remotely
* Hackers Bypass Recently Patched MS Office Bug to Deliver Formbook Malware
* Tropic Trooper Hackers Group Targets Transportation & Government Companies
* Active Directory Domain Service Bug Let Attackers To Takeover Windows Domains
* Critical SSRF Bug in VMware Workspace ONE UEM Console Let Attacker Steal Sensitive Data

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS STAR Live Stream
* Join us for the FREE Virtual Cyber Threat Intelligence Summit 2022!
* Wrap Up Panel
* Open Threat Research - The Hunt for Red Apples: How to threat hunt and emulate Ocean Lotus on macOS

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelgänger Your Häx Dollars at Work
* DEF CON 29 Red Team Village - CTF Day 2
* DEF CON 29 Recon Village - Ben S - Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

Hak5

* Detect Vulnerable Log4J Websites with CanaryTokens | HakByte
* Inject Payloads with an Evil CircuitPython Keyboard
* The Biggest Hacks of 2021 - ThreatWire

The PC Security Channel [TPSC]

* Ransomware disables AV using Safe Mode: Avos Locker
* How to know if your PC is hacked? Digital Forensics 101

Eli the Computer Guy

* APPLE ABUSED FACTORY WORKERS in INDIA - indian women eating worms in deplorable conditions
* 20,000 FLIGHTS CANCELLED DUE TO COVID
* CDC SAYS VACCINATIONS ARE FAILING - CANCELS CRUISE SHIP INDUSTRY
* COVID CREATES PET FOOD SHORTAGE - starving dogs is not good for democrats

Security Now

* Best of 2021 - The Year's Best Stories on Security Now
* It's a Log4j Christmas - Another Chrome 0-Day, Cloud Clipboard Disabled, Wi-Fi/Bluetooth Leakage

Troy Hunt

* Weekly Update 276

Intel Techniques: The Privacy, Security, & OSINT Show

* 244-2021 Show Review & Updates
* 243-Emergency Bags

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For 2021
* Packet Storm New Exploits For December, 2021
* ManageEngine ServiceDesk Plus Remote Code Execution
* Terramaster F4-210 / F2-210 Remote Code Execution
* Backdoor.Win32.FTP.Simpel.12 Insecure Crypto Implementation
* Windows Explorer Preview Pane HTML File Link Spoofing
* Backdoor.Win32.FTP.Simpel.12 Man-In-The-Middle
* Backdoor.Win32.Visiotrol.10 Insecure Password Storage
* Microsoft Windows Explorer Preview Pane Security Bypass
* Accu-Time Systems MAXIMUS 1.0 Buffer Overflow / Denial Of Service
* Aver EVC300 Firmware 00.10.16.36 Hardcoded Secrets
* Exponent CMS 2.6 Cross Site Scripting / Brute Force
* phpKF CMS 3.00 Beta y6 Remote Code Execution
* WBCE CMS 1.5.1 Admin Password Reset
* WordPress Popular Posts 5.3.2 Remote Code Execution
* Bazaar Web PHP Social Listings Shell Upload
* Video Sharing Website 1.0 SQL Injection
* Signup PHP Portal 2.1 Shell Upload
* Alfa Team Shell Tesla 4.1 Remote Code Execution
* Android VM_MAYWRITE Access To Shared Zygote JIT Mapping
* Backdoor.Win32.Mellpon.b Information Disclosure
* Backdoor.Win32.BNLite Buffer Overflow
* Chrome NavigationPreloadRequest Site Isolation Bypass
* Chrome ThreadedIconLoader::DecodeAndResizeImageOnBackgroundThread Heap Use-After-Free
* Chrome blink::NativeIOFile::DoRead Heap Use-After-Free

CXSecurity

* ManageEngine ServiceDesk Plus Remote Code Execution
* Terramaster F4-210 / F2-210 Remote Code Execution
* Accu-Time Systems MAXIMUS 1.0 Buffer Overflow / Denial Of Service
* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG ABAP Code Injection
* SAP Netweaver IUUC_GENERATE_ACPLAN_DELIMITER ABAP Code Injection
* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG SQL Injection
* Apache Log4j2 2.14.1 Information Disclosure

Proof of Concept (PoC) & Exploits

Exploit Database

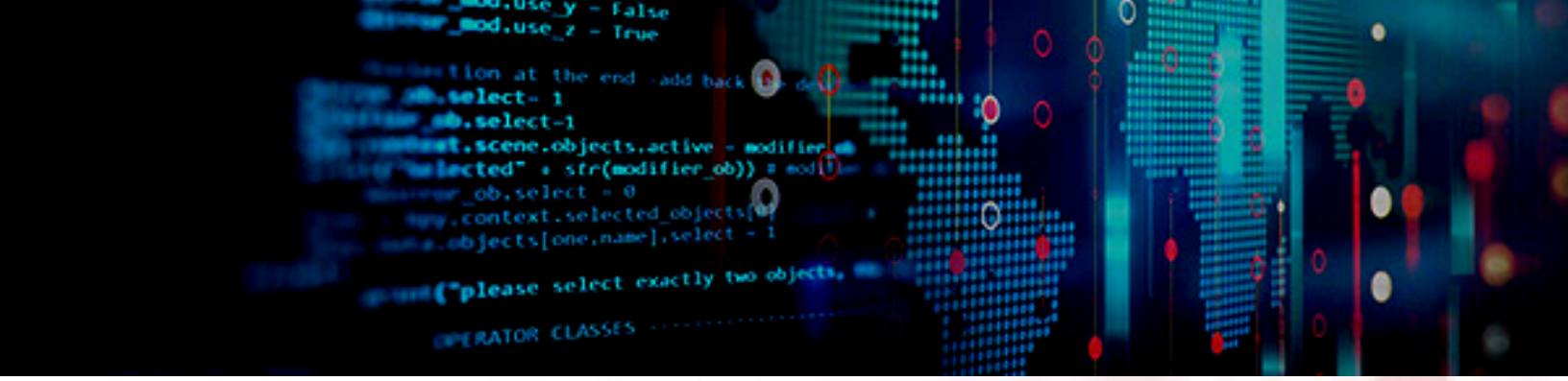
* [webapps] Exponent CMS 2.6 - Multiple Vulnerabilities
* [webapps] phpKF CMS 3.00 Beta y6 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] WBCE CMS 1.5.1 - Admin Password Reset
* [webapps] Arunna 1.0.0 - 'Multiple' Cross-Site Request Forgery (CSRF)
* [webapps] Croogo 3.0.2 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Croogo 3.0.2 - Unrestricted File Upload
* [webapps] Cibele Thinfinity VirtualUI 2.5.41.0 - User Enumeration
* [remote] Oliver Library Server v5 - Arbitrary File Download
* [local] Microsoft Internet Explorer / ActiveX Control - Security Bypass
* [webapps] Online Thesis Archiving System 1.0 - SQLi Authentication Bypass
* [webapps] meterN v1.2.3 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Zucchetti Axess CLOKI Access Control 1.64 - Cross Site Request Forgery (CSRF)
* [webapps] Booked Scheduler 2.7.5 - Remote Command Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin Typebot 1.4.3 - Stored Cross Site Scripting (XSS) (Authenticated)
* [remote] Apache Log4j 2 - Remote Code Execution (RCE)
* [local] Laravel Valet 2.0.3 - Local Privilege Escalation (macOS)
* [remote] Apache Log4j2 2.14.1 - Information Disclosure
* [webapps] WebHMI 4.0 - Remote Code Execution (RCE) (Authenticated)
* [remote] HD-Network Real-time Monitoring System 2.0 - Local File Inclusion (LFI)
* [webapps] Free School Management Software 1.0 - Remote Code Execution (RCE)
* [webapps] Free School Management Software 1.0 - 'multiple' Stored Cross-Site Scripting (XSS)
* [webapps] OpenCATS 0.9.4 - Remote Code Execution (RCE)
* [webapps] Employees Daily Task Management System 1.0 - 'multiple' Cross Site Scripting (XSS)
* [webapps] Employees Daily Task Management System 1.0 - 'username' SQLi Authentication Bypass
* [webapps] Grafana 8.3.0 - Directory Traversal and Arbitrary File Read

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

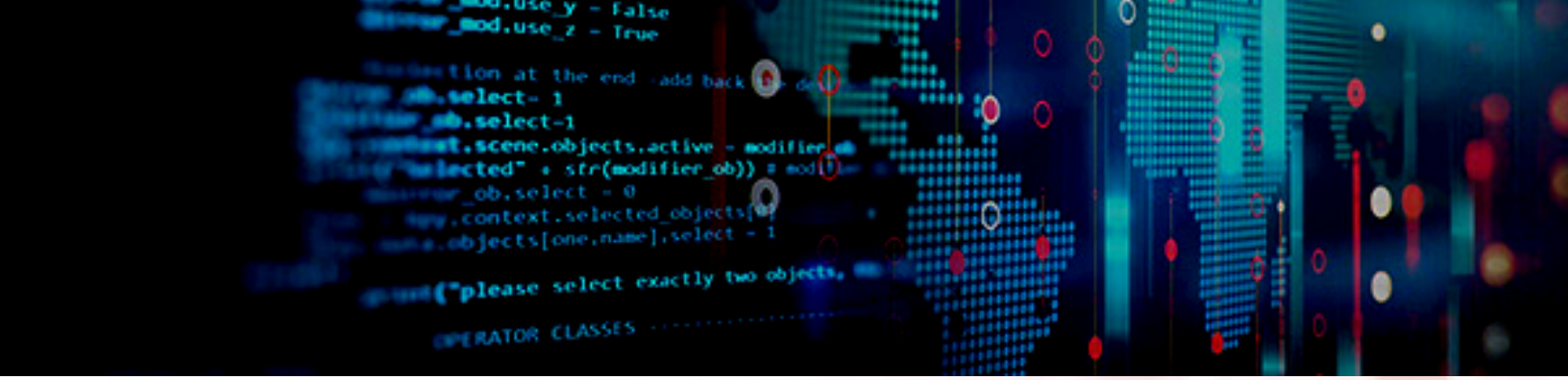
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://sikm.pn-lhokseumawe.go.id/id.txt
http://sikm.pn-lhokseumawe.go.id/id.txt notified by AnonCoders
http://sipak.pn-lhokseumawe.go.id/id.txt
http://sipak.pn-lhokseumawe.go.id/id.txt notified by AnonCoders
http://www.pn-boyolali.go.id/alone.txt
http://www.pn-boyolali.go.id/alone.txt notified by AnonCoders
https://drc.gov.eg
https://drc.gov.eg notified by boksha
https://www.banchop.go.th
https://www.banchop.go.th notified by Mr.Grim
https://escolasuperior.mppr.mp.br
https://escolasuperior.mppr.mp.br notified by Paraná Cyber Mafia
http://www.prevfogo.pr.gov.br
http://www.prevfogo.pr.gov.br notified by Paraná Cyber Mafia
https://patrimoniopublico.mppr.mp.br
https://patrimoniopublico.mppr.mp.br notified by Paraná Cyber Mafia
https://educacao.mppr.mp.br
https://educacao.mppr.mp.br notified by Paraná Cyber Mafia
https://gaeco.mppr.mp.br
https://gaeco.mppr.mp.br notified by Paraná Cyber Mafia
https://civel.mppr.mp.br
https://civel.mppr.mp.br notified by Paraná Cyber Mafia
https://criminal.mppr.mp.br
https://criminal.mppr.mp.br notified by Paraná Cyber Mafia
https://meioambiente.mppr.mp.br
https://meioambiente.mppr.mp.br notified by Paraná Cyber Mafia
https://transparencia.mppr.mp.br
https://transparencia.mppr.mp.br notified by Paraná Cyber Mafia
https://crianca.mppr.mp.br
https://crianca.mppr.mp.br notified by Paraná Cyber Mafia
https://idoso.mppr.mp.br
https://idoso.mppr.mp.br notified by Paraná Cyber Mafia
https://consumidor.mppr.mp.br
https://consumidor.mppr.mp.br notified by Paraná Cyber Mafia



Dark Web News

Darknet Live

ToRReZ Market Has Officially Retired

ToRReZ Market has officially shut down. They completed all transactions and disputes before closing their doors, according to an official announcement. The market announced their closure in early December, giving users time to finalize their orders and withdraw funds. From the lack of complaints, it appears as if the majority of users succeeded in pulling their funds prior to the market's shutdown. ToRReZ, it appears, has joined the list of graceful closures. In their original retirement announcement, the market administrators hinted at one day returning. Below is the message posted by Mr_blonde, the ToRReZ administrator, on Dread. Dear Users. Market will go down in 72-96h from now (Dec 30 - 14:30 UTC). Please remove all your funds immediately. We have completed all orders / disputes. If we made any mistake during it - we are truly sorry. Please leave feedback on your order ASAP. Thanks for being with us. mrblonde signed copy -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA512 Dear Users. Market will go down in 72-96h from now (Dec 30 - 14:30 UTC). Please remove all your funds immediately. We have completed all orders / disputes. If we made any mistake during it - we are truly sorry. Please leave feedback on your order ASAP. Thanks for being with us. mrblonde -----BEGIN PGP SIGNATURE-----
iQIzBAEBCgAdFiEE4DNkCTAjr9sqIxybuRj8IbVCmCgFAmHNwscACgkQuRj8IbVC
mCg7mg/9E3KFUys9v/VUvMMHReewrLiwiOzEtiBYm4rNShkPu78jOn6BcQFfIrJ9
PVzqw84QAldqMFZ/8gpmolCZgUU73s/JoIc80bwmv4mYfg4xYEUIXU8AqqpRZ52n
nQkqPDmbdb3CjfMLx8VualWWQUgHqunnRwAfFT7xjNOpgOmA2uxP+dtvETxCa5c+
PM8vFiu/RG+JpfAx36EAdcElx41ZedbrCTV2qeZ9DttH2ZKV+ogewVN15IVmQWHH
QOZpmzGVS3oOtCGEdwVqRsEx5ccj8d3yLcPsLKjNuSWudbfmRnf6QVvObC9akLV5
hI+XgBLHBJKLuh43tDRy6SYE1+MxNKHKtWVtIqx/awUvOnbs1mslHDJHmHAUciGk
z44TRNtKnCRpJ9P2pUkGbhzY1QiMHX0aBZNUfNbXhtJhzIA4gw5ucvXpzVebkoo/
BWxUS6LyH+EEISA0ot3n9hPHp5HKYMBUNTTgXNo19tzjMT51AAsFRonD7euE0Ue2
f6q1XN/BmdN7VA8AozO9TdBr5s3xnKWTycT7A6npKc3Xt2PXuITkGKypK+JWIy1Z
P7EGUxfIwRw1IlzKQreVb2R0gft3IXSnVPzL2v0y3wbM+POoDzcIwubYtOSibE2K
Df+fWuFR/FBuO2Zd92I8+VIYty4RFtsx+wJbDQWOvr/R1rhQkdw= =6Jem -----END PGP SIGNATURE-----
Retiring in such a way is a rarity. What is the market version of "honor among thieves”? Also, as for the rest of the darkweb: AK hit your dog and you can't bring ol yellow back

Hacker Factor on Snowflake Pluggable Transports

I missed this from earlier when Dr. Neal Krawetz posted his entry titled "Tor 0day: Snowflake.” I will include the relevant part about detecting snowflake below. The other parts of his article cover the other issues with Tor covered in his previous blog posts as well as Nusenu's discovery of an entity running hundreds of malicious Tor relays. I also included a bit about Snowflake for those who are unaware. What is Snowflake? Per the Tor Project: Snowflake is a pluggable transport that uses a combination of domain fronting and peer-to-peer WebRTC connections between clients and volunteers to circumvent Internet censorship. Snowflake, which is the spiritual successor to flashproxy, aims to lower the barrier for running anti-censorship

proxies, resulting in a large pool of proxies for users to connect to. Instead of requiring a server with consistent up-time, Snowflake proxies run as an addon or extension in your browser. These proxies can move locations as users connect to different networks, providing a moving target that is more difficult to block. We currently have about 8 thousand available Snowflake proxies each day. When a user connects to Snowflake in order to circumvent censorship, they are matched with a currently available proxy. If this proxy "melts,” or disappears, the user will be seamlessly matched with a new proxy. Snowflake proxies are run by volunteers. Complete documentation is available at Kerosene.net where much more information is available: Snowflake is a new circumvention tool which provides access to the free and open internet. As a Pluggable Transport, it provides easy-to-use access to a censorship circumvention system such as Tor. It is inspired by and builds upon the previous work of Flashproxy. Snowflake is much like a hybrid of previous Pluggable Transports, and this document will serve as a guide for exploring this system.

The website hosting snowflake is not the snowflake proxy. The visitors are the proxy. And yes this is the same diagram. To illustrate in the context of Tor, Snowflake allows anyone to leave a browser tab open to become an ephemeral Tor bridge. Much like the Flashproxy design, Snowflake involves a large network of highly ephemeral volunteer proxies, with the goal of outpacing the censor's ability to block proxy IP addresses and providing a very easy to use, reliable, and hard-to-filter method of circumventing censorship. Previously, users faced difficulties in manually configuring port-forwarding, which limited adoption of older tools like Flashproxy. Snowflake addresses NAT traversal by making it automatic and not the user's responsibility, among a number of new advantages. Snowflake Issues This is Hacker Factor Of all of the pluggable transports that the Tor Project has released, I think snowflake is the easiest to detect. I'm not saying that the others were difficult to detect and filter. Rather, the other protocols (fte, obfs3, obfs4, meek, etc.) only had a few ways that they could be detected. Snowflake has literally dozens of trivial ways to detect it. For example, video chats rely on a protocol called STUN (Session Traversal Utilities for NAT; network address translation). Basically, STUN identifies your external network address. This is needed to establish any kind of video chat when you use a firewall. Snowflake uses a hard-coded list of available STUN servers. The current list is: stun.voip.blackberry.com:3478 stun:stun.altar.com.pl:3478 stun:stun.antisip.com:3478 stun:stun.bluesip.net:3478 stun:stun.dus.net:3478 stun:stun.epygi.com:3478 stun:stun.sonetel.com:3478 stun:stun.sonetel.net:3478 stun:stun.stunprotocol.org:3478 stun:stun.uls.co.za:3478 stun:stun.voipgate.com:3478 stun:stun.voys.nl:3478 When the snowflake client first starts up, it queries DNS for a randomly selected subset of these STUN servers. It looks for the hostname resolution using both IPv4 and IPv6 (DNS 'A' and 'AAAA' records). However, it doesn't just look up the hostnames; it checks if the name is on the local network. Like most companies, my lab uses a private network behind the firewall and runs an internal DNS server. All computers on my private network use the domain name "internal.lan”. When I started snowflake, I immediately saw a set of DNS queries for the STUN servers: client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.epygi.com' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.voipgate.com' client -> dnsserver : DNS Query Type[1]=A Name='stun.epygi.com' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.sonetel.net' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.epygi.com.internal.lan' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.voipgate.com.internal.lan' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.epygi.com.internal.lan' client -> dnsserver : DNS Query Type[28]=AAAA Name='stun.voipgate.com.internal.lan' Each line is one packet, and all of this happened in one second. This means that I have multiple ways to detect a Tor snowflake client before it even tries to connect to the Tor snowflake server! A single WebRTC client typically connects to one STUN server. If you see a single client immediately lookup multiple STUN servers and all of the servers are in the snowflake hard-coded list, then you've found a Tor snowflake client. Regular WebRTC clients do not do hostname lookups for remote STUN servers on the local network. If you see any DNS lookups for snowflake's STUN servers on the local network (stun.epygi.com.internal.lan, stun.voipgate.com.internal.lan, etc.) then you've found a Tor snowflake client. About a second later - after doing the DNS lookups - there are queries for the snowflake hard-coded domain fronting server: client -> dnsserver : DNS Query Type[1]=A Name='cdn.sstatic.net' client -> dnsserver : DNS

Query Type[1]=AAAA Name='cdn.sstatic.net' Again, if you see any IP address that first does a DNS lookup for a snowflake STUN server and then does a lookup for the snowflake domain fronting service, then you've found a Tor snowflake client. These are just 3 ways for an administrator to watch DNS in order to detect or block Tor snowflake users before they can connect to the Tor network. There are another dozen ways to detect snowflake (zero false positives, zero false negatives) if you start looking at how it uses STUN and ICE. In addition, a snowflake client can be used to identify the IP addresses of other Tor users because other Tor users provide the snowflake proxies. (The entire snowflake protocol strikes me as a project created by a group that put no consideration into how an adversary might detect or block this pluggable transport.) I want to emphasize the warning from my earlier blog entries: If you are in a location where using Tor can result in an arrest, being tracked by government agents, or losing your job, then do not rely on snowflake for anonymity or to protect your privacy. The Tor Project provides zero solutions if you are located in a repressive location. i2p In response to a comment on one of his previous posts about Tor, Dr. Krawetz wrote this: I'm very familiar with i2p. I won't go near it unless someone is paying me for exploits. My short opinion: As many problems that Tor has, i2p is substantially worse. It is worse BECAUSE every user is also a relay. I can sit at watch the connection, allowing me to map out each user's address. If your server is up long enough, you should see everyone eventually. Then there are the i2p servers (like Tor's hidden services). It's basically a Russian ghost town with a very strong anti-muslim vibe. (Seriously - it was like every site was "Drugs! No Arabs!” but written in Russian.) And then there are the i2p exit nodes. Tor has a problem with hostile exit nodes. i2p has a problem because there are no exit nodes. (Well, there is ONE exit node, but it's either down or so heavily congested by everyone else that it's unusable.) So if you're using i2p, you're not accessing the Internet (no exits). You're likely only going to internal i2p sites that cater to illegal activity - making you a suspect just for being on i2p. And since every user is a relay, I can sit and collect the network addresses of every suspect user. Yeah, that's worse than Tor. All of the Hacker Factor posts about Tor make me concerned about the usefulness of Tor in the long term, even if the problems described in his posts are not ones that will immediately impact the users of drug markets (which, if I had to guess, make up the majority of my readership). As for i2p, I am not particularly concerned with the Russian ghost town part or the "anti-muslim vibe” part as neither of those impact the usefulness of i2p but it is irritating that there are so few eepsites that exist for purposes unrelated to drugs. Of course, being "a suspect just for being on i2p” is not evidence of crime in a court of law in many countries but it certainly could be an issue with ISPs and whatnot. Or make you a potential target for further scrutiny by LE. The full Hacker Factor post is available here.

NJ Town Auctioning a Maserati Seized from a Fraudster

A town in New Jersey is auctioning off a 2015 Maserati Quattroporte seized from a convicted fraudster. The fraudster bought a "significant amount of stolen personal identifying information via the dark web,” police said. The Maserati is surprisingly boring, honestly. As one user on Jalopnik commented, So, the answer to "why does this town have a fancy car to sell?” is: "Dumbass Thief couldn't live low and people started wondering how some weird unemployed guy living in his mom's basement could afford a Maserati. And why it was "gifted to him” from 4 people that were all filing complaints about identity thief.” Per DailyVoice.com: Working with others, [Ralph Taylor] bought a "significant amount of stolen personal identifying information via the dark web, including bank account information and online security question answers,” a complaint on file in federal court in Newark says. Taylor used the information to access victim accounts in New Jersey, New York, and elsewhere, the complaint says.[Taylor] and her cohorts went to the victims' banks and impersonated them to withdraw money, it says. They also called to request wire transfers. (The pronoun change in the above quote is apparently the result of a transition that took place while in police custody.)

The Maserati is a 3.0L V6 which seems underwhelming. I thought the modern Quattroporte's had TT V8s. As far as flexing criminal money goes, OxyGod had much better taste in my opinion. Wyatt Pasek poses with cash and a rental supercar Of course, he rented all the vehicles in his Instagram pictures.

Wyatt Pasek poses with cash and a rental yet again The Maserati is available on the municibid website.

LKA: Darkweb Accounts for 40% of Drug Deals in Vorarlberg

Darkweb drug transactions account for up to 40 percent of the drug deals in the Austrian state of Vorarlberg, according to an authority on the matter. The claim seems dubious to me though. Peter Gruber, head of the drug-related crime department at the State Office of Criminal Investigation, said that "all kinds of drugs” are available in Vortharlberg because the demand exists. "Due to the internet and the darknet, of course, we already have the problem that almost all drugs are found in Vorarlberg,” says Gruber. Wastewater at sewage treatment plants in Vorarlberg is the source of Gruber's claim about the types of drugs available in the region. Legal drugs, such as alcohol and nicotine, are consumed the most. Marijuana is the most frequently used illegal substance. Marijuana is followed by cocaine, amphetamines, and other stimulants. Gruber estimated that between 30 and 40 percent of drug deals in Vorarlberg are initiated on the darkweb. The rest, he explained, "take place in person on the street or at other meeting points. (This seems like the logical conclusion about the remainder of the transactions.) Gruber complained that a new drug dealer would enter the business as soon as the police jailed a different dealer. "Of course, whenever someone is arrested, the next one will gise up,” he said. I only covered this because the 30 to 40 percent claim seems unusually high. I thought, in most places, purchases on darkweb marketplaces accounted for a single-digit percent of drug trafficking activity.

Dark Web Link

White House Market Plans Retirement: What Important Things You Missed?

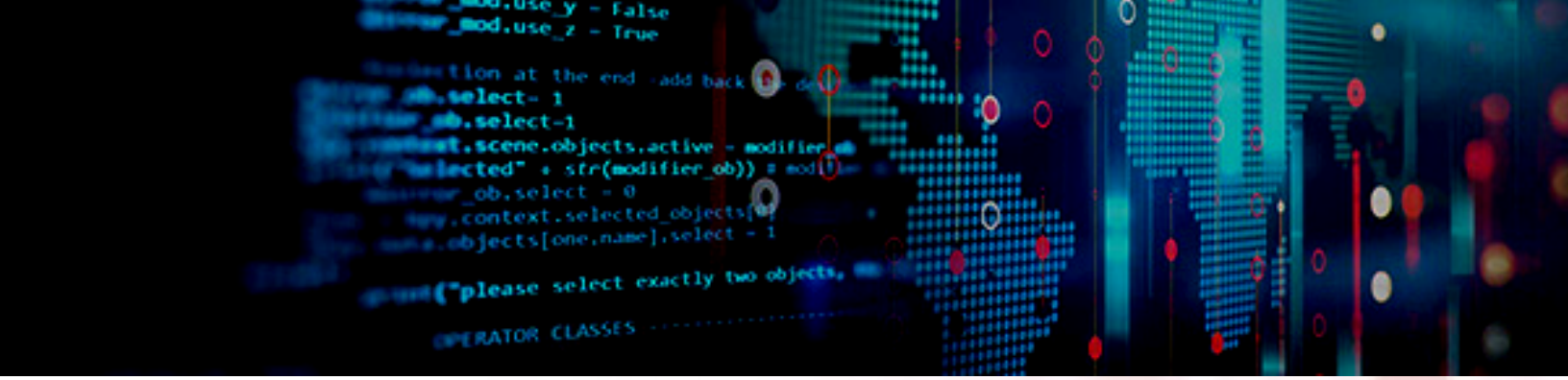
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere 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.

Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats

Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from “Dark web” persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that “you didn't take any shit from anyone.” During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug

Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

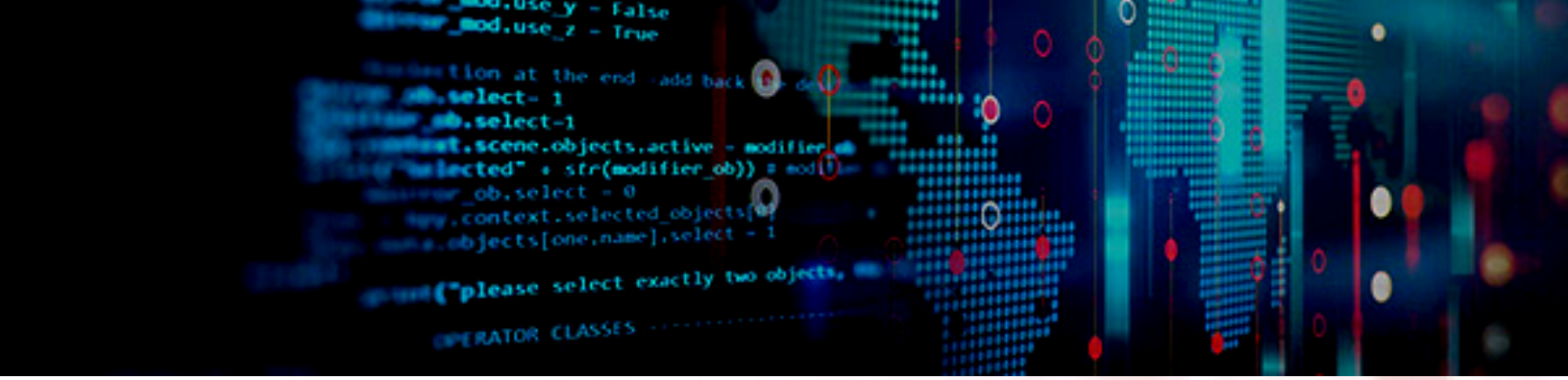
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management
* Discord CDN Abuse Found to Deliver 27 Unique Malware Types
* The Threat Landscape is Dynamic and Ever-Changing - Can You Keep Up?
* Mana Tools: A Malware C2 Panel with a Past

FireEye

* Sharing the Gifts of Cybersecurity - Or, a Lesson From My First Year Without Santa
* Test for Log4Shell With InsightAppSec Using New Functionality
* Metasploit Wrap-Up
* The Everyperson's Guide to Log4Shell (CVE-2021-44228)
* How to Protect Your Applications Against Log4Shell With tCell
* Patch Tuesday - December 2021
* Log4Shell Makes Its Appearance in Hacker Chatter: 4 Observations
* Using InsightVM to Find Apache Log4j CVE-2021-44228
* Update on Log4Shell's Impact on Rapid7 Solutions and Systems
* Hacky Holidays: Celebrating the Best of Security Nation [Video]



Advisories

US-Cert Alerts & bulletins

* Apache Releases Security Update for HTTP Server
* Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
* CISA Issues ED 22-02 Directing Federal Agencies to Mitigate Apache Log4j Vulnerabilities
* VMware Releases Security Advisory
* NSA and CISA Release Final Part IV of Guidance on Securing 5G Cloud Infrastructures
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Immediate Steps to Strengthen Critical Infrastructure against Potential Cyberattacks
* Adobe Releases Security Updates for Multiple Products
* AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
* AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus
* Vulnerability Summary for the Week of December 20, 2021
* Vulnerability Summary for the Week of December 13, 2021

Zero Day Initiative Advisories

ZDI-CAN-15469: Checkmk
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Esjay' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16087: Foxit
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16065: Microsoft
A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'JeongOh Kyea of THEORI' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16210: Tencent
A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16212: Tencent
A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-30, 4 days

ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16211: Tencent

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15812: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15525: KeySight

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15470: KeySight

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16062: X.Org

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jan-Niklas Sohn' was reported to the affected vendor on: 2021-12-30, 4 days ago. The vendor is given until 2022-04-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16157: Expat

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-24, 10 days ago. The vendor is given until 2022-04-23 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15747: Apple

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jeonghoon Shin at Theori' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15191: Apple

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jeremy Brown' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15588: Apple

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Wojciech Regu\xc5\x82a (@_r3ggi)' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16134: Parallels

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Reno Robert of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15915: Microsoft

A CVSS score 9.6 (AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Uncodable' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16137: Parallels

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15787: Parallels

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xavier Danest - Decathlon' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16026: Oracle

A CVSS score 6.5 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Ryota Shiga(@Ga_ryo_) of Flatt Security' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15980: FreeBSD

A CVSS score 8.3 (AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'm00nbsd' was reported to the affected vendor on: 2021-12-22, 12 days ago. The vendor is given until 2022-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16025: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-20, 14 days ago. The vendor is given until 2022-04-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16082: Apache

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-16, 18 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16119: Apache

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-16, 18 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16115: Foxit

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Ashfaq Ansari and Krishnakant Patil - HackSys Inc' was reported to the affected vendor on: 2021-12-16, 18 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-5238-02

Red Hat Security Advisory 2021-5238-02 - Kernel-based Virtual Machine offers a full virtualization solution for Linux on numerous hardware platforms. The virt:rhel module contains packages which provide user-space components used to run virtual machines using KVM. The packages also provide APIs for managing and interacting with the virtualized systems.

Red Hat Security Advisory 2021-5235-02

Red Hat Security Advisory 2021-5235-02 - PostgreSQL is an advanced object-relational database management system. Issues addressed include a man-in-the-middle vulnerability.

Red Hat Security Advisory 2021-5236-02

Red Hat Security Advisory 2021-5236-02 - PostgreSQL is an advanced object-relational database management system. Issues addressed include a man-in-the-middle vulnerability.

Red Hat Security Advisory 2021-5227-07

Red Hat Security Advisory 2021-5227-07 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Red Hat Security Advisory 2021-5226-02

Red Hat Security Advisory 2021-5226-02 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.

Red Hat Security Advisory 2021-5241-05

Red Hat Security Advisory 2021-5241-05 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements.

Ubuntu Security Notice USN-5186-2

Ubuntu Security Notice 5186-2 - USN-5186-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem. Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct spoofing attacks, bypass CSP restrictions, or execute arbitrary code. A security issue was discovered with the handling of WebExtension permissions. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to create and install a service worker that wouldn't be uninstalled with the extension. Various other issues were also addressed.

Red Hat Security Advisory 2021-5218-02

Red Hat Security Advisory 2021-5218-02 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This is an asynchronous patch for Red Hat Single Sign-On 7.5, and includes one security fix.

Red Hat Security Advisory 2021-5219-02

Red Hat Security Advisory 2021-5219-02 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This is an asynchronous patch for Red Hat Single Sign-On 7.5, and includes one security fix.

Red Hat Security Advisory 2021-5217-02

Red Hat Security Advisory 2021-5217-02 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This is an asynchronous patch for Red Hat Single Sign-On 7.5, and includes one security fix.

Red Hat Security Advisory 2021-5206-02

Red Hat Security Advisory 2021-5206-02 - Log4j is a tool to help the programmer output log statements to a variety of output targets. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5203-1

Ubuntu Security Notice 5203-1 - Hideki Okamoto and Guy Lederfein discovered that Apache Log4j 2 did not

protect against infinite recursion in lookup evaluation. A remote attacker could possibly use this issue to cause Apache Log4j 2 to crash, leading to a denial of service.

VMware Security Advisory 2021-0030

VMware Security Advisory 2021-0030 - VMware Workspace ONE Access, Identity Manager and vRealize Automation updates address multiple vulnerabilities.

VMware Security Advisory 2021-0028.4

VMware Security Advisory 2021-0028.4 - VMware has released a response to the Apache Log4j remote code execution vulnerability. They have updated this advisory.

Ubuntu Security Notice USN-5198-1

Ubuntu Security Notice 5198-1 - It was discovered that HTMLDOC improperly handled malformed URIs from an input html file. An attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5199-1

Ubuntu Security Notice 5199-1 - It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex with a quadratic worst-case time complexity. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. It was discovered that the Python urllib http client could enter into an infinite loop when incorrectly handling certain server responses. Specially crafted traffic from a malicious HTTP server could cause a denial of service condition for a client. Various other issues were also addressed.

Ubuntu Security Notice USN-5201-1

Ubuntu Security Notice 5201-1 - It was discovered that the Python urllib http client could enter into an infinite loop when incorrectly handling certain server responses. Specially crafted traffic from a malicious HTTP server could cause a denial of service condition for a client.

Ubuntu Security Notice USN-5200-1

Ubuntu Security Notice 5200-1 - It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex allowing for catastrophic backtracking. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex with a quadratic worst-case time complexity. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. Various other issues were also addressed.

Apple Security Advisory 2021-12-15-7

Apple Security Advisory 2021-12-15-7 - Safari 15.2 addresses buffer overflow, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-6

Apple Security Advisory 2021-12-15-6 - watchOS 8.3 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-5

Apple Security Advisory 2021-12-15-5 - tvOS 15.2 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-4

Apple Security Advisory 2021-12-15-4 - Security Update 2021-008 Catalina addresses buffer overflow, bypass, code execution, heap corruption, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-3

Apple Security Advisory 2021-12-15-3 - macOS Big Sur 11.6.2 addresses buffer overflow, bypass, code execution, heap corruption, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-2

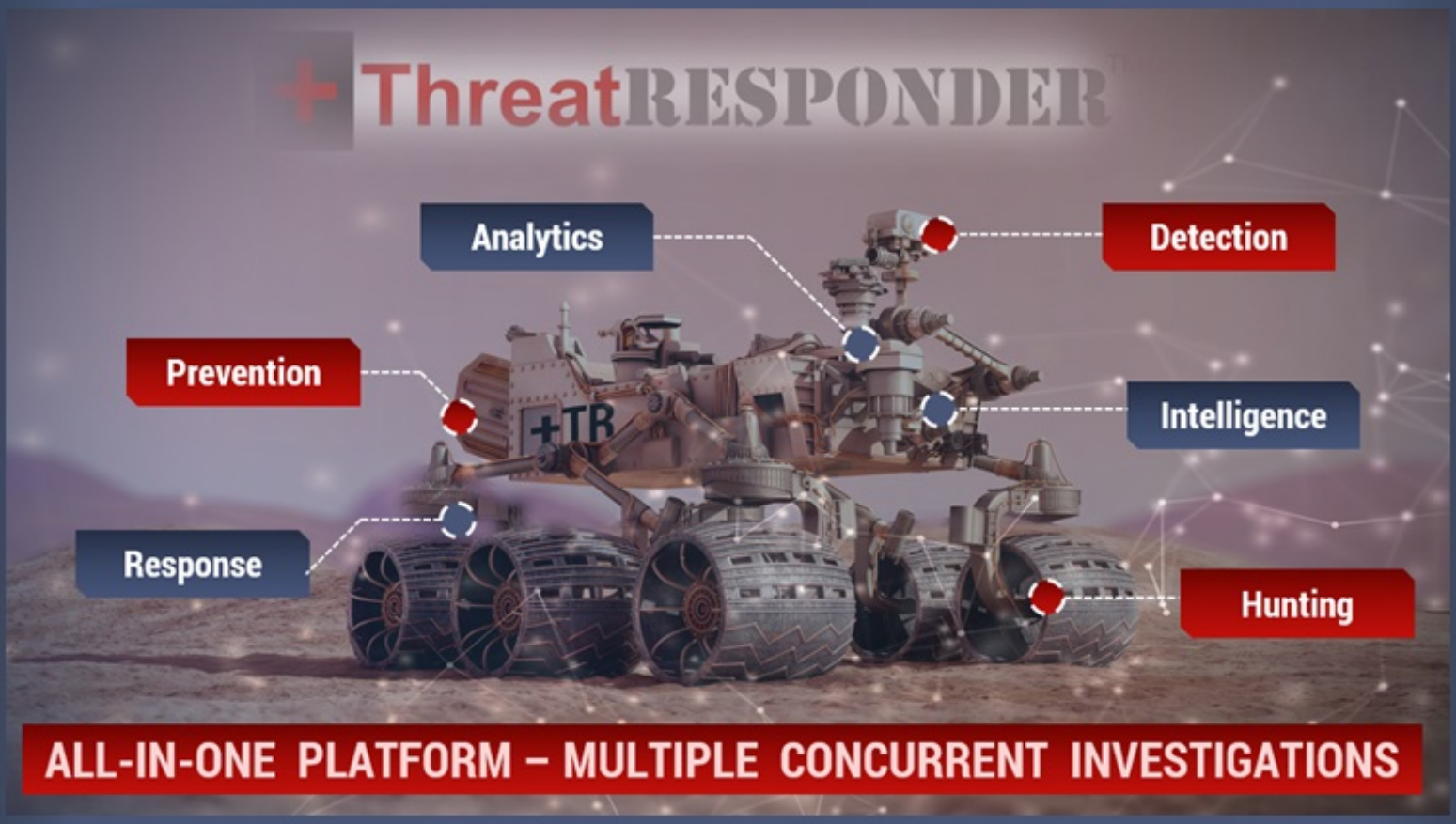
Apple Security Advisory 2021-12-15-2 - macOS Monterey 12.1 addresses buffer overflow, bypass, code execution, heap corruption, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

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



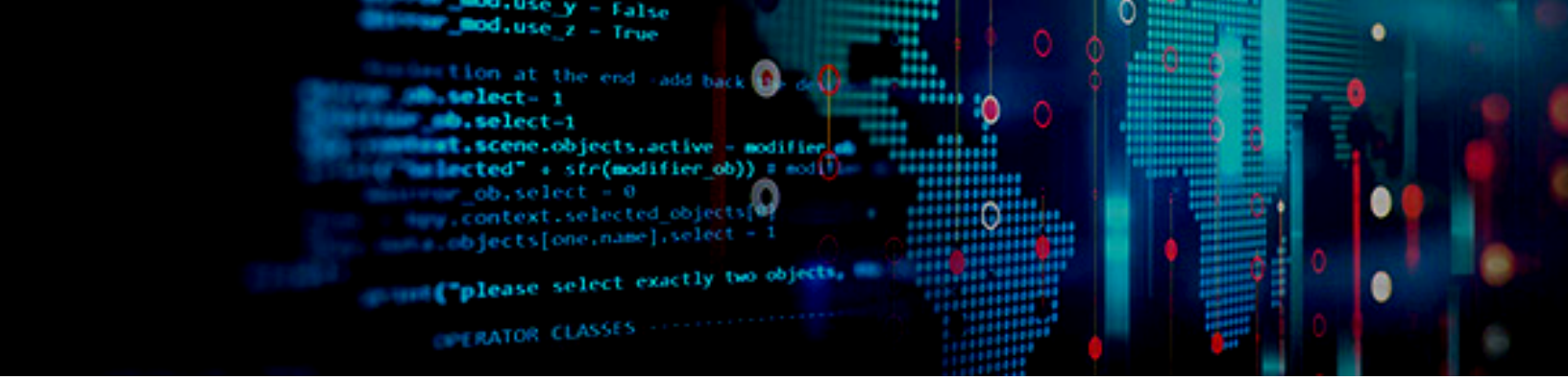
The Solution – ThreatResponder® Platform

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

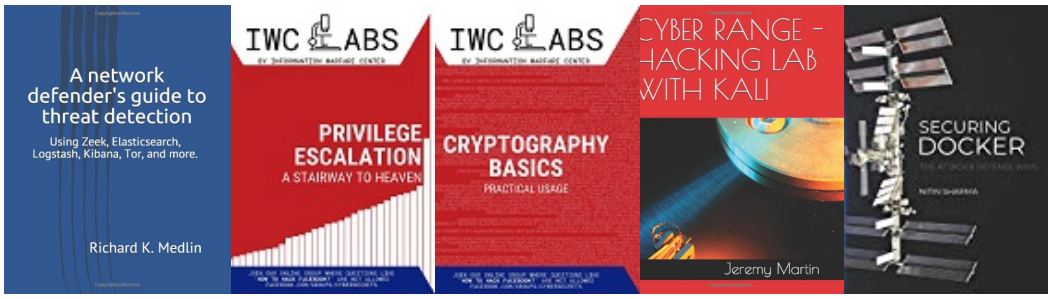


The Cyber Secrets publications on Amazon

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