Dec-13-21

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

December 13, 2021

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

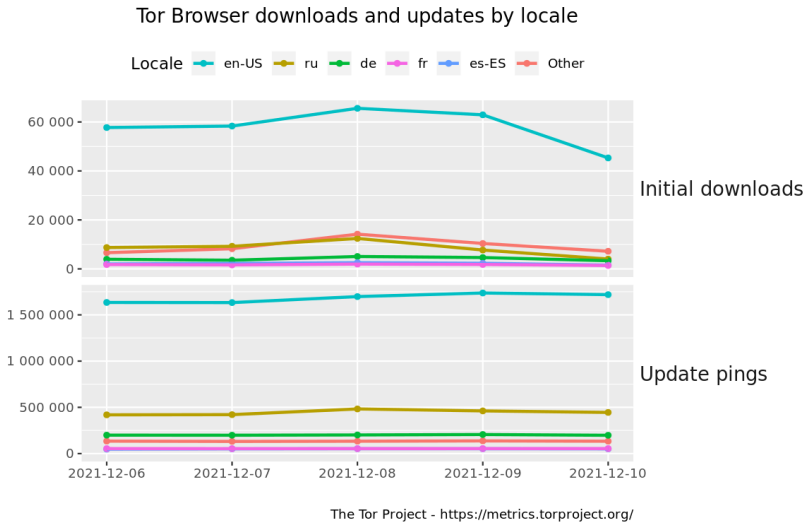
Internet Storm Center Infocon Status

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

* **Cyber Monday:** 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. This is a prerequizite for all other courses CSI Linux offers.

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

Index of Sections

Packet Storm Security

* Polish Regulator To Investigate Apple's Privacy Policy
* Are Your Home Security Cameras Vulnerable To Hacking?
* Indian PM Modi's Twitter Hacked With Bitcoin Tweet
* Log4j Zero Day Flaw: What You Need To Know And How To Protect Yourself
* Julian Assange Can Be Extradited To US, Court Rules
* 300,000 MikroTik Routers Are Security Ticking Timebombs, Say Researchers
* Worst Apache Log4j RCE Dropped On Internet
* This Decade Old Malware Has Picked Up Some Nasty New Tricks
* Ransomwared Payroll Provider Leaks Data On 38,000 Australian Government Workers
* AWS Is The Internet's Biggest Single Point Of Failure
* Tor Is Under Threat From Russian Censorship And Sybil Attacks
* Malicious npm Code Packages Built For Hijacking Discord Servers
* Deepfakes Widen Fraud Opportunities For Financial Hackers
* AWS Among 12 Cloud Services Affected By Flaws In Eltima SDK
* Everyone Is Burned Out. That's Becoming A Security Nightmare
* Hacker Named Bowser Must Pay Nintendo $10 Million In Piracy Case
* Google Takes Down Glupteba Botnet
* Canadian Indicted For Launching Ransomware Attacks
* RTF Injection Poised For More Widespread Adoption
* Apache Kafka Cloud Clusters Expose Sensitive Data For Companies
* Court Allows Microsoft To Dismantle Infrastructure Of APT15
* Founder Of Massive Robo Text Service Accused Of Running Secret Spying Operation
* Losses From BitMart Breach Reach $200 Million
* BitMart Crypto Exchange Loses $150 Million To Hackers
* SolarWinds Hackers Keep Compromising Targets

Krebs on Security

* 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
* Tech CEO Pleads to Wire Fraud in IP Address Scheme
* Hoax Email Blast Abused Poor Coding in FBI Website
* SMS About Bank Fraud as a Pretext for Voice Phishing
* Microsoft Patch Tuesday, November 2021 Edition

Dark Reading

* Tales from the Dark Web: Fingerprinting Access Brokers on Criminal Forums
* Why Classifying Ransomware as a National Security Threat Matters
* How Do I Find My Servers With the Log4j Vulnerability?
* Volvo Confirms R&D Data Stolen in Breach
* Kronos Suffers Ransomware Attack, Expects Full Restoration to Take 'Weeks'
* 40% of Corporate Networks Targeted by Attackers Seeking to Exploit Log4j
* Bug-Bounty Programs Shift Focus to Most Critical Flaws
* Name That Toon: Modern-Day Frosty
* Darktrace Reports Information Technology and Communications Sector Most Targeted by Cyberattackers in
* Kaspersky Opens Doors to New Transparency Center in North America
* 2 Website Threats to Address for the Holiday Shopping Rush
* Why the Private Sector Is Key to Stopping Russian Hacking Group APT29
* Why Cloud Service Providers Are a Single Point of Failure
* What to Do While Waiting for the Log4J Updates
* Security Experts Sound Alarm on Zero-Day in Widely Used Log4j Tool
* NIST Cyber-Resiliency Framework Extended to Include Critical Infrastructure Controls
* Russian National Sentenced for Role in Kelihos Botnet
* Identity Authentication Access Market Set to Hit $28.9B in 2021
* Dark Reading Reflects on a Legacy and Life Well-Written: Tim Wilson
* The Vulnerability Lag: Cut Ransomware Risks Resulting From Digital Transformation

The Hacker News

* Karakurt: A New Emerging Data Theft and Cyber Extortion Hacking Group
* Top 3 SaaS Security Threats for 2022
* Microsoft Details Building Blocks of Widely Active Qakbot Banking Trojan
* Apache Log4j Vulnerability - Log4Shell - Widely Under Active Attack
* Extremely Critical Log4J Vulnerability Leaves Much of the Internet at Risk
* BlackCat: A New Rust-based Ransomware Malware Spotted in the Wild
* 1.6 Million WordPress Sites Under Cyberattack From Over 16,000 IP Addresses
* Russia Blocks Tor Privacy Service in Latest Censorship Move
* Over 300,000 MikroTik Devices Found Vulnerable to Remote Hacking Bugs
* Why Holidays Put Your Company at Risk of Cyber Attack (And How to Take Precautions)
* Over a Dozen Malicious NPM Packages Caught Hijacking Discord Servers
* SonicWall Urges Customers to Immediately Patch Critical SMA 100 Flaws
* Google Disrupts Blockchain-based Glupteba Botnet; Sues Russian Hackers
* 140,000 Reasons Why Emotet is Piggybacking on TrickBot in its Return from the Dead
* [eBook] Guide to Achieving 24x7 Threat Monitoring and Response for Lean IT Security Teams

Security Week

* Apple Patches 42 Security Flaws in Latest iOS Refresh
* Ransomware Affiliate Arrested in Romania
* Logistics Firm Hellmann Scrambling to Recover From Cyberattack
* Cybersecurity M&A Roundup for December 1-12, 2021
* Germany Jails Operators of 'Cyberbunker' Darknet Hub
* CISA Expands 'Must-Patch' List With Log4j, FortiOS, Other Vulnerabilities
* Companies Respond to Log4Shell Vulnerability as Attacks Rise
* Mirai-Based 'Manga' Botnet Targets Recent TP-Link Vulnerability
* Indian PM's Twitter Hacked Again by Crypto Scammers
* Hackers Steal Research Data From Sweden's Volvo Cars
* Exploits Swirling for Major Security Defect in Apache Log4j
* WD Updates SanDisk SecureAccess to Prevent Dictionary, Brute Force Attacks
* Fujitsu Retires Tool Targeted by Threat Actors
* Afero Raises $50 Million for Its Secure IoT Platform
* Russian Who Helped Kelihos Malware Evade Detection Sentenced to 4 Years in Prison
* UK Court Allows Assange's Extradition to US for Spying Case
* Saudi Activist Sues 3 Former U.S. Officials Over Hacking
* Work-from-Anywhere Requires "Work-from-Anywhere Security"
* Ex-Googlers Snag $5 Million for Software Supply Chain Security Tech
* Email Security Company IronScales Raises $64 Million
* Volume of Attacks on IoT/OT Devices Increasing: Microsoft Study
* Facebook, GDPR and Max Schrems - Under the Hood of GDPR Legal Processes
* Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird
* Ransomware Operators Leak Data Stolen From Wind Turbine Giant Vestas
* 'Moobot' Botnet Targets Hikvision Devices via Recent Vulnerability

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Socially Engineering Your Way to Customer Data
* 2021 Security Hints & Tips for Holiday Travels
* Real Cyberattack as Phishbait for a Scammer
* Credential-Harvesting Phishing Campaign Urges Review of Spam
* Victims: After a Data Breach, Changing Passwords and Good Password Hygiene Remain Unimportant
* New TSA PreCheck Scam Seeks to Collect Your Personal and Credit Card Details
* Half of All Organizations Have Had Employees Approached to Aid in Ransomware Attacks
* SideCopy: How an Intelligence Service Uses Phishbait
* CyberheistNews Vol 11 #48 [Heads Up] Morgan Stanley Warns Against Recent "Brushing Scam"
* Conducting Data Protection Impact Assessments on Your Cloud Environments

ISC2.org Blog

* CCSP vs. Microsoft Azure Certified Security Engineer Associate - How Does Vendor Focus Factor In?
* What is Relevant Work Experience for CISSP?
* (ISC)² Ransomware Study: Collaboration and Communication are Essential for Ransomware Readiness
* CCSP vs. Google Cloud Certified-Professional Cloud Security Engineer: Which Shows Broader Mastery in
* (ISC)² Cybersecurity Scholarship Opportunities - Open Now!

HackRead

* Indian PM Modi's Twitter Account HACKED for Bitcoin scam
* Ascendex cryptocurrency exchange hacked - $77 million stolen
* Canadian Citizen Charged for Ransomware Attacks in Alaska
* Hackers actively exploiting 0-day in Ubiquitous Apache Log4j tool
* Fields of application of artificial intelligence
* Kali Linux 2021.4 released with Samba compatibility, Apple M1 support, 9 new tools
* US Military's Hacking Unit to take on ransomware gangs

Koddos

* Indian PM Modi's Twitter Account HACKED for Bitcoin scam
* Ascendex cryptocurrency exchange hacked - $77 million stolen
* Canadian Citizen Charged for Ransomware Attacks in Alaska
* Hackers actively exploiting 0-day in Ubiquitous Apache Log4j tool
* Fields of application of artificial intelligence
* Kali Linux 2021.4 released with Samba compatibility, Apple M1 support, 9 new tools
* US Military's Hacking Unit to take on ransomware gangs

Naked Security

* Log4Shell explained - how it works, why you need to know, and how to fix it
* "Log4Shell" Java vulnerability - how to safeguard your servers
* S3 Ep62: The S in IoT stands for security (and much more) [Podcast+Transcript]
* Firefox update brings a whole new sort of security sandbox
* Cryptocurrency startup fails to subtract before adding, loses $31m
* Mozilla patches critical "BigSig" cryptographic bug: Here's how to track it down and fix it
* S3 Ep61: Call scammers, cloud insecurity, and facial recognition creepiness [Podcast+Transcript]
* IoT devices must "protect consumers from cyberharm", says UK government
* Clearview AI face-matching service set to be fined over $20m
* Cloud Security: Don't wait until your next bill to find out about an attack!

Threat Post

* Kronos Ransomware Outage Drives Widespread Payroll Chaos
* Where the Latest Log4Shell Attacks Are Coming From
* Malicious PyPI Code Packages Rack Up Thousands of Downloads
* Log4Shell Is Spawning Even Nastier Mutations
* Next-Gen Maldocs & How to Solve the Human Vulnerability
* 'Appalling' Riot Games Job Fraud Takes Aim at Wallets
* Zero Day in Ubiquitous Apache Log4j Tool Under Active Attack
* Sprawling Active Attack Aims to Take Over 1.6M WordPress Sites
* 'Karakurt' Extortion Threat Emerges, But Says No to Ransomware
* Canadian Ransomware Arrest Is a Meaningful Flex, Experts Say

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

* A Journey in Organizational Resilience: Geopolitical and Socio-Economic Trends and Threats
* One-Time Password Security Might Fail 80% of the Time. IAM is Better
* How Log4j Vulnerability Could Impact You
* How to Include Cybersecurity Training in Employee Onboarding
* IoT Security: Protecting Food and Agriculture Organizations
* IAM OT Security Risks Call for Strategic Defenses
* Edge Computing and 5G: Will Security Concerns Outweigh Benefits?
* What to Do When a Ransomware Group Disappears
* Understanding the Cyber Risk Exposures Within the Health Care Industry
* 7 Holiday Cybersecurity Tips to Try Before The Year Ends

InfoWorld

* JDK 18: The new features in Java 18
* Mulesoft updates Anypoint to streamline API management, support devops
* What should HashiCorp do now?
* How canary releases enable continuous deployment
* How to choose a cloud data warehouse
* How to detect the Log4j vulnerability in your applications
* Visual Studio Code tweaks problem navigation, screencast mode
* The true value of serverless computing
* GitHub previews enhanced code search
* Get started with Git

C4ISRNET - Media for the Intelligence Age Military

* The Navy is testing this adorable sailboat drone
* US Army officials: Service needs 'true data fabric'
* Officials say US Army armored brigades need a stronger network
* Pentagon creates new digital and artificial intelligence office
* Five things the Army learned about its network at Project Convergence 21
* Extend the unmanned revolution to our allies
* Space Force launches experimental payloads into orbit
* Air Force previews plan to phase out enlisted drone pilots
* French defense minister: Shifting from a new frontier to a new front
* IISS analysts: Fiscal constraints drive the state of South America's defense

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

* This shouldn't have happened: A vulnerability postmortem
* Windows Exploitation Tricks: Relaying DCOM Authentication

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.

* CTF Internacional MetaRed 2021 - 5th STAGE
* hxp CTF 2021
* X-MAS CTF 2021 Second Weekend
* Trend Micro CTF 2021 - Raimund Genes Cup - Virtual Final
* STAY ~/ CTF 2021
* ASIS CTF Finals 2021
* ISITDTU CTF 2021 Finals
* SCTF 2021
* TetCTF 2022
* Global CyberPeace Challenge 3.0 CTF-IT

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

* 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
* Stegano 0.10.1
* Photon OSINT Crawler 1.3.2
* OpenStego Free Steganography Solution 0.8.2
* GNU Privacy Guard 2.2.33
* Wireshark Analyzer 3.6.0

Kali Linux Tutorials

* FakeDataGen : Full Valid Fake Data Generator
* ELFXtract : An Automated Analysis Tool Used For Enumerating ELF Binaries
* Nanobrok : Web Service For Control And Protect Your Android Device Remotely
* LOLBins : PyQT5 App For LOLBAS And GTFOBins
* goEnumBruteSpray : User Enumeration And Password Bruteforce On Azure, ADFS, OWA, O365 And Gather Emai
* Redherd Framework : A Collaborative And Serverless Framework
* Whoc : A Container Image That Extracts The Underlying Container Runtime
* Whispers : Identify Hardcoded Secrets In Static Structured Text
* Hashdb-Ida : HashDB API Hash Lookup Plugin For IDA Pro
* Etl-Parser : Event Trace Log File Parser In Pure Python

GBHackers Analysis

* Oxeye Identifies Vulnerabilities Cloud Native Applications with CNAST Platform
* Printing Shellz - New Vulnerabilities That Affects 150 Different Multifunction Printers
* North Korean Hackers Group Posed as Samsung Recruiters To Target Security Firms
* Two Iranian Hackers Charged For Gaining Access to Confidential Voter Information
* Void Balaur - Hacker-for-Hire Group Stealing Emails & Sensitive Data From More Than 3,500 Targets

Weekly Cyber Security Video and Podcasts

SANS DFIR

* 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
* Hunting Beacon Activity with Fourier Transforms

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

* Keep Computers From Locking with a CircuitPython Mouse Jiggler | HakByte
* Government Employee Phones Hacked, Cryptocurrency Scams On The Rise - ThreatWire
* Making a Hardware WiFi Recon Tool with the ESP8266 | HakByte

The PC Security Channel [TPSC]

* Antivirus Tierlist: Best Antivirus in 2021
* Phobos Ransomware

Eli the Computer Guy

* OMICRON INFECTS the VACCINATED and BOOSTED... and previously infected...
* Why COVID KILLS FAT PEOPLE - 30% hospitalization due to obesity...
* FOURTH COVID VACCINE DOSE COMING SOON... says pfizer ceo...
* Office Hours - Tech Question and Answers

Security Now

* XSinator - NSS Has a Bug, Botnet on the Blockchain, HP's Vulnerable Printers, Microsoft Edge Relief
* Bogons Begone! - 0-Day Windows Exploit, Major MediaTek Flaw, Super Duper Secure Mode

Troy Hunt

* Weekly Update 273

Intel Techniques: The Privacy, Security, & OSINT Show

* 243-Emergency Bags
* 242-Privacy News & Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Oracle Database Weak NNE Integrity Key Derivation
* Backdoor.Win32.Phase.11 Code Execution
* Oracle Database Protection Mechanism Bypass
* Backdoor.Win32.Ramus Code Execution
* WebHMI 4.0 Remote Code Execution
* Backdoor.Win32.Jokerdoor Buffer Overflow
* Backdoor.Win32.FTP.Matiteman Weak Hardcoded Password
* Backdoor.Win32.BackAttack.20 Authentication Bypass / Code Execution
* Simple Forum-Discussion System 1.0 SQL Injection
* Backdoor.Win32.BackAttack.20 Code Execution
* Backdoor.Win32.Ncx.b Buffer Overflow
* Backdoor.Win32.Ncx.b Code Execution
* HD-Network Real-Time Monitoring System 2.0 Local File Inclusion
* Backdoor.Win32.Nucleroot.mf Buffer Overflow
* Backdoor.Win32.Asylum.014 Insecure Password Storage
* Backdoor.IRC.Subhuman Unauthenticated Open Proxy
* Backdoor.Win32.Mechbot.a Insecure Permissions
* OpenCATS 0.9.4 Remote Code Execution
* Free School Management Software 1.0 Cross Site Scripting
* Free School Management Software 1.0 Shell Upload
* Polkit CVE-2021-3560 Research
* Apache Log4j2 2.14.1 Remote Code Execution
* Grafana 8.3.0 Directory Traversal / Arbitrary File Read
* Microsoft Office Word MSHTML Remote Code Execution
* LimeSurvey 5.2.4 Remote Code Execution

CXSecurity

* WebHMI 4.0 Remote Code Execution
* Microsoft Office Word MSHTML Remote Code Execution
* LimeSurvey 5.2.4 Remote Code Execution
* Grafana 8.3.0 Directory Traversal / Arbitrary File Read
* Ubuntu Overlayfs Local Privilege Escalation
* Advanced Comment System 1.0 Remote Command Execution
* Pinkie 2.15 TFTP Remote Buffer Overflow (PoC)

Proof of Concept (PoC) & Exploits

Exploit Database

* [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
* [webapps] Wordpress Plugin Catch Themes Demo Import 1.6.1 - Remote Code Execution (RCE) (Authenticate
* [webapps] Student Management System 1.0 - SQLi Authentication Bypass
* [webapps] TestLink 1.19 - Arbitrary File Download (Unauthenticated)
* [remote] Raspberry Pi 5.10 - Default Credentials
* [local] MTPutty 1.0.1.21 - SSH Password Disclosure
* [webapps] LimeSurvey 5.2.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Chikitsa Patient Management System 2.0.2 - 'backup' Remote Code Execution (RCE) (Authentica
* [webapps] Chikitsa Patient Management System 2.0.2 - 'plugin' Remote Code Execution (RCE) (Authentica
* [webapps] Croogo 3.0.2 - Remote Code Execution (Authenticated)
* [remote] Auerswald COMpact 8.0B - Multiple Backdoors
* [remote] Auerswald COMpact 8.0B - Arbitrary File Disclosure
* [remote] Auerswald COMpact 8.0B - Privilege Escalation
* [local] HCL Lotus Notes V12 - Unquoted Service Path
* [remote] Auerswald COMfortel 2.8F - Authentication Bypass
* [webapps] WordPress Plugin DZS Zoomsounds 6.45 - Arbitrary File Read (Unauthenticated)
* [webapps] WordPress Plugin Slider by Soliloquy 2.6.2 - 'title' Stored Cross Site Scripting (XSS) (Aut
* [webapps] WordPress Plugin All-in-One Video Gallery plugin 2.4.9 - Local File Inclusion (LFI)

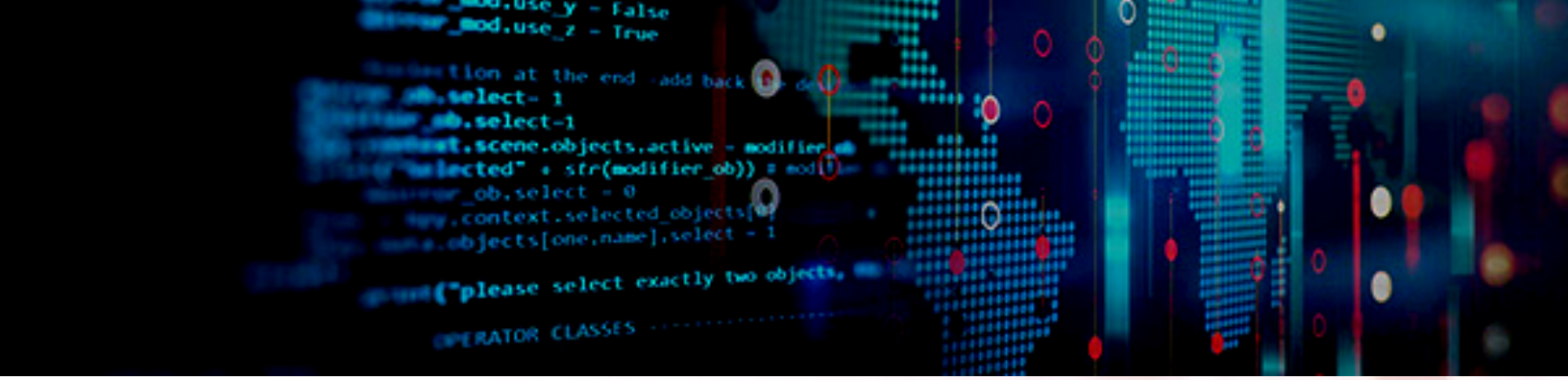
Exploit Database for offline use

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

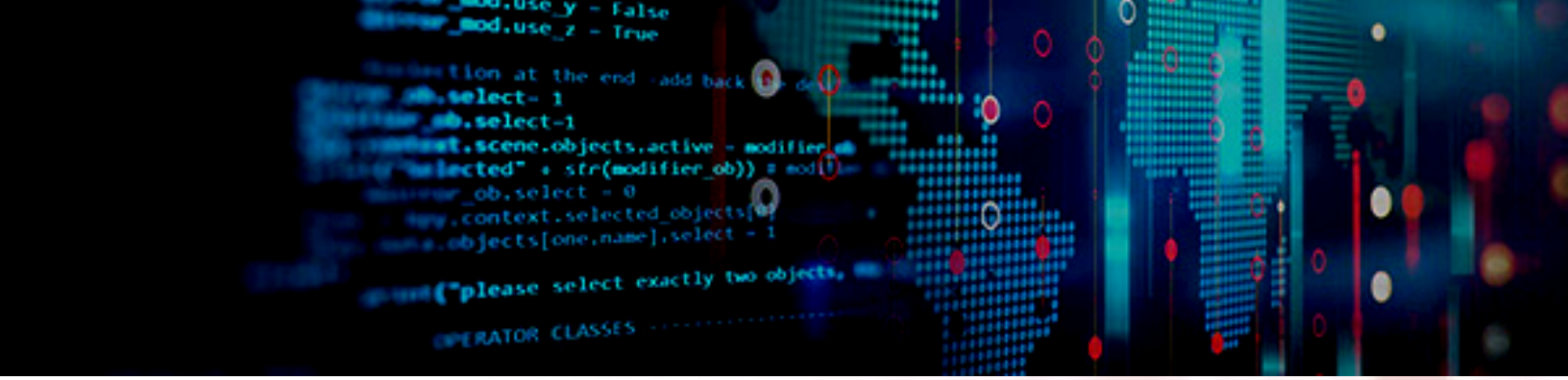
also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://sikhiu.go.th/wh.html
https://sikhiu.go.th/wh.html notified by Mr.Kro0oz.305
https://nongbuokhok.go.th/wh.html
https://nongbuokhok.go.th/wh.html notified by Mr.Kro0oz.305
https://nonthai.go.th/wh.html
https://nonthai.go.th/wh.html notified by Mr.Kro0oz.305
https://srd.gov.al/er.php
https://srd.gov.al/er.php notified by LahBodoAmat
https://banzae.ba.gov.br
https://banzae.ba.gov.br notified by Shield iran
https://turismovilleta.gov.co/jkt48.htm
https://turismovilleta.gov.co/jkt48.htm notified by Melody-x48
https://semed.manaus.am.gov.br
https://semed.manaus.am.gov.br notified by TheLevelSevenCrew
http://trem.trensurb.gov.br
http://trem.trensurb.gov.br notified by Paraná Cyber Mafia
http://www.trensurb.com.br
http://www.trensurb.com.br notified by Paraná Cyber Mafia
http://www.trensurb.gov.br
http://www.trensurb.gov.br notified by Paraná Cyber Mafia
https://sgi.corpamag.gov.co/b4.html
https://sgi.corpamag.gov.co/b4.html notified by 0x1998
http://bapelkescikarang.bppsdmk.kemkes.go.id/miaw.php
http://bapelkescikarang.bppsdmk.kemkes.go.id/miaw.php notified by SABUNMANDI CYBER TEAM
http://reg-users.dft.go.th/mad.txt
http://reg-users.dft.go.th/mad.txt notified by Royal Battler bd
http://puskan.lan.go.id/log.htm
http://puskan.lan.go.id/log.htm notified by I Love INDONESIA
https://www.disnakan.musirawaskab.go.id/index.php
https://www.disnakan.musirawaskab.go.id/index.php notified by I Love INDONESIA
https://www.lampungselatankab.go.id/index.php
https://www.lampungselatankab.go.id/index.php notified by I Love INDONESIA
https://bqsm.gov.my/kurd.html
https://bqsm.gov.my/kurd.html notified by 0x1998



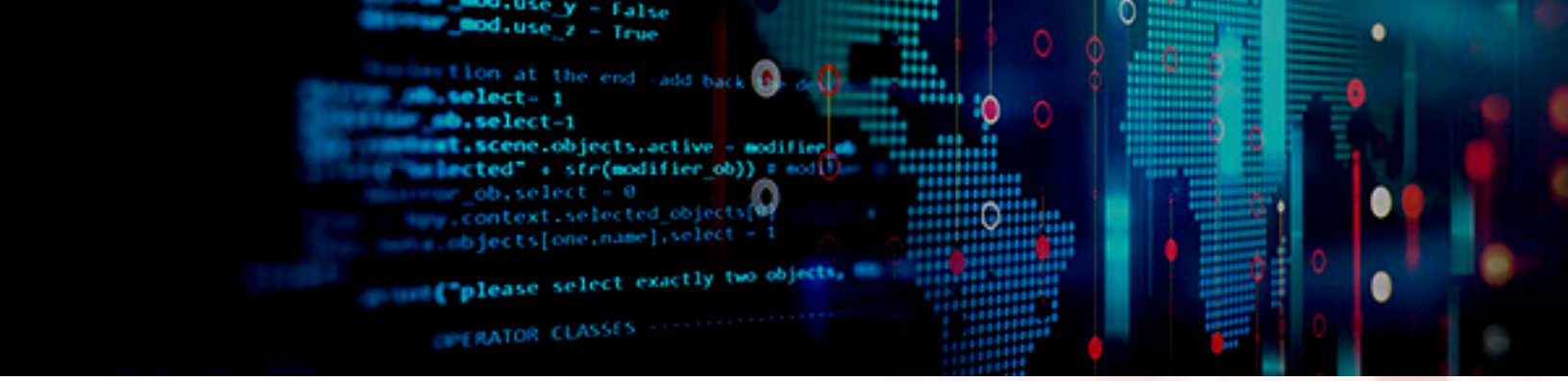
Dark Web News

Darknet Live

Empire Vendor "XanScriptz" Admits Selling Fake Xanax Pills
A man living in Virginia admitted selling counterfeit Xanax pills through a vendor account on the darkweb. (via darknetlive.com)
Bitcoin ATM CEO Pleads Guilty to FinCEN Violations
Brannen Mehaffey, the CEO of BASH Bitcoin ATMs, admitted exchanging Bitcoin for cash for undercover feds pretending to be drug dealers. (via darknetlive.com)
US Wins Appeal in Assange Extradition Case
The US won their appeal against a UK court's refusal to extradite Julian Assange, the co-founder of WikiLeaks. (via darknetlive.com)
Who is Running Hundreds of Malicious Tor Relays?
A threat actor is running hundreds of malicious Tor relays as part of what researchers suspect is an attempt to deanonymize Tor users. (via darknetlive.com)

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

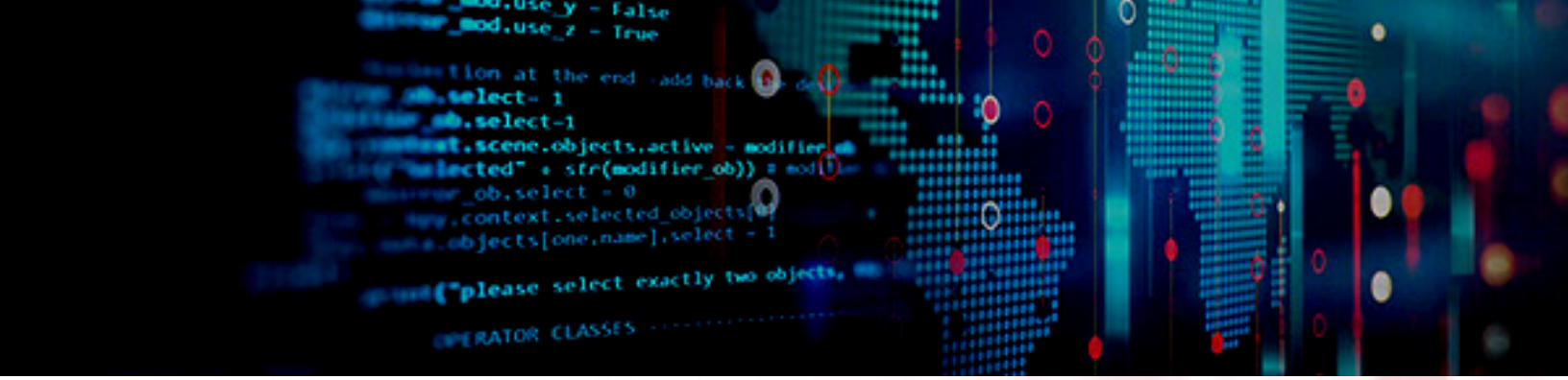
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

RiskIQ

* 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
* What 10,000 Analysts Showed Us About the State of Threat Hunting

FireEye

* Update on Log4Shell's Impact on Rapid7 Solutions and Systems
* Hacky Holidays: Celebrating the Best of Security Nation [Video]
* Driver-Based Attacks: Past and Present
* Metasploit Wrap-Up
* Widespread Exploitation of Critical Remote Code Execution in Apache Log4j
* Stay Ahead of Threats With Cloud Workload Protection
* 2022 Planning: Simplifying Complex Cybersecurity Regulations
* A Dream Team-Up: Integrate InsightAppSec With ServiceNow ITSM
* Patch Now: SonicWall Fixes Multiple Vulnerabilities in SMA 100 Devices
* Demystifying XDR: A Forrester Analyst Lays the Foundation



Advisories

US-Cert Alerts & bulletins

* CISA Creates Webpage for Apache Log4j Vulnerability CVE-2021-44228
* CISA Adds Thirteen Known Exploited Vulnerabilities to Catalog
* Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation
* CISA Releases Security Advisory for Hillrom Welch Allyn Cardiology Products
* Cisco Releases Security Advisory for Multiple Products Affected by Apache HTTP Server Vulnerabilities
* CISA Releases Guidance on Protecting Organization-Run Social Media Accounts
* SonicWall Releases Security Advisory for SMA 100 Series Appliances
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus
* AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet V
* Vulnerability Summary for the Week of December 6, 2021
* Vulnerability Summary for the Week of November 29, 2021

Zero Day Initiative Advisories

ZDI-CAN-16050: Microsoft
A CVSS score 4.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Eduardo Braun Prado' was reported to the affected vendor on: 2021-12-10, 3 days ago. The vendor is given until 2022-04-09 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-15761: Microsoft
A CVSS score 4.2 (AV:L/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: 2021-12-10, 3 days ago. The vendor is given until 2022-04-09 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-15465: Microsoft
A CVSS score 7.0 (AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Eduardo Braun Prado' was reported to the affected vendor on: 2021-12-10, 3 days ago. The vendor is given until 2022-04-09 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-16120: Oracle
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Reno Robert and Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-12-10, 3 days ago. The vendor is given until 2022-04-09 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-16033: Microsoft
A CVSS score 2.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2021-12-10, 3 days ago. The vendor is given until

2022-04-09 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-15698: Adobe

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: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15754: Microsoft

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 'kdot' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15861: 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 'Rich' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15966: Ivanti

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 'chudy' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15919: Ivanti

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15987: 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 'Rich' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-15967: Ivanti

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-12-08, 5 days ago. The vendor is given until 2022-04-07 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-16072: Apple

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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-16073: Apple

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 'Qi Sun and Robert Ai of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-16076: Apple

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 'Mickey Jin

(@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-16074: Apple

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 'Qi Sun and Robert Ai of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-16075: Apple

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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-16084: Apple

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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-15764: Microsoft

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 'kdot' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-15359: GE

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 'kimiya' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-14733: SAP

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 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-15484: Omron

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' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-15730: Microsoft

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 'kdot' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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-14868: KOYO

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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-03, 10 days ago. The vendor is given until 2022-04-02 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 2021-5082-01

Red Hat Security Advisory 2021-5082-01 - 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 2021-5002-01

Red Hat Security Advisory 2021-5002-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.9.11.

Red Hat Security Advisory 2021-5080-01

Red Hat Security Advisory 2021-5080-01 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Ubuntu Security Notice USN-5186-1

Ubuntu Security Notice 5186-1 - 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 2021-5070-02

Red Hat Security Advisory 2021-5070-02 - An update for python-django20 is now available for Red Hat OpenStack Platform 16.1 (Train). Issues addressed include local file inclusion, remote file inclusion, server-side request forgery, and traversal vulnerabilities.

Red Hat Security Advisory 2021-5072-01

Red Hat Security Advisory 2021-5072-01 - A highly-available key value store for shared configuration.

Red Hat Security Advisory 2012-5055-03

Red Hat Security Advisory 2012-5055-03 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.4.0. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5071-01

Red Hat Security Advisory 2021-5071-01 - Eventlet is a networking library written in Python. It achieves high scalability by using non-blocking io while at the same time retaining high programmer usability by using coroutines to make the non-blocking io operations appear blocking at the source code level. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-5065-05

Red Hat Security Advisory 2021-5065-05 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products.

Red Hat Security Advisory 2021-5047-02

Red Hat Security Advisory 2021-5047-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.4.0. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5036-04

Red Hat Security Advisory 2021-5036-04 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-5183-1

Ubuntu Security Notice 5183-1 - Julian Rauchberger discovered that BlueZ incorrectly handled memory when processing SDP attribute requests. A remote attacker could use this issue to cause BlueZ to crash, leading to a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2021-5045-02

Red Hat Security Advisory 2021-5045-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.4.0. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5048-02

Red Hat Security Advisory 2021-5048-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.4.0. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5046-03

Red Hat Security Advisory 2021-5046-03 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.4.0. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5038-04

Red Hat Security Advisory 2021-5038-04 - Red Hat Advanced Cluster Management for Kubernetes 2.2.10 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console — with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which provide security fixes, bug fixes and container upgrades. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-5053-03

Red Hat Security Advisory 2021-5053-03 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-5030-01

Red Hat Security Advisory 2021-5030-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR7.

Red Hat Security Advisory 2021-5014-03

Red Hat Security Advisory 2021-5014-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.4.0 ESR. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Ubuntu Security Notice USN-5180-1

Ubuntu Security Notice 5180-1 - It was discovered that Mailman incorrectly handled CSRF tokens. A remote list member or moderator could possibly use their own token to craft an admin request CSRF attack and set a new admin password or make other changes.

Red Hat Security Advisory 2021-5017-03

Red Hat Security Advisory 2021-5017-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.4.0 ESR. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Red Hat Security Advisory 2021-5016-03

Red Hat Security Advisory 2021-5016-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.4.0 ESR. Issues addressed include buffer overflow, bypass, denial of service, and spoofing vulnerabilities.

Ubuntu Security Notice USN-5168-4

Ubuntu Security Notice 5168-4 - USN-5168-3 fixed a vulnerability in NSS. Unfortunately that update introduced a regression that could break SSL connections. This update fixes the problem. Tavis Ormandy discovered that NSS incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause

NSS to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-5006-04

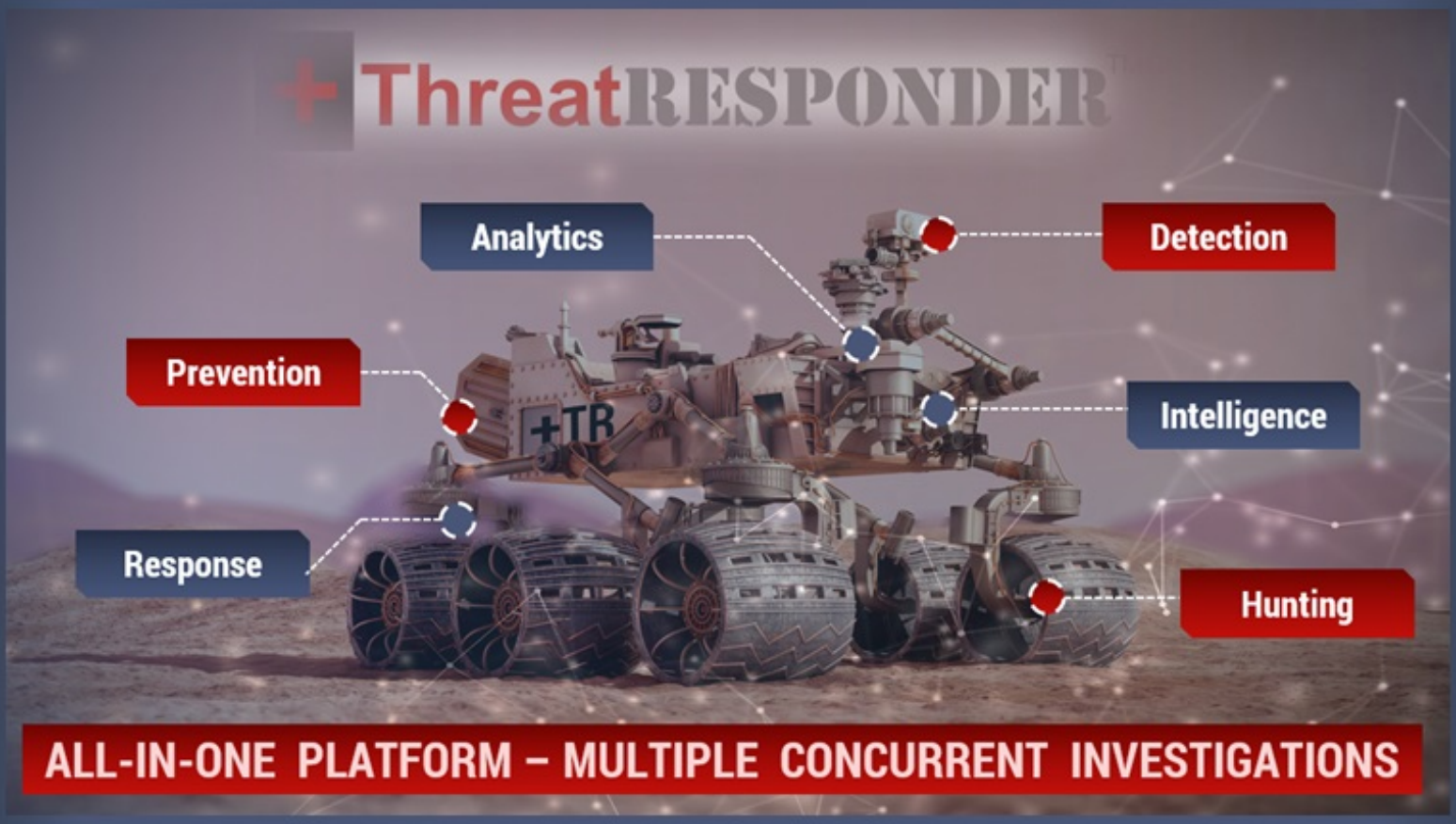
Red Hat Security Advisory 2021-5006-04 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks.

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



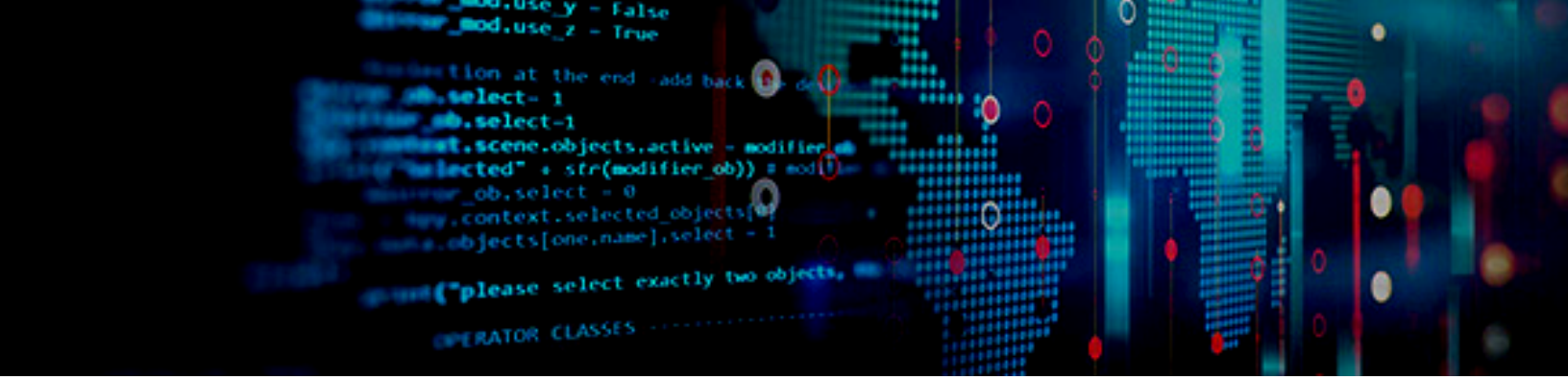
The Solution – ThreatResponder® Platform

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

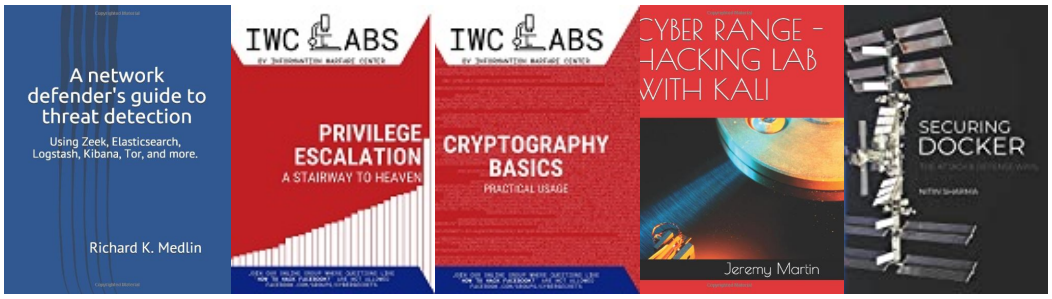


The Cyber Secrets publications on Amazon

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