Jan-10-22

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 10, 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

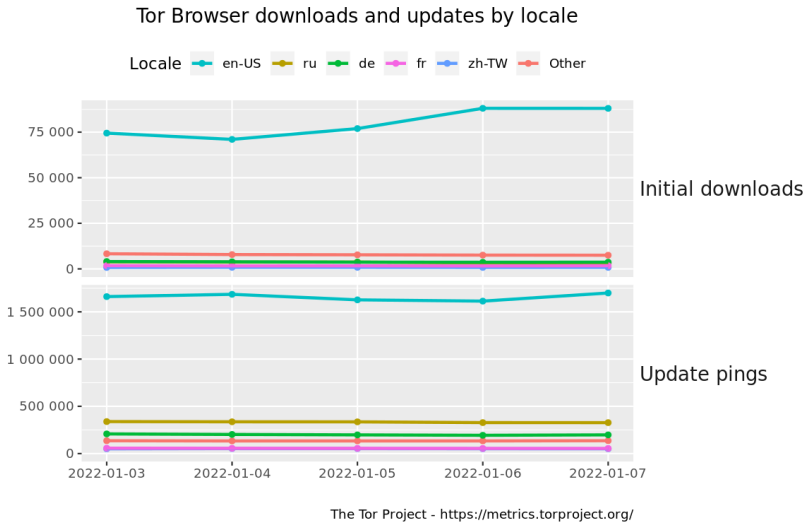
Internet Storm Center Infocon Status

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

* Google Project Zero 0-Days Exploited In-The-Wild
* QNAP: Get NAS Devices Off The Internet Now
* Log4J-Related RCE Flaw In H2 Database Earns Critical Rating
* Bitcoin Prices Fall To Lowest In Months After US Fed Remarks
* France Fines Google And Facebook â‚¬210m Over User Tracking
* Warning: Log4j Still Lurks Where Dependency Analysis Can't Find It
* Hacking Group Targets Old Java Applications To Break Into Networks
* VMware Bug Opens Door To Hypervisor Takeover
* iPhone Malware Tactic Causes Fake Shutdowns To Enable Spying
* Report: $2.2 Billion In Cryptocurrency Stolen From DeFi Platforms In 2021
* Activision Sues And Unmasks Alleged Call Of Duty: Warzone Cheat Sellers
* Malsmoke Exploits Microsoft's E-Signature Validation
* This iOS 15 Bug Could Crash Your iPhone Permanently
* Kosovo Bans Cryptocurrency Mining After Blackouts
* Purple Fox Rootkit Dropped By Malicious Telegram Installers
* John Edwards Takes The Reins At The UK's Data Protection Watchdog
* Microsoft Fixes Y2K22 Exchange Bug That Crashed Servers Worldwide
* Log4j Flaw Attack Levels Remain High, Microsoft Warns
* Silicon Valley's Trial Of The Century
* January 6 Committee Gets Inside Trump's West Wing Wall Of Obstruction
* The Biggest Data Breaches, Hacks Of 2021
* Portugal's Impresa Media Outlets Hit By Hackers
* Broward Health Warns 1.3 Million Patients, Staff Of Medical Identity Theft After Data Breach
* Chinese Espionage Group Leveraged Log4j Bug In VMware
* Polish Prosecutors Decline To Investigate Phone Hacking Allegation

Krebs on Security

* 500M Avira Antivirus Users Introduced to Cryptomining
* Norton 360 Now Comes With a Cryptominer
* 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

Dark Reading

* The Evolution of Patch Management: How and When It Got So Complicated
* NHS Warns of Attackers Targeting Log4j Flaws in VMware Horizon
* MSP Thrive Acquires InCare Technologies
* Cerberus Sentinel Acquires True Digital Security
* IT/OT Convergence Is More Than a Catchy Phrase
* How to Proactively Limit Damage From BlackMatter Ransomware
* 7 Predictions for Global Energy Cybersecurity in 2022
* Enterprises Worry About Increased Data Risk in Cloud
* Google Docs Comments Weaponized in New Phishing Campaign
* New Mexico's Bernalillo County Investigates Ransomware Attack
* Convergence Zone: CNAPP Aids in Integrated Cloud-Native Security
* CDN Cache Poisoning Allows DoS Attacks Against Cloud Apps
* Rethinking Cybersecurity Jobs as a Vocation Instead of a Profession
* New Mac Malware Samples Underscore Growing Threat
* Hybrid Multicloud Strategies Are Keeping the Public Sector at the Forefront of Threat Mitigation
* New Attack Campaign Exploits Microsoft Signature Verification
* NY AG: 1.1M Online Consumer Accounts Found Compromised in Credential-Stuffing Attacks
* FTC: Companies Could Face Legal Action for Failing to Patch Log4j
* Which Cloud Strategy Is Right For My Organization's Security Needs?
* Why We Need To Reframe the False-Positive Problem

The Hacker News

* Researchers Find Bugs in Over A Dozen Widely Used URL Parser Libraries
* Abcbot Botnet Linked to Operators of Xanthe Cryptomining malware
* BADNEWS! Patchwork APT Hackers Score Own Goal in Recent Malware Attacks
* Facebook Launches 'Privacy Center' to Educate Users on Data Collection and Privacy Options
* NHS Warns of Hackers Targeting Log4j Flaws in VMware Horizon
* Log4Shell-like Critical RCE Flaw Discovered in H2 Database Console
* France Fines Google, Facebook â‚¬210 Million Over Privacy Violating Tracking Cookies
* North Korean Hackers Start New Year with Attacks on Russian Foreign Ministry
* NIST Cybersecurity Framework: A Quick Guide for SaaS Security Compliance
* New Trick Could Let Malware Fake iPhone Shutdown to Spy on Users Secretly
* VMware Patches Important Bug Affecting ESXi, Workstation and Fusion Products
* Google Releases New Chrome Update to Patch Dozens of New Browser Vulnerabilities
* Researchers Uncover Hacker Group Behind Organized Financial-Theft Operation
* New Zloader Banking Malware Campaign Exploiting Microsoft Signature Verification
* Hackers Target Real Estate Websites with Skimmer in Latest Supply Chain Attack

Security Week

* U.S. Government Issues Warning Over Commercial Surveillance Tools
* Abcbot DDoS Botnet Linked to Older Cryptojacking Campaign
* SecurityWeek Cyber Insights 2022: Ransomware
* SonicWall Patches Y2K22 Bug in Email Security, Firewall Products
* WordPress 5.8.3 Patches Several Injection Vulnerabilities
* Indian Cyberspies Expose Their Operation After Infecting Themselves With RAT
* QNAP Urges Users to Secure NAS Devices as Attacks Surge
* Attackers Hitting VMWare Horizon Servers With Log4j Exploits
* Eight New macOS Malware Families Emerged in 2021
* Log4Shell-Like Vulnerability Found in Popular H2 Database
* Cyber Ninjas Faces Fine Over Arizona Election Review Records
* California Man Pleads Guilty Over Role in $50 Million Fraud Scheme
* Online Pharmacy Service Ravkoo Discloses Data Breach
* Polish Leader Admits Country Bought Powerful Israeli Spyware
* Thousands of School Websites Go Offline Due to Ransomware Attack on Finalsite
* Swiss Army Knifes WhatsApp at Work
* Rights Group Verifies Polish Senator Was Hacked With Spyware
* Biometric Face Authentication Firm iProov Takes $70M Investment
* Fresh Warnings Issued Over Abuse of Google Services
* Microsoft Announces Zero-Touch Onboarding for 'Defender for Endpoint' on iOS
* Senators Ask DHS, DOT About Transportation Infrastructure Cybersecurity
* The Second Building Block for the SOC of the Future: An Open Integration Framework
* NY AG: Credential Stuffing Impacts 1.1 Million Users at 17 Companies
* Hackers Hit Major Portuguese Media Group, Take Down Websites
* Chemicals Company Element Solutions Discloses Cybersecurity Incident

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Ransomware Attacks Could Result in Higher Cybersecurity Stocks
* Your KnowBe4 Fresh Content Updates from December 2021
* Hive Ransomware-as-a-Service Races to the Top as Affiliates Breach 350 Organizations in Just 4 Months
* Over 1200 Man-in-the-Middle Phishing Toolkits Designed to Intercept 2FA Found in the Wild
* 121 Brands Impersonated in Massive 91-Country Survey-Turned-Fraud Scam
* Obvious, but Probably Effective: Konni RAT Screensaver
* New York State Warns of Credential Stuffing
* CyberheistNews Vol 12 #01 [Heads Up] New Omicron-Themed Phishing Attack is Now Running Rampant
* Cryptocurrency Scam Profits Jump 81% in 2021 to $7.7 Billion
* Reducing Stress with CBD Is the Latest Theming for Phishing Attacks

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

* FBI warns of hackers mailing malicious USB drives to spread ransomware
* Norton antivirus installs cryptominer on devices but there is a way out
* Cloud video platform abused in web skimmer attack against real estate sites
* 9-year-old Windows flaw abused to drop ZLoader malware in 111 countries
* 4 things that you didn't know your smartphone could do
* 5 Things to Consider When Getting into Cryptocurrency
* How Data Analytics and AI Solve the Toughest Global Problems

Koddos

* FBI warns of hackers mailing malicious USB drives to spread ransomware
* Norton antivirus installs cryptominer on devices but there is a way out
* Cloud video platform abused in web skimmer attack against real estate sites
* 9-year-old Windows flaw abused to drop ZLoader malware in 111 countries
* 4 things that you didn't know your smartphone could do
* 5 Things to Consider When Getting into Cryptocurrency
* How Data Analytics and AI Solve the Toughest Global Problems

Naked Security

* Honda cars in flashback to 2002 - "Can't Get You Out Of My Head"
* Log4Shell-like security hole found in popular Java SQL database engine H2
* S3 Ep64: Log4Shell again, scammers keeping busy, and Apple Home bug [Podcast + Transcript]
* FTC threatens "legal action" over unpatched Log4j and other vulns
* Apple Home software bug could lock you out of your iPhone
* 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!

Threat Post

* EoL Systems Stonewalling Log4j Fixes for Fed Agencies
* Cyberattackers Hit Data of 80K Fertility Patients
* 3.7M FlexBooker Records Dumped on Hacker Forum
* QNAP: Get NAS Devices Off the Internet Now
* Log4J-Related RCE Flaw in H2 Database Earns Critical Rating
* Activision Files Unusual Lawsuit over Call of Duty Cheat Codes
* Google Voice Authentication Scam Leaves Victims on the Hook
* Partially Unpatched VMware Bug Opens Door to Hypervisor Takeover
* Apple iPhone Malware Tactic Causes Fake Shutdowns to Enable Spying
* Attackers Exploit Flaw in Google Docs' Comments Feature

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

* Omnichannel E-commerce Growth Increases API Security Risk
* 5 Things New with Bug Bounty Programs
* The Most Important Security Takeaway from the October Facebook Outage
* Cyber Awareness 2022: Consider Deepfakes, NFTs and More
* The 5 Most Hotly Contested Security Trends and Questions
* Protecting Your Data From a Unique Threat: Misinformation
* Data Protection: What Needs to Be Protected?
* Everything You Need To Know About Ransomware Attacks and Gangs In 2022
* Intelligent Adversary Engagement: Deceiving the Attacker
* Changing the Conversation with Risk Quantification

InfoWorld

* Multicloud and your career
* 5 questions to consider about agile capacity planning
* 16 irresistible cloud innovations
* The cloud comes down to earth
* AngularJS reaches end of life
* What is streaming data? Event stream processing explained
* The real value of 5G and cloud computing
* Visual Studio 2022 update offers Git improvements
* A simple automated build pipeline for Node.js
* Demystifying the Program and Startup classes in ASP.NET Core

C4ISRNET - Media for the Intelligence Age Military

* Northrop looks to adapt electronic attack system for smaller ships
* What will the US Space Force be able to do with its new GPS III variant?
* New in 2022: A changing outlook for air warfare in US Central Command
* Naval Surface Warfare Center invests in additive manufacturing prototypes
* Eying military gains, France goes big on national quantum technology
* Security forces airmen step up anti-drone training after recent attacks in Iraq, Syria
* DoD well on its way to creating data centric future, says chief data officer
* Kristin Robertson to lead Raytheon's space efforts
* Why the US should fight Russia, China in the 'gray zone'
* New in 2022: Marines are finally leveling up their drone game

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.

* 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
* Basic CTF 2022 QUALS
* Insomni'hack 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

* Haveged 1.9.16
* SQLMAP - Automatic SQL Injection Tool 1.6
* Wireshark Analyzer 3.6.1
* 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

Kali Linux Tutorials

* Kube-Applier : Enables Automated Deployment And Declarative Configuration For Your Kubernetes Cluster
* Covery: Online Fraud Detection Software
* 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

GBHackers Analysis

* Elephant Beetle Hacking Group Attack Organizations To Steal Financial Data
* Chinese Hackers Using Log4Shell Exploit Tools to Perform Post-Exploitation Attacks
* 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

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Applying DS/ML to Forensics and Incident Response: An Interview with Jess Garcia
* Inside FOR608: Enterprise-Class Incident Response & Threat Hunting - Course Preview
* SANS Threat Analysis Rundown
* SANS STAR Live Stream

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

* Deploy 5 Duckyscript Payloads with CircuitPython | HakByte
* Detect Vulnerable Log4J Websites with CanaryTokens | HakByte
* Inject Payloads with an Evil CircuitPython Keyboard

The PC Security Channel [TPSC]

* Best Browser Security: Edge vs Firefox vs Chrome
* Ransomware disables AV using Safe Mode: Avos Locker

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

* December 33rd - Log4j Update, RSA Postponed, Hack the DHS Expanded, Cyber Insurance Cost Rising
* Best of 2021 - The Year's Best Stories on Security Now

Troy Hunt

* Weekly Update 277

Intel Techniques: The Privacy, Security, & OSINT Show

* 245-OSINT 9 & Privacy Updates
* 244-2021 Show Review & Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Microsoft Windows SMB Direct Session Takeover
* Chrome storage::BlobURLStoreImpl::Revoke Heap Use-After-Free
* Online Veterinary Appointment System 1.0 SQL Injection
* Backdoor.Win32.SVC Directory Traversal
* Backdoor.Win32.SubSeven.c Buffer Overflow
* Backdoor.Win32.Dsklite.a Insecure Transit
* XNU inm_merge Heap Use-After-Free
* Backdoor.Win32.SVC Buffer Overflow
* Backdoor.Win32.Jtram.a Man-In-The-Middle
* Simple Music Cloud Community System 1.0 SQL Injection
* Backdoor.Win32.Dsklite.a Denial Of Service
* Backdoor.Win32.Jtram.a Insecure Credential Storage
* WordPress Catch Themes Demo Import Shell Upload
* Dixell XWEB 500 Arbitrary File Write
* Gerapy 0.9.7 Remote Code Execution
* Affiliate Pro 1.7 Cross Site Scripting
* Hostel Management System 2.1 Cross Site Scripting
* TermTalk Server 3.24.0.2 Arbitrary File Read
* Rocket LMS 1.1 Cross Site Scripting
* openSIS Student Information System 8.0 SQL Injection
* Online Admission System 1.0 Remote Code Execution
* Hospitals Patient Records Management System 1.0 Account TakeOver
* WordPress AAWP 3.16 Cross Site Scripting
* uDoctorAppointment 2.1.1 Cross Site Scripting
* Automox Agent 32 Local Privilege Escalation

CXSecurity

* Automox Agent 32 Local Privilege Escalation
* Siemens S7 Layer 2 Denial of Service (DoS)
* AWebServer GhostBuilding 18 Denial Of Service
* Gerapy 0.9.7 Remote Code Execution
* Vodafone H-500-s 3.5.10 WiFi Password Disclosure
* WordPress Catch Themes Demo Import Shell Upload
* ManageEngine ServiceDesk Plus Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

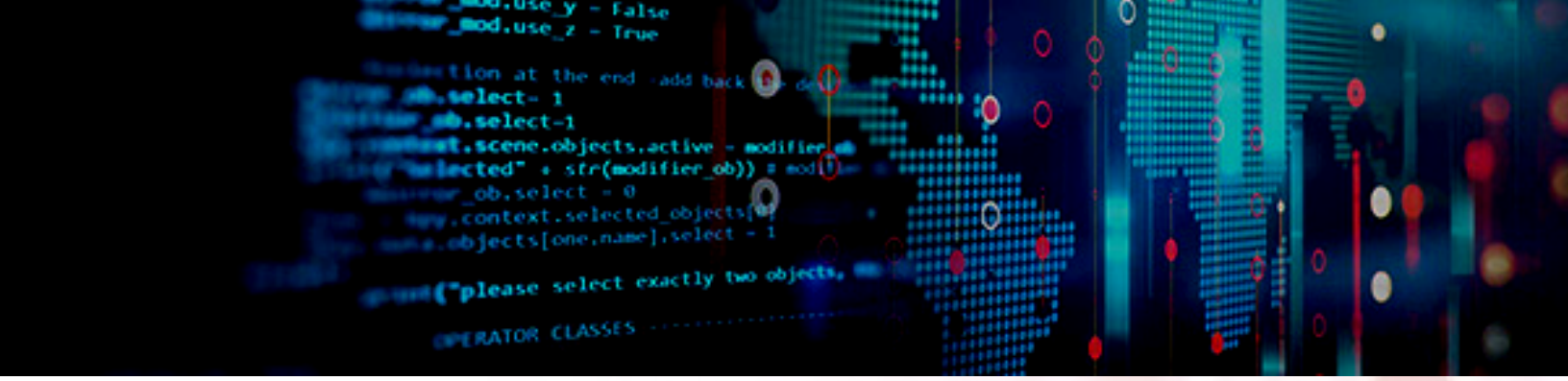
* [remote] CoreFTP Server build 725 - Directory Traversal (Authenticated)
* [webapps] Open-AudIT Community 4.2.0 - Cross-Site Scripting (XSS) (Authenticated)
* [local] VUPlayer 2.49 - '.wax' Local Buffer Overflow (DEP Bypass)
* [webapps] Online Railway Reservation System 1.0 - 'Multiple' Stored Cross Site Scripting (XSS) (Unaut
* [webapps] Online Railway Reservation System 1.0 - Admin Account Creation (Unauthenticated)
* [webapps] Online Railway Reservation System 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Online Railway Reservation System 1.0 - 'id' SQL Injection (Unauthenticated)
* [webapps] HTTP Commander 3.1.9 - Stored Cross Site Scripting (XSS)
* [webapps] Online Veterinary Appointment System 1.0 - 'Multiple' SQL Injection
* [webapps] WordPress Plugin AAWP 3.16 - 'tab' Reflected Cross Site Scripting (XSS) (Authenticated)
* [local] Automox Agent 32 - Local Privilege Escalation
* [webapps] Projeqtor v9.3.1 - Stored Cross Site Scripting (XSS)
* [remote] Gerapy 0.9.7 - Remote Code Execution (RCE) (Authenticated)
* [remote] Dixell XWEB 500 - Arbitrary File Write
* [remote] TermTalk Server 3.24.0.2 - Arbitrary File Read (Unauthenticated)
* [webapps] openSIS Student Information System 8.0 - 'multiple' SQL Injection
* [webapps] Vodafone H-500-s 3.5.10 - WiFi Password Disclosure
* [webapps] Terramaster TOS 4.2.15 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Virtual Airlines Manager 2.6.2 - 'multiple' SQL Injection
* [local] TRIGONE Remote System Monitor 3.61 - Unquoted Service Path
* [webapps] BeyondTrust Remote Support 6.0 - Reflected Cross-Site Scripting (XSS) (Unauthenticated)
* [webapps] Hospitals Patient Records Management System 1.0 - Account TakeOver
* [webapps] Hospitals Patient Records Management System 1.0 - 'id' SQL Injection (Authenticated)
* [remote] AWebServer GhostBuilding 18 - Denial of Service (DoS)
* [webapps] Hostel Management System 2.1 - Cross Site Scripting (XSS)

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

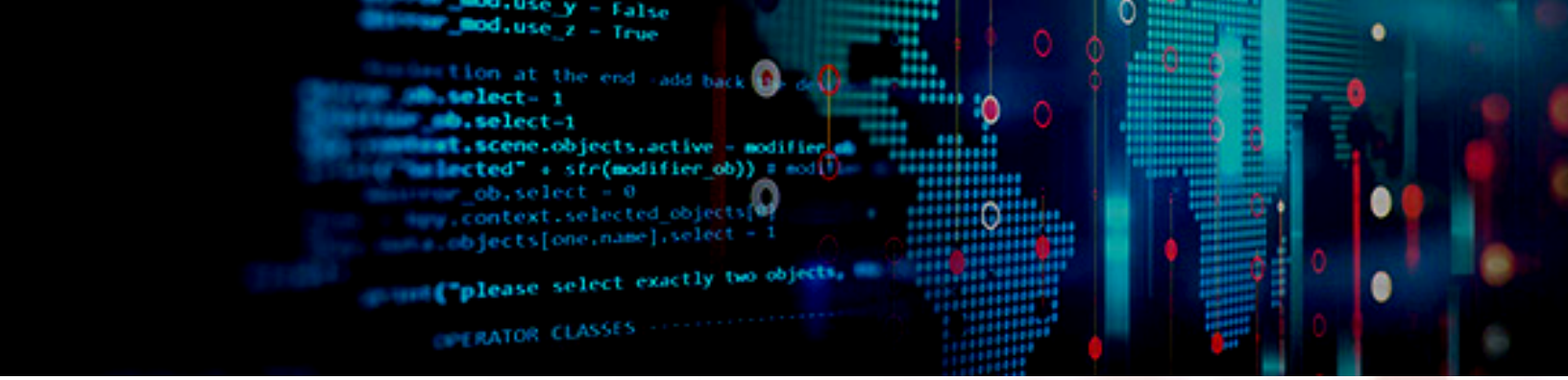
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.ntiprit.gov.in/Mwd.html
https://www.ntiprit.gov.in/Mwd.html notified by Mr.kEsrA
http://sahl.gov.sd/shin.htm
http://sahl.gov.sd/shin.htm notified by ByME
http://drdipregional.igad.int/007.html
http://drdipregional.igad.int/007.html notified by 0x1998
https://luglis.gov.ua/b4.html
https://luglis.gov.ua/b4.html notified by 0x1998
http://www.judiciary.gov.mv/b4.html
http://www.judiciary.gov.mv/b4.html notified by 0x1998
https://www.deped.gov.ph/b4.html
https://www.deped.gov.ph/b4.html notified by 0x1998
http://olevsk-gromada.gov.ua/kurd.html
http://olevsk-gromada.gov.ua/kurd.html notified by 0x1998
http://www.pge.ba.gov.br/b4.html
http://www.pge.ba.gov.br/b4.html notified by 0x1998
http://nilopolis.rj.gov.br/b4.html
http://nilopolis.rj.gov.br/b4.html notified by 0x1998
https://santaritadoitueto.mg.gov.br/b4.html
https://santaritadoitueto.mg.gov.br/b4.html notified by 0x1998
http://schmelzer-musikschule-scheibbs.gv.at/indonesia.html
http://schmelzer-musikschule-scheibbs.gv.at/indonesia.html notified by /Rayzky_
https://www.samburu.go.ke/robots.txt
https://www.samburu.go.ke/robots.txt notified by YOSF DOSKY
http://mobgis.youth.gov.eg
http://mobgis.youth.gov.eg notified by Moroccan Islamic Union-Mail
http://www.lottosport.com.tw/news_detail.php?code=tv5b24tkfkyhwg58rd47
http://www.lottosport.com.tw/news_detail.php?code=tv5b24tkfkyhwg58rd47 notified by Moroccan Islamic Union-Mail
http://www.sudarecboard.gov.sd
http://www.sudarecboard.gov.sd notified by Moroccan Islamic Union-Mail
http://www.vans.co.nz
http://www.vans.co.nz notified by Moroccan Islamic Union-Mail
http://www.mot.gov.kh
http://www.mot.gov.kh notified by Moroccan Islamic Union-Mail



Dark Web News

Darknet Live

2022: Companies to Report Payments of $600 or More

Payment services such as CashApp, Venmo, and Zelle are now required to report transactions totaling $600 or more to the Internal Revenue Service. As of January 1, 2022, payment services like Cash App, Venmo, and Zelle, among others, are required to report transactions that total $600 or more in one year to the Internal Revenue Service. Forbes tells us how reasonable this is: The IRS is cracking down on payments received through apps, such as Cash App, Zelle, or Paypal to ensure those using the third-party payment networks are paying their fair share of taxes. It seems like common sense that the people failing to pay their "fair share of taxes” are the people earning $601 through Cash App. Previously, the IRS required third-party payment networks to report transactions when the gross payments exceeded $20,000 and had more than 200 transactions per year. Related: Yellen Defends Proposed Bank Reporting Requirements The requirement is not limited to Cash App, Zelle, or Venmo; all payment networks, including bank accounts, have the same reporting requirements. __ Form 1099-K PayPal, the owner of Venmo, published a document with answers to potential questions from their customers. The company broke down the changes as follows: 1099-K Threshold Change: This new Threshold Change is currently only for payments received for goods and services transactions, so this doesn't include things like paying your family or friends back using PayPal or Venmo for dinner, gifts, shared trips, etc. This change was introduced in the American Rescue Plan Act of 2021, which amended some sections of the Internal Revenue Code to require Third-Party Settlement Organizations (TPSOs), like PayPal and Venmo, to report goods and services transactions made by customers with $600 or more in annual gross sales on 1099-K forms. Currently, a 1099-K is only required when a user receives more than $20,000 in goods and services transactions and more than 200 goods and services transactions in a calendar year. In-flow and Out-flow Reporting Changes The In-flow and Out-flow Reporting Changes are currently only a legislative proposal, which could potentially be considered by Congress this year. The proposed change would ultimately require all banks and payment service providers, including PayPal and Venmo, to report total inflows and outflows for accounts with at least $10,000 of total deposits and/or withdrawals to the IRS. This is intended to increase the visibility the IRS has into money coming in and out of customer accounts. At this stage, unlike the 1099-K Threshold Change, this is just a proposal and the details are still up for debate. As the situation changes, we'll be sure to keep this updated as we learn more. If a user transacted more than $600 in one year, the financial service is supposed to send them a Form 1099-K which PayPal described as "an IRS informational tax form used to report payments received by a business or individual for the sale of goods and services that were paid via a third-party network.” There presumably will not be any changes to the lives of US citizens who file accurate tax information with the IRS. However, considering the apparent need to add almost 90,000 IRS employees, it seems as if the government is anticipating something… __ Ah, at least the IRS workforce would grow at a fiscally responsible rate! PayPal warned: For the 2022 tax year, you should consider the amounts shown on your Form 1099-K when calculating gross receipts for your income tax return. The IRS will be able to cross-reference both our report and yours. Should have used Monero?

Second Chemical Revolution Trial Starts on January 10

The second trial for the defendants behind the "Chemical Revolution” darkweb shop starts on January 10, according to an announcement made on Tuesday. The District Court of Giessen announced the schedule for the second trial of the men who sold drugs through the Chemical Revolution storefront on the darkweb. The Frankfurt Public Prosecutor's Office accuses the group of five defendants of operating the storefront between April 2018 and February 2019. In August 2021, the court sentenced seven defendants to prison for crimes committed between late summer 2017 and January 2018. One of the defendants sentenced to prison in 2021 will be back in court for the upcoming trial. Chemical Revolution had vendor shops on the darkweb and the surface web. In total, Chemical Revolution sold and shipped more than 130 kilograms of amphetamine, 42 kilograms of cannabis, 17 kilograms MDMA, 6 kilograms of cocaine, one kilogram of heroin, as well as an unknown number of LSD blotters. From an earlier article about Chemical Revolution: German authorities charged 11 people in connection with the operation of the Chemical Revolution drug shop. According to the Frankfurt Public Prosecutor, Chemical Revolution sold hundreds of kilograms of drugs and earned a profit of more than one million euros. Some of the defendants also face charges for selling drugs through the Wallstreet Market darkweb marketplace. The "Chemical Revolution” shop was shut down as a result of a joint operation by the German Federal Criminal Police Office and the French criminal police. A 2018 drug trafficking arrest in Brandenburg set the Chemical Revolution investigation into motion; German authorities arrested a 26-year-old in Brandenburg who had close to 50 kilograms of amphetamine, 16 kilograms of cannabis, 2 kilograms of MDMA, 900 grams of cocaine, 600 grams of heroin, and many other substances in his possession. Investigators learned that the suspected drug trafficker had been storing drugs for Germany's largest drug shop. They were the largest darkweb drug trafficking organization in Germany at the time of the bust. The second suspect, a 43-year-old Dutchman suspected of procuring drugs in the Netherlands and organizing transportation to Germany, was arrested in Hamburg on February 13, 2019. His arrest led to the seizure of over a total of 14 kilograms of a variety of drugs. A 24-year-old German from Hamburg suspected of mailing the drugs sold by Chemical Revolution was arrested the same day. On February 19, 2019, a 34-year-old Hamburg man was arrested. Authorities accused the man of renting apartments in Hamburg as a part of the Chemical Revolution operation. According to prosecutors, co-conspirators used the apartments as staging areas where they packaged the drugs and prepared them for shipment to customers. Authorities arrested a 26-year-old and a 25-year-old the same day. Both had allegedly helped package and ship drugs for Chemical Revolution. A 35-year-old German from Teltow-Fläming allegedly organized the transport of the drugs from the Netherlands to Germany for resale. Police arrested him on February 25, 2019. On February 28, 2019, a 44-year-old Polish man was arrested in Diepholz. He is also suspected of overseeing the transport of narcotics to Germany. On March 27, 2019, the police arrested another package courier-a 32-year-old Polish man was arrested in Poland. German authorities won the extradition case and had the man in custody in Germany on April 12, 2019. German police arrested a 29-year-old man from Hamburg on April 29, 2019. Authorities accused the 29-year-old of overseeing the transportation of drugs between different Chemical Revolution co-conspirators. Law enforcement in Spain arrested a 26-year-old German man on May 28, 2019. German authorities accused the 26-year-old of creating and managing the accounts and sites used by Chemical Revolution. The suspect also managed the organization's funds, according to prosecutors. Only three sentences are final, according to the public prosecutor's office. The District Court expects the trial to take 15 days.

Australian Vendor "Underlinecost" Made Up to $25K Every Day

Three Australians made as much as $25,000 a day by selling drugs through the vendor account "underlinecost.” (1 AUD = 0.73 USD) In November 2021, SA Police reported arresting three people for their alleged roles in a prolific darkweb drug trafficking operation: Two men and a woman have been arrested following an operation by the Financial and Cybercrime Investigation Branch, High Tech Crime Section into their alleged drug trafficking activities on the dark web. On Monday 22 November, Detectives from SAPOL's Financial and Cybercrime Investigation Branch and Australian Federal Police searched a home and business

address in Adelaide and a property in Kings Park. Cash seized during the investigation | SA Police One million dollars in cash and $700, 000 of cryptocurrency was seized along with drugs suspected to be cocaine, LSD, cannabis, and steroids with an estimated street value of over $150, 000. In addition; Confiscations Section has seized two residential properties and a sports motorcycle, collectively valued at $1.27 million. This is the largest ever seizure of cryptocurrency by SAPOL. A 27-year-old man and a 32-year-old woman, both from Adelaide, and a 24-year-old man from Kings Park were arrested and charged with multiple counts of commercial drug trafficking, money laundering, and importation of a large commercial quantity of LSD. All three have appeared in the Adelaide Magistrates Court and were remanded in custody to next appear in court on 24 May 2022. After the arrest, it appeared as if some Dread users correctly identified the vendor as underlinecost. Local news outlets have confirmed as much. The underlinecost vendor account on Darkode has also confirmed this; SA police changed the profile picture to an announcement that they had a search warrant for the account. Very clever police. darkodemard3wjoe63ld6zebog73ncy77zb2iwjtdjam4xwvpjmjitid.onion/underlinecost/profile It does not appear as if law enforcement accessed the account since November 2021 though. A listing on the underlinecost profile on Darkode market. Investigation Australian law enforcement started investigating the alleged syndicate after intercepting a package from Germany containing 8,000 LSD tabs. A phone number on the package led investigators to a mailbox where they observed former police officer Thomas James Booker, 27, dropping off packages. Erin Gold, 32, who worked as "an accountant and burlesque dancer,” apparently had a relationship with Booker. They lived together and co-owned properties. Cocaine seized during the investigation | SA Police Police have not revealed how they made the connection between the identification of Booker and the underlinecost vendor account. However, undercover law enforcement officers purchased drugs from underlinecost as a part of the investigation. Police identified fingerprints on the packages that belonged to Booker and one of his co-conspirators, Ryan Suri-Tucker, 24. Booker, Gold, and the other guy Arrests In November 2021, the police raided a Kings Park property and arrested both men. Police reported that both men had drugs piled up around them at a desk. On the desk was a computer that was signed into the underlinecost account on a marketplace, according to the police. Police later arrested Gold at her workplace. Marijuana seized during the investigation | SA Police During a bail hearing, a prosecutor explained the discoveries made by police after searching the property: "When police attended the address they found the pair sitting at a desk together in front of a computer with an open TOR session, which is access to the dark web, open into the vendor account of Underline Costs with a list of unfilled orders. There were drugs seized at that location, including a commercial quantity of LSD and trafficable quantities of cocaine, cannabis, and MDMA. Those items were on the table in front of them. Some of them had been divided into smaller quantities ready for delivery. Also on the table in front of them packaged ready to be shipped in Australia Post packages. There was also a ledger book, which appeared to be a record of every sale including the amount and tracking number. It appears this was all run as a business. Police estimate they were turning over about $25,000 a day.” Assets A raid at the house belonging to Booker and Gold resulted in the seizure of $350,000. A locked box at the Public Trustee's office belonging to Booker contained $460,000. Police froze $900,000 in cryptocurrency. All three suspects had cryptocurrency holdings. Police have applied to freeze an apartment worth $500,000 owed by Booker and Gold, a property in Athol Park worth $500,000 owned by Gold, and a 2020 Ducati. Steroids seized during the investigation | SA Police Updates Gold, in her bail applications, is trying to place the blame entirely on Booker. Gold's lawyer: "The involvement of Ms. Gold is in effect because of her association with her partner, one of the co-accused. She was not at that location when the arrest occurred. Ms. Gold was arrested at her workplace where she was undergoing full-time employment. In my submission, her connection to Mr. Booker is the basis for her being charged.” Her bail application was adjourned until later this month.

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

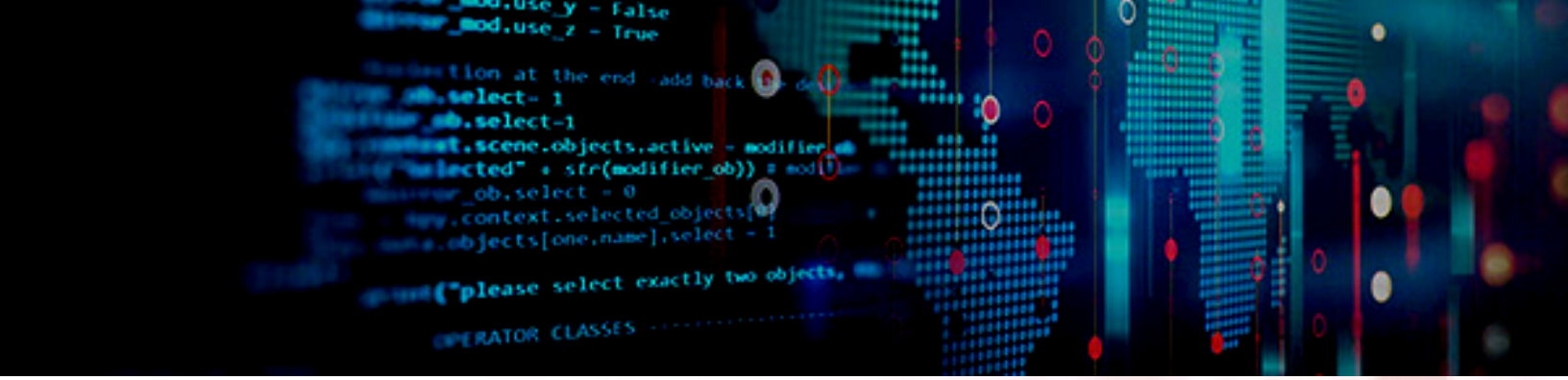
users time to finalize their orders and withdraw funds. From the lack of complaints, it appears as if the majority of users succeeded in pulling their funds prior to the market's shutdown. ToRReZ, it appears, has joined the list of graceful closures. In their original retirement announcement, the market 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

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

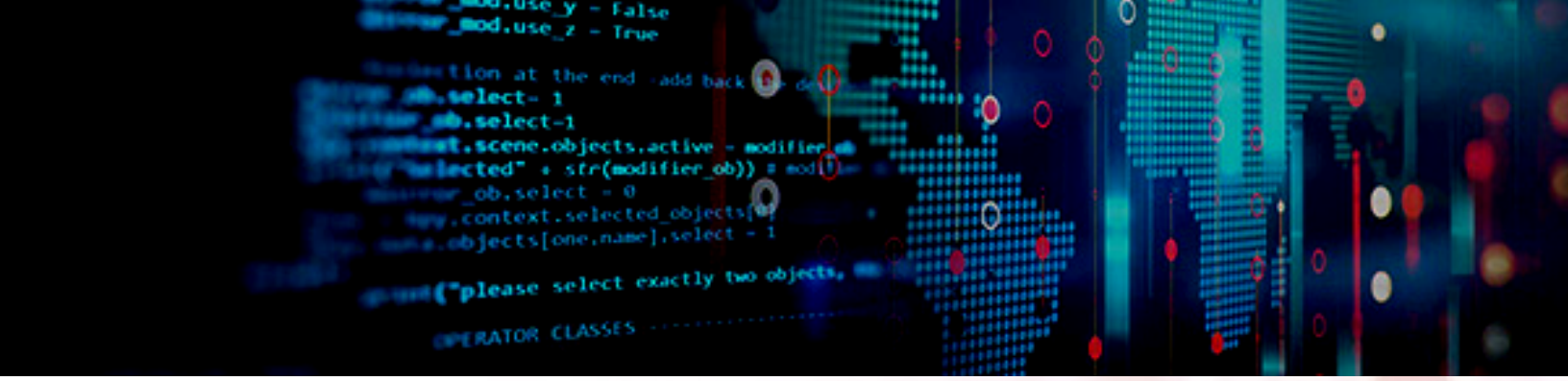
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* The 2021 Naughty and Nice Lists: Cybersecurity Edition
* Log4Shell Strategic Response: 5 Practices for Vulnerability Management at Scale
* Metasploit Wrap-Up
* What's New in Threat Intelligence: 2021 Year in Review
* What's New in InsightIDR: Q4 2021 in Review
* 2022 Cybersecurity Predictions: The Experts Clear Off the Crystal Ball
* Rapid7 2021 Wrap-Up: Highlights From a Year of Empowering the Protectors
* Metasploit 2021 Annual Wrap-Up
* 5 Security Projects That Are Giving Back
* Sharing the Gifts of Cybersecurity - Or, a Lesson From My First Year Without Santa



Advisories

US-Cert Alerts & bulletins

* WordPress Releases Security Update
* Google Releases Security Updates for Chrome
* VMware Releases Security Updates
* 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
* 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 27, 2021
* Vulnerability Summary for the Week of December 20, 2021

Zero Day Initiative Advisories

ZDI-CAN-15633: Cisco
A CVSS score 4.3 (AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-15782: NETGEAR
A CVSS score 3.1 (AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N) severity vulnerability discovered by ' Flashback Team: Pedro Ribeiro (@pedrib1337) && Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-14791: ZyXel
A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-15756: Trend Micro
A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-15757: Trend Micro
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 'Anonymous' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-16159: Trend Micro

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 '@Kharosx0' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-16162: Zoom

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 '@Kharosx0' was reported to the affected vendor on: 2022-01-07, 3 days ago. The vendor is given until 2022-05-07 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-15594: Siemens

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 'xina1i at psbc' was reported to the affected vendor on: 2022-01-05, 5 days ago. The vendor is given until 2022-05-05 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-15599: Siemens

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 'xina1i at psbc' was reported to the affected vendor on: 2022-01-05, 5 days ago. The vendor is given until 2022-05-05 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-15738: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-01-05, 5 days ago. The vendor is given until 2022-05-05 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-15602: Siemens

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 'xina1i at psbc' was reported to the affected vendor on: 2022-01-05, 5 days ago. The vendor is given until 2022-05-05 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-16070: 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, 11 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-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, 11 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, 11 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, 11 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, 11 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, 11 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, 11 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, 11 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, 11 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, 11 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, 11 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, 17 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, 19 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.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5213-1

Ubuntu Security Notice 5213-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Red Hat Security Advisory 2021-5208-05

Red Hat Security Advisory 2021-5208-05 - 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 4.8.25.

Ubuntu Security Notice USN-5211-1

Ubuntu Security Notice 5211-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages.

Ubuntu Security Notice USN-5210-1

Ubuntu Security Notice 5210-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. It was discovered that the Linux kernel did not properly enforce certain types of entries in the Secure Boot Forbidden Signature Database protection mechanism. An attacker could use this to bypass UEFI Secure Boot restrictions.

Kernel Live Patch Security Notice LSN-0083-1

The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence where inner instructions require substantial expansions into multiple BPF instructions, leading to an overflow. This affects kernel/bpf/core.c and net/core/filter.c. Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. Other vulnerabilities have also been addressed.

Ubuntu Security Notice USN-5209-1

Ubuntu Security Notice 5209-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. It was discovered that a race condition existed in the timer implementation in the Linux kernel. A privileged attacker could use this cause a denial of service.

Red Hat Security Advisory 2022-0034-01

Red Hat Security Advisory 2022-0034-01 - Red Hat Single Sign-On 7.5 container images for IBM P/Z, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This is a security update Red Hat Single Sign-On 7.5, and includes one security fix.

Ubuntu Security Notice USN-5208-1

Ubuntu Security Notice 5208-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5207-1

Ubuntu Security Notice 5207-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages. It was discovered that the eBPF implementation in the Linux kernel contained a race condition around read-only maps. A privileged attacker could use this to modify read-only maps.

Ubuntu Security Notice USN-5212-1

Ubuntu Security Notice 5212-1 - It was discovered that the Apache HTTP Server incorrectly handled certain forward proxy requests. A remote attacker could use this issue to cause the server to crash, resulting in a

denial of service, or possibly perform a Server Side Request Forgery attack. It was discovered that the Apache HTTP Server Lua module incorrectly handled memory in the multipart parser. A remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5206-1

Ubuntu Security Notice 5206-1 - Nadav Amit discovered that the hugetlb implementation in the Linux kernel did not perform TLB flushes under certain conditions. A local attacker could use this to leak or alter data from other processes that use huge pages.

Ubuntu Security Notice USN-5204-1

Ubuntu Security Notice 5204-1 - Chris Bailey discovered that Django incorrectly handled evaluating submitted passwords. A remote attacker could possibly use this issue to consume resources, resulting in a denial of service. Dennis Brinkrolf discovered that Django incorrectly handled the dictsort template filter. A remote attacker could possibly use this issue to obtain sensitive information. Dennis Brinkrolf discovered that Django incorrectly handled certain file names. A remote attacker could possibly use this issue to save files to arbitrary filesystem locations.

Red Hat Security Advisory 2022-0015-01

Red Hat Security Advisory 2022-0015-01 - Red Hat Single Sign-On 7.5 container images, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This is a security update Red Hat Single Sign-On 7.5, and includes one security fix.

VMware Security Advisory 2022-0001

VMware Security Advisory 2022-0001 - VMware Workstation, Fusion and ESXi updates address a heap overflow vulnerability.

Red Hat Security Advisory 2022-0008-03

Red Hat Security Advisory 2022-0008-03 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Red Hat Security Advisory 2022-0007-02

Red Hat Security Advisory 2022-0007-02 - Red Hat Identity Management is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments.

Red Hat Security Advisory 2022-0011-04

Red Hat Security Advisory 2022-0011-04 - Telnet is a popular protocol for logging in to remote systems over the Internet. The telnet-server packages include a telnet service that supports remote logins into the host machine. The telnet service is disabled by default. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-0003-03

Red Hat Security Advisory 2022-0003-03 - X.Org is an open-source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon. Issues addressed include an out of bounds access vulnerability.

Red Hat Security Advisory 2022-0001-01

Red Hat Security Advisory 2022-0001-01 - Grafana is an open source, feature rich metrics dashboard and graph editor for Graphite, InfluxDB & OpenTSDB.

Red Hat Security Advisory 2022-0002-01

Red Hat Security Advisory 2022-0002-01 - Grafana is an open source, feature rich metrics dashboard and graph editor for Graphite, InfluxDB & OpenTSDB.

Red Hat Security Advisory 2021-5269-03

Red Hat Security Advisory 2021-5269-03 - Log4j is a tool to help the programmer output log statements to a variety of output targets. Issues addressed include a code execution vulnerability.

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

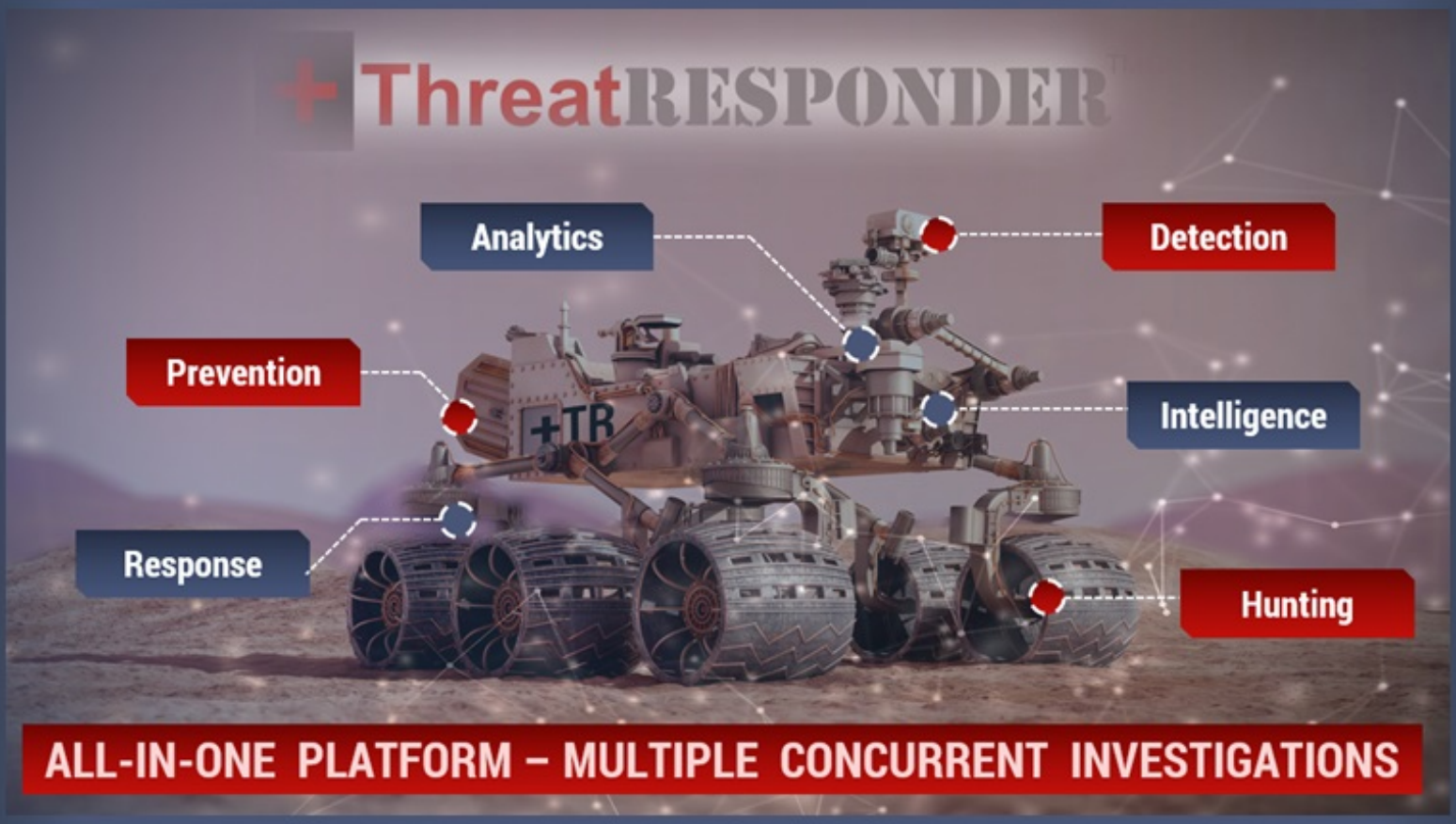
Red Hat Security Advisory 2021-5236-02 - PostgreSQL is an advanced object-relational database management system. Issues addressed include a man-in-the-middle vulnerability.

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



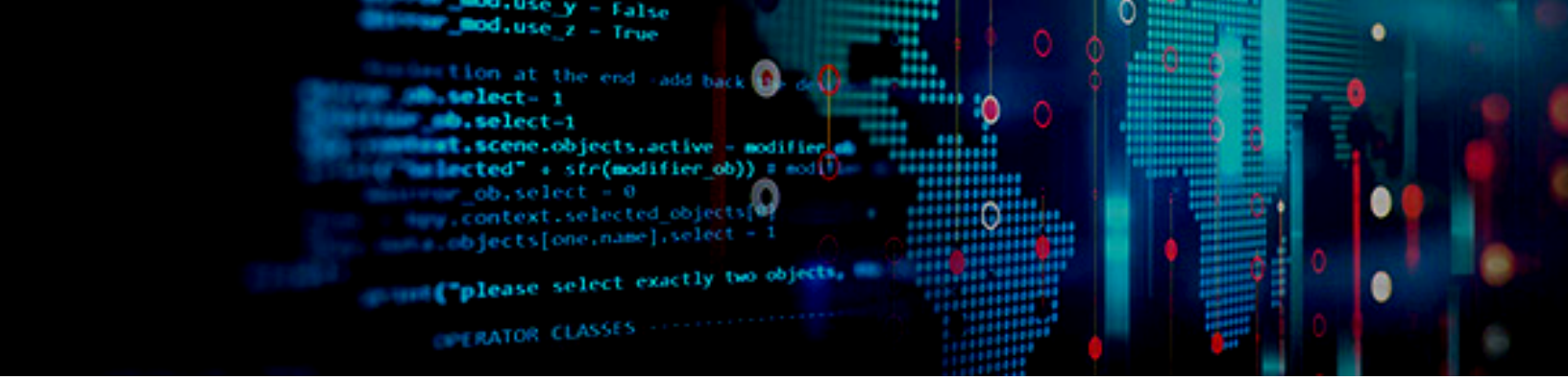
The Solution – ThreatResponder® Platform

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

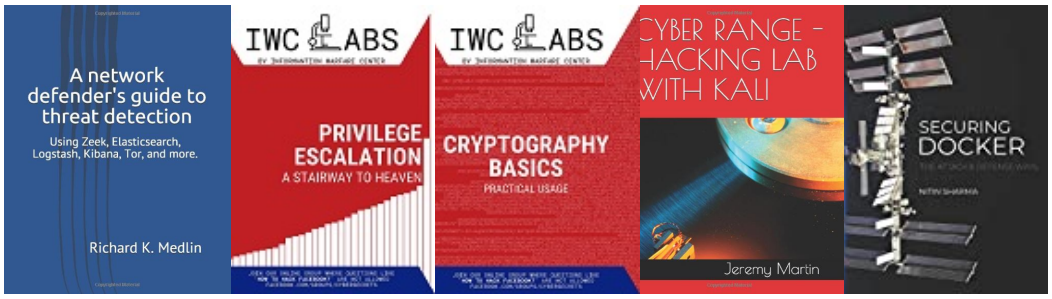


The Cyber Secrets publications on Amazon

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