Nov-29-21

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

November 29, 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

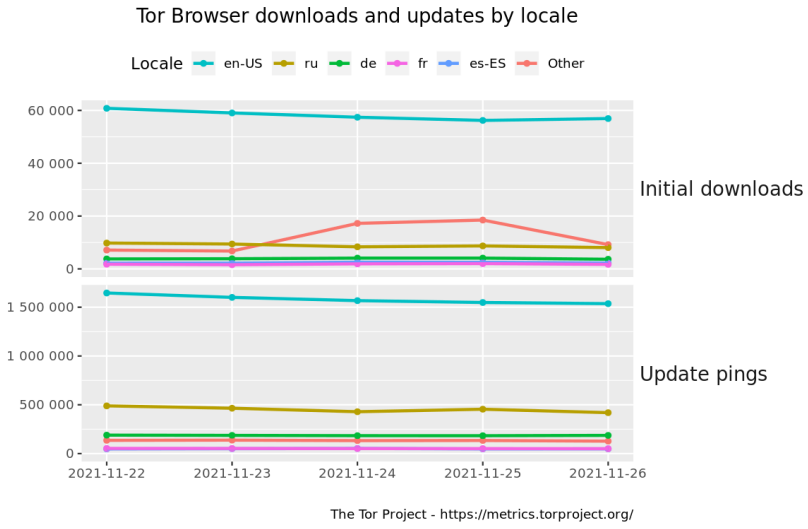
Internet Storm Center Infocon Status

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

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:
* Security Conferences
* Google Zero Day Project

Cyber Range Content
* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques
* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week
* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified
* CyberCrime-Tracker

Advisories
* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products
* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

Packet Storm Security

* Chinese Could Hack Data For Future Quantum Decryption, Report Warns
* What The SEC Requires From Businesses After A Data Breach
* Panasonic Confirms Data Breach After Hackers Access Internal Network
* 1,000 Arrests Made In Online Fraud Crackdown, Says Interpol
* This Stealthy Malware Hides Behind An Impossible Date
* Mr Goxx, The Cryptocurrency Trading Hamster, Dies
* Credentials Exposed For Majority Of US Financial Firms
* Google Warns Crypto Miners Are Hacking Cloud Accounts
* China Trying To Export Its Great Firewall And Governance Model
* Attackers Actively Target Windows Installer Zero-Day
* Cybercriminals Continue Using Zelle To Scam Victims
* Tolkien Estate Blocks JRR Token Crypto Currency
* Apple Sues 'Amoral 21st Century Mercenaries' NSO For Infecting iPhones With Pegasus Malware
* Analyzing A Watering Hole Campaign Using macOS Exploits
* Suspect Arrested In Ransom Your Employer Scheme
* FBI And CISA Issue Holiday Ransomware, Cyberattack Warning
* Code Execution Bug Patched In Imunify360 Linux Server Security Suite
* UK Ministry Of Justice Secures HVAC Systems After Register Tipoff
* NCSC Alerts Over 4,000 Retailers With Hackers Card Skimming Using Magento Flaw
* GoDaddy Security Breach Exposes WordPress Users' Data
* Locked Out Of God Mode, Runners Are Hacking Their Treadmills
* People Are Still Using Dumb Passwords In 2021
* Facebook And Instagram Encryption Plans Delayed
* Six Million Sky Routers Had Serious Security Flaw
* Facebook Demands LAPD End Social Media Surveillance

Krebs on Security

* 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
* REvil Ransom Arrest, $6M Seizure, and $10M Reward
* 'Tis the Season for the Wayward Package Phish
* The 'Groove' Ransomware Gang Was a Hoax

Dark Reading

* Paving the Road to Zero Trust With Adaptive Authentication
* NanoLock Security and Waterfall Security Partner to Deliver OT Security for Industrial and Energy App
* How Threat Actors Get Into OT Systems
* In Appreciation: Dark Reading's Tim Wilson
* MediaTek Chip Flaw Could Have Let Attackers Spy on Android Phones
* OpenText Acquires Bricata
* When Will Security Frameworks Catch Up With the New Cybersecurity Normal?
* Baffle's Data Privacy Cloud Protects Data for Amazon Redshift Customers
* New Android Spyware Variants Linked to Middle Eastern APT
* Why Should I Adopt a Zero-Trust Security Strategy?
* Apple Sues NSO Group for Spyware Use
* Holiday Scams Drive SMS Phishing Attacks
* How Sun Tzu's Wisdom Can Rewrite the Rules of Cybersecurity
* Don't Help Cybercriminals Dash With Your Customers' Cash This Black Friday
* Pentagon Partners With GreyNoise to Investigate Internet Scans
* GoDaddy Breach Exposes SSL Keys of Managed WordPress Hosting Customers
* CISA Urges Critical Infrastructure to Be Alert for Holiday Threats
* Bug Bounties Surge as Firms Compete for Talent
* 10 Stocking Stuffers for Security Geeks
* Is It OK to Take Your CEO Offline to Protect the Network?

The Hacker News

* 4 Android Banking Trojan Campaigns Targeted Over 300,000 Devices in 2021
* New Chinotto Spyware Targets North Korean Defectors, Human Rights Activists
* Hackers Using Compromised Google Cloud Accounts to Mine Cryptocurrency
* CleanMyMac X: Performance and Security Software for Macbook
* Interpol Arrests Over 1,000 Cyber Criminals From 20 Countries; Seizes $27 Million
* Italy's Antitrust Regulator Fines Google and Apple for "Aggressive" Data Practices
* Hackers Targeting Biomanufacturing Facilities With Tardigrade Malware
* Crypto Hackers Using Babadeda Crypter to Make Their Malware Undetectable
* CronRAT: A New Linux Malware That's Scheduled to Run on February 31st
* Israel Bans Sales of Hacking and Surveillance Tools to 65 Countries
* Product Releases Should Not Be Scary
* This New Stealthy JavaScript Loader Infecting Computers with Malware
* Hackers Using Microsoft MSHTML Flaw to Spy on Targeted PCs with Malware
* If You're Not Using Antivirus Software, You're Not Paying Attention
* Warning - Hackers Exploiting New Windows Installer Zero-Day Exploit in the Wild

Security Week

* Project Zero Flags High-Risk Zoom Security Flaw
* Marine Services Provider Swire Pacific Offshore Discloses Data Breach
* Panasonic Investigating Data Breach
* CISA Releases Guidance on Securing Enterprise Mobile Devices
* Armis Raises $300 Million at $3.4 Billion Valuation
* Recently Patched Apache HTTP Server Vulnerability Exploited in Attacks
* Ransomware Operators Threaten to Leak 1.5TB of Supernus Pharmaceuticals Data
* UK Cyber Firm Faces Investors Over Stock Turmoil
* VMware Patches File Read, SSRF Vulnerabilities in vCenter Server
* IoT Security Company Shield-IoT Raises $7.4 Million
* Two Nigerians Sentenced to Prison in U.S. for Role in BEC Scams
* 3 Key Questions for CISOs on the Wave of Historic Industrial Cybersecurity Legislation
* GoDaddy Says Several Brands Hit by Recent WordPress Hosting Breach
* CISA, FBI Warn of Potential Critical Infrastructure Attacks on Holidays
* Researcher Awarded $10,000 for Google Cloud Platform Vulnerability
* Industrial Cybersecurity Firm Applied Risk Acquired by DNV
* Japan, Vietnam Look to Cyber Defense Against China
* Apple Slaps Lawsuit on NSO Group Over Pegasus iOS Exploitation
* PoC Exploit Published for Latest Microsoft Exchange Zero-Day
* Preventing a Cyber Pandemic in Healthcare
* Serious Vulnerability Found in Imunify360 Web Server Security Product
* Low Code/No Code App Security Firm Zenity Emerges From Stealth
* Biomanufacturing Facilities Warned of Attacks Involving Sophisticated Malware
* Schwarz Group Acquires XM Cyber for $700 Million
* Cyber Insurance Firm Resilience Raises $80 Million

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Phishing Reported in IKEA's Internal Email System
* John Scimone, SVP and Chief Security Officer at Dell Technologies, says "security is everyone's job."
* FBI: Cyber Attacks Target Organizations Involved in Mergers and Acquisitions
* Email Classified as 'Malicious' by Employees Has Increased by 35% in the Last Year
* Phishing Attacks Impersonating Amazon Continue, Raising Concerns on the Cusp of Black Friday and the
* Planning on Relaxing During the Holiday? Think Again - Ransomware Attacks May Have You Working Over a
* Avoid Donating to Charity Scammers During Giving Tuesday 2021
* [Scam of the Week] Black Friday & Cyber Monday Cybersecurity Tips 2021
* [FREE Resource Kit] Stay Safe This Holiday Season with KnowBe4
* SEC Warns of Spoofed Emails Impersonating Their Employees

ISC2.org Blog

* How to Prepare for CISSP Exam Day
* The Best Way to Start Your Cloud Security Career
* Four Cybersecurity Tips Everyone Should Know Before Black Friday and Cyber Monday
* Insider Threats Can Turn Your Cloud Security Into a Storm
* The Importance of Security Control Baselines

HackRead

* Attackers exploiting Windows Installer vulnerability despite patching
* How To Secure Your Broadband?
* Remote access tools abused to spread malware and steal cryptocurrency
* Microsoft MSHTML flaw exploited in Gmail and Instagram phishing scam
* Swire Pacific Offshore Operations hit by Cl0p ransomware gang
* About 10 million Android devices found infected with Cynos malware
* WiFi software management firm exposed millions of users' data

Koddos

* Attackers exploiting Windows Installer vulnerability despite patching
* How To Secure Your Broadband?
* Remote access tools abused to spread malware and steal cryptocurrency
* Microsoft MSHTML flaw exploited in Gmail and Instagram phishing scam
* Swire Pacific Offshore Operations hit by Cl0p ransomware gang
* About 10 million Android devices found infected with Cynos malware
* WiFi software management firm exposed millions of users' data

Naked Security

* Cloud Security: Don't wait until your next bill to find out about an attack!
* S3 Ep60: Exchange exploit, GoDaddy breach and cookies made public [Podcast]
* US government securities watchdog spoofed by investment scammers - don't fall for it!
* Check your patches - public exploit now out for critical Exchange bug
* GoDaddy admits to password breach: check your Managed WordPress site!
* Black Friday and Cyber Monday - here's what you REALLY need to do!
* Github cookie leakage - thousands of Firefox cookie files uploaded by mistake
* S3 Ep59: Emotet, an FBI hoax, Samba bugs, and a hijackable suitcase [Podcast]
* Apple's Mail Privacy Protection feature - watch out if you have a Watch!
* The self-driving smart suitcase… that the person behind you can hijack!

Threat Post

* ScarCruft APT Mounts Desktop/Mobile Double-Pronged Spy Attacks
* Unpatched Windows Zero-Day Allows Privileged File Access
* Shape-Shifting 'Tardigrade' Malware Hits Vaccine Makers
* New Twists on Gift-Card Scams Flourish on Black Friday
* 9.3M+ Androids Running 'Malicious' Games from Huawei AppGallery
* GoDaddy Breach Widens to Include Reseller Subsidiaries
* Apple's NSO Group Lawsuit Amps Up Pressure on Pegasus Spyware-Maker
* Attackers Actively Target Windows Installer Zero-Day
* Attackers Will Flock to Crypto Wallets, Linux in 2022: Podcast
* How to Defend Against Mobile App Impersonation

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

* How the Rise in Cyberattacks Is Changing Consumer Behavior
* What the SEC Requires From Businesses After a Data Breach
* Hospital Ransomware Attacks Go Beyond Health Care Data
* IoT Security: Are Personal Devices Dragging Your Work Network Down?
* A Journey in Organizational Resilience: Insider Threats
* The Cost of a Data Breach Goes Beyond the Bottom Line
* Patch Management: Keep an Eye on App Software Updates
* How to Design IoT Security From the Ground Up
* Penetration Testing for Cloud-Based Apps: A Step-by-Step Guide
* Rising Cyber Insurance Premiums Highlight Importance of Ransomware Prevention

InfoWorld

* UNESCO launches global standard for AI ethics
* Inside the new AWS
* How the public clouds are innovating on AI
* Google Cloud AppSheet review: No-code with extras
* JDK 18: What to expect in Java 18
* Send Outlook email and Teams messages with R
* Take a look at Azure Monitor
* Windows Forms advances in .NET 6 but still needs work
* Build a cloud culture to attract and keep skilled people
* How CI/CD is different for data science

C4ISRNET - Media for the Intelligence Age Military

* Morocco buys Israeli counter-drone system Skylock Dome
* Army to work with satellite radar imagery provider ICEYE
* Defense Innovation Unit publishes ethical AI guidelines
* DoD identifies companies to bid on its new cloud effort
* New report sees near-term strength in space industrial base, but calls for government guidance
* EU nations add air, space and drone tech to their defense cooperation roster
* Israeli, Emirati companies partner up on unmanned surface vessels
* Counter-drone tech at Dubai Airshow reflects UAE's interest in the capability
* Air Force Research Laboratory awards university $1 billion for space technology research
* Edge Group's CEO talks drone swarms, 3D printing and export plans

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

* Windows Exploitation Tricks: Relaying DCOM Authentication
* Using Kerberos for Authentication Relay Attacks

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.

* Ledger Donjon CTF 2021
* Cyber Santa is Coming to Town
* m0leCon CTF 2021
* iCTF 2020
* ph0wn 2021
* 2021 Metasploit community CTF
* MetaCTF CyberGames 2021
* HITCON CTF 2021
* VULNCON CTF 2021
* OverTheWire Advent Bonanza 2021

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

* OpenStego Free Steganography Solution 0.8.2
* GNU Privacy Guard 2.2.33
* Wireshark Analyzer 3.6.0
* OpenStego Free Steganography Solution 0.8.1
* Hashcat Advanced Password Recovery 6.2.5 Source Code
* Hashcat Advanced Password Recovery 6.2.5 Binary Release
* Packet Fence 11.1.0
* Wireshark Analyzer 3.4.10
* Suricata IDPE 6.0.4
* SQLMAP - Automatic SQL Injection Tool 1.5.11

Kali Linux Tutorials

* Certipy : Python Implementation For Active Directory Certificate Abuse
* Tor-Rootkit : A Python 3 Standalone Windows 10 / Linux Rootkit Using Tor
* PyRDP : RDP Monster-In-The-Middle (Mitm) And Library For Python With The Ability To Watch Connections
* Androidqf : (Android Quick Forensics) Helps Quickly Gathering Forensic Evidence From Android Devices,
* How to Protect Small and Medium-Sized Businesses From Cyberattacks
* LDAPmonitor : Monitor Creation, Deletion And Changes To LDAP Objects Live During Your Pentest Or Syst
* TIWAP : Totally Insecure Web Application Project
* Cybersecurity Tips For Startups
* HandleKatz : PIC Lsass Dumper Using Cloned Handles
* aDLL : Adventure of Dynamic Link Library

GBHackers Analysis

* 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
* Hackers Exploit Microsoft Exchange Vulnerabilities To Drop Babuk Ransomware
* Unauthenticated RCE Flaw in Gitlab Exploited Widely by Hackers

Weekly Cyber Security Video and Podcasts

SANS DFIR

* 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
* Common misconceptions and mistakes made in Threat Hunting

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

* What parts should you use for a 3d printed drone
* Parse Wi-Fi Packets with Monitor Mode in CircuitPython | HakByte
* Designing & Building Your Own 3D Printed Drone - Introduction

The PC Security Channel [TPSC]

* Windows 11 vs Ransomware
* Vice Society Ransomware & Print Nightmare

Eli the Computer Guy

* COVID FAIL - COUNTRIES CLOSE BORDERS over OMICRON variant (japan, israel, morocco)
* BIDEN FAIL - RACIST TRAVEL BAN ON SOUTH AFRICA for COVID VARIANT OMICRON
* BUILD BACK BETTER FAIL - TREE EQUITY
* LETS GO BRANDON - UNEMPLOYMENT LOWEST SINCE 1969

Security Now

* HTTP Request Smuggling - NetGear Routers 0-Day, The Most Brute Forced Passwords, GoDaddy Breach
* Blacksmith - Patch Tuesday's 55 Flaws, The Zen of Code, Ryuk Ransomware Gang

Troy Hunt

* Weekly Update 271

Intel Techniques: The Privacy, Security, & OSINT Show

* 241-Listener Questions
* Announcement: Listener Questions Show

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Orangescrum 1.8.0 Privilege Escalation
* Orangescrum 1.8.0 SQL Injection
* Orangescrum 1.8.0 Cross Site Scripting
* Opencart 3.0.3.8 Session Injection
* Apache HTTP Server 2.4.50 CVE-2021-42013 Exploitation
* Polkit Authentication Bypass / Local Privilege Escalation
* Nextar C472 POS DLL Hijacking
* ManageEngine ADSelfService Plus Authentication Bypass / Code Execution
* D-Link DSL-3782 Pre-Authentication Remote Root
* Backdoor.Win32.Coredoor.10.a Man-In-The-Middle
* Email-Worm.Win32.Deltad Insecure Permissions
* Backdoor.Win32.Coredoor.10.a Authentication Bypass / Code Execution
* Bagisto 1.3.3 Client-Side Template Injection
* Gerdab.ir SQL Injection
* Apple ColorSync CMMNDimLinear::Interpolate Uninitialized Memory
* HTTPDebuggerPro 9.11 Unquoted Service Path
* CMSimple 5.4 Local File Inclusion / Remote Code Execution
* Serva 4.4.0 TFTP Remote Buffer Overflow
* WordPress WP Guppy 1.1 Information Disclosure
* Linux Kernel 5.1.x PTRACE_TRACEME pkexec Local Privilege Escalation
* Webrun 3.6.0.42 SQL Injection
* FLEX 1085 Web 1.6.0 HTML Injection
* GNU gdbserver 9.2 Remote Command Execution
* Samsung NPU (Neural Processing Unit) Memory Corruption
* Wipro Holmes Orchestrator 20.4.1 Report Disclosure

CXSecurity

* D-Link DSL-3782 Pre-Authentication Remote Root
* CMSimple 5.4 Local File Inclusion / Remote Code Execution
* Apache HTTP Server 2.4.50 Remote Code Execution Py ver
* GNU gdbserver 9.2 Remote Command Execution
* Apache Storm Nimbus 2.2.0 Command Execution
* Pinkie 2.15 Remote Buffer Overflow
* Modbus Slave 7.3.1 Buffer Overflow

Proof of Concept (PoC) & Exploits

Exploit Database

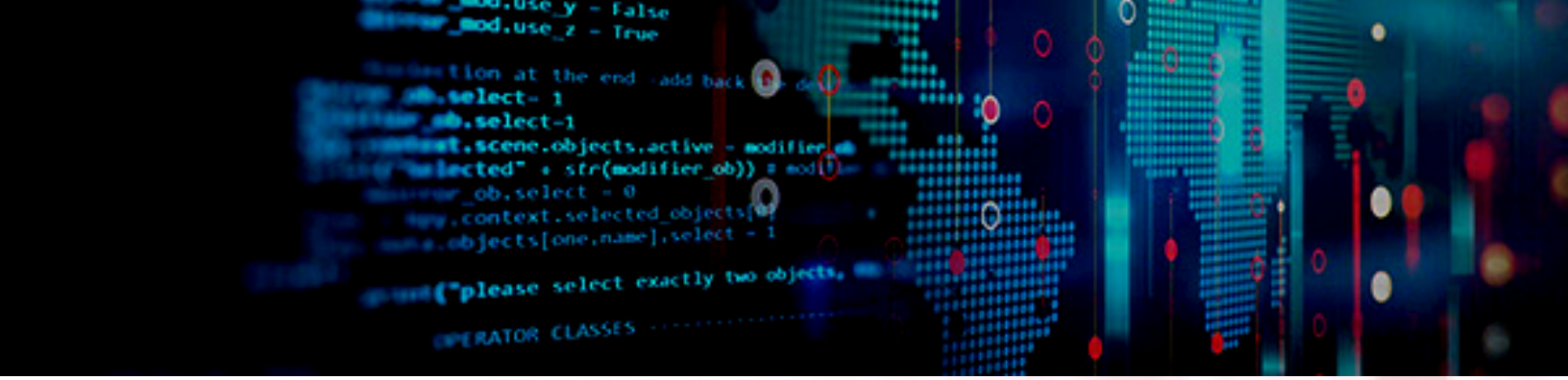
* [webapps] opencart 3.0.3.8 - Sessjion Injection
* [webapps] orangescrum 1.8.0 - 'Multiple' Cross-Site Scripting (XSS) (Authenticated)
* [webapps] orangescrum 1.8.0 - 'Multiple' SQL Injection (Authenticated)
* [webapps] orangescrum 1.8.0 - Privilege escalation (Authenticated)
* [webapps] Bagisto 1.3.3 - Client-Side Template Injection
* [webapps] CMSimple 5.4 - Local file inclusion (LFI) to Remote code execution (RCE) (Authenticated)
* [local] HTTPDebuggerPro 9.11 - Unquoted Service Path
* [webapps] FLEX 1085 Web 1.6.0 - HTML Injection
* [webapps] Bus Pass Management System 1.0 - 'Search' SQL injection
* [webapps] Webrun 3.6.0.42 - 'P_0' SQL Injection
* [local] Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2)
* [webapps] Wordpress Plugin WP Guppy 1.1 - WP-JSON API Sensitive Information Disclosure
* [remote] GNU gdbserver 9.2 - Remote Command Execution (RCE)
* [webapps] Aimeos Laravel ecommerce platform 2021.10 LTS - 'sort' SQL injection
* [dos] Modbus Slave 7.3.1 - Buffer Overflow (DoS)
* [dos] Pinkie 2.15 - TFTP Remote Buffer Overflow (PoC)
* [webapps] Wordpress Plugin Smart Product Review 1.0.4 - Arbitrary File Upload
* [webapps] GitLab 13.10.2 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] SuiteCRM 7.11.18 - Remote Code Execution (RCE) (Authenticated) (Metasploit)
* [webapps] Quick.CMS 6.7 - Cross Site Request Forgery (CSRF) to Cross Site Scripting (XSS) (Authentica
* [webapps] Bludit 3.13.1 - 'username' Cross Site Scripting (XSS)
* [webapps] CMDBuild 3.3.2 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Online Learning System 2.0 - Remote Code Execution (RCE)
* [webapps] PHP Laravel 8.70.1 - Cross Site Scripting (XSS) to Cross Site Request Forgery (CSRF)
* [webapps] WordPress Plugin Contact Form to Email 1.3.24 - Stored Cross Site Scripting (XSS) (Authenti

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*

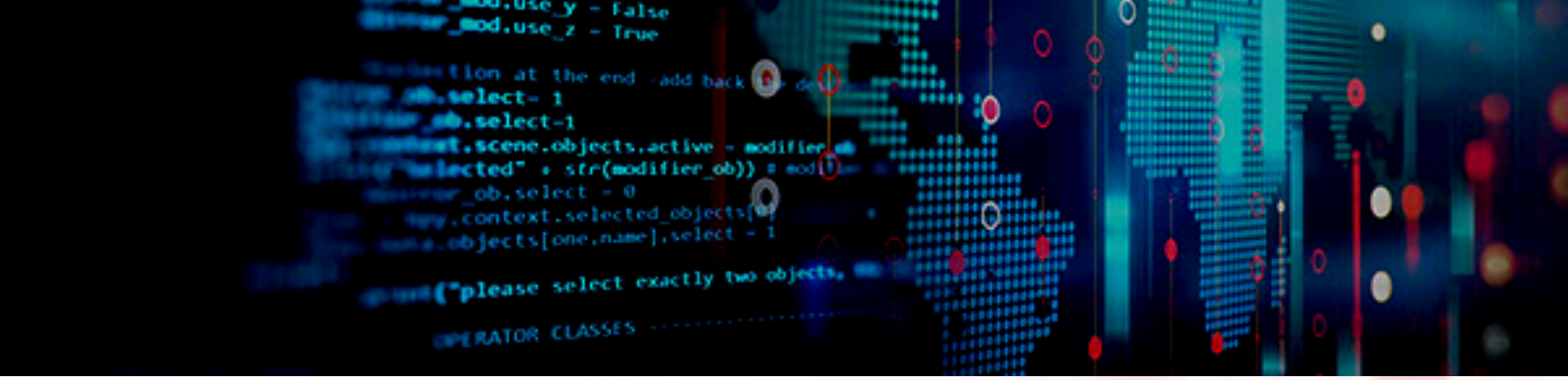
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://gadsigsipamba.gob.ec/dz.txt
https://gadsigsipamba.gob.ec/dz.txt notified by Admeral zino_dz
https://registropropiedadymercantilhuaca.gob.ec/dz.txt
https://registropropiedadymercantilhuaca.gob.ec/dz.txt notified by Admeral zino_dz
http://www.ccpdantonioante.gob.ec/dz.txt
http://www.ccpdantonioante.gob.ec/dz.txt notified by Admeral zino_dz
https://juntaparroquialaltotambo.gob.ec/dz.txt
https://juntaparroquialaltotambo.gob.ec/dz.txt notified by Admeral zino_dz
https://gadimbaya.gob.ec/dz.txt
https://gadimbaya.gob.ec/dz.txt notified by Admeral zino_dz
http://inifapcirpac.gob.mx
http://inifapcirpac.gob.mx notified by SLNTAR
http://coacoatzintla.gob.mx/b4.html
http://coacoatzintla.gob.mx/b4.html notified by 0x1998
https://tresvalles.gob.mx/b4.html
https://tresvalles.gob.mx/b4.html notified by 0x1998
https://www.pa-maros.go.id/dim.txt
https://www.pa-maros.go.id/dim.txt notified by Kurdistan FUCKTARD
http://www.camaradoisirmaosdoburiti.ms.gov.br
http://www.camaradoisirmaosdoburiti.ms.gov.br notified by Paraná Cyber Mafia
http://jatei.ms.gov.br
http://jatei.ms.gov.br notified by Paraná Cyber Mafia
http://noticiaspoliciales.gob.ar
http://noticiaspoliciales.gob.ar notified by aDriv4
https://bappeda-litbang.enrekangkab.go.id/wh.html
https://bappeda-litbang.enrekangkab.go.id/wh.html notified by Mr.Kro0oz.305
https://www.pustaka.pn-sukoharjo.go.id
https://www.pustaka.pn-sukoharjo.go.id notified by TangerangXploit Team
https://paranapua.sp.gov.br
https://paranapua.sp.gov.br notified by Paraná Cyber Mafia
http://insopesca.gob.ve
http://insopesca.gob.ve notified by 0x1998
http://donggala.go.id/b4.html
http://donggala.go.id/b4.html notified by 0x1998



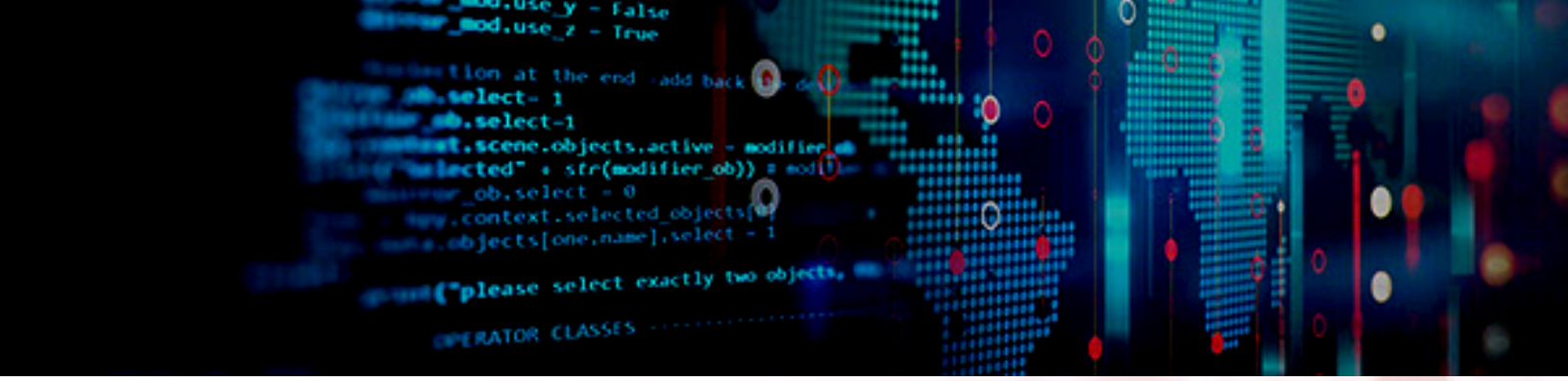
Dark Web News

Darknet Live

Parallel Construction: The DEA Once "Stole" a Dealer's Car
This is an old tale of how the U.S. Drug Enforcement Administration used parallel construction to arrest a drug trafficker after secretly intercepting his phone calls. (via darknetlive.com)
Trio Admits Selling Psychedelics on the Darkweb
Three defendants admitted selling psychedelic mushroom analogues through the "TripWithScience” account on the darkweb. (via darknetlive.com)
Police Found 145 Sales Records on a Vendor's USB Drive
The Public Prosecution Service in the Netherlands demanded a prison sentence of eight years for a large-scale darkweb vendor. (via darknetlive.com)
Three Germans Arrested for Selling Drugs on the Darkweb
Authorities in Germany arrested a trio for allegedly distributing drugs through darkweb marketplaces. (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

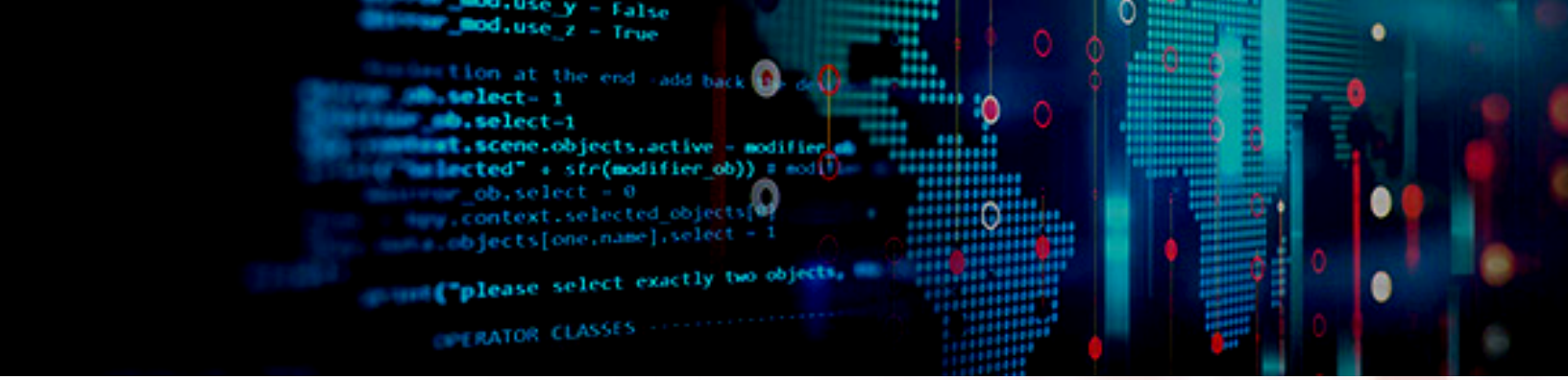
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing 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

* 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
* "Bom" Skimmer is Magecart Group 7's Latest Model
* Untangling the Spider Web

FireEye

* Metasploit Wrap-Up
* [Security Nation] Chris John Riley on Minimum Viable Secure Product (MVSP)
* OWASP Top 10 Deep Dive: Defending Against Server-Side Request Forgery
* The End of the Cybersecurity Skills Crisis (Maybe?)
* Metasploit Wrap-Up
* 2022 Planning: A First-Year CISO Shares Her Point of View
* Make Room for Cloud Security in Your 2022 Budget
* Distribute Reports to Email Addresses in InsightVM
* 2022 Planning: Prioritizing Defense and Mitigation Through Left of Boom
* Announcing the 2021 Metasploit Community CTF



Advisories

US-Cert Alerts & bulletins

* CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Or
* VMware Releases Security Updates
* Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends
* Updated: APT Exploitation of ManageEngine ADSelfService Plus Vulnerability
* NSA and CISA Release Guidance on Securing 5G Cloud Infrastructures
* Drupal Releases Security Updates
* NCSC Releases 2021 Annual Review
* CISA Adds Four Known Exploited Vulnerabilities to Catalog
* AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet V
* AA21-291A: BlackMatter Ransomware
* Vulnerability Summary for the Week of November 22, 2021
* Vulnerability Summary for the Week of November 15, 2021

Zero Day Initiative Advisories

ZDI-CAN-14650: Delta Industrial Automation
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-14479: Delta Industrial Automation
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-14653: Delta Industrial Automation
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-14651: Delta Industrial Automation
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-14480: Delta Industrial Automation
A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was

reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-14654: Delta Industrial Automation

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 5 days ago. The vendor is given until 2022-03-24 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-16045: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16046: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16044: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16043: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16042: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15689: Autodesk

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16041: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15687: Autodesk

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15677: Autodesk

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16040: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16015: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15697: NIKON

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16047: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15154: Altair

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16048: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15741: Linux

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Ryota Shiga(@Ga_ryo_) of Flatt Security' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14481: Delta Industrial Automation

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: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15179: Rockwell Automation

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-19, 10 days ago. The vendor is given until 2022-03-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-4844-01

Red Hat Security Advisory 2021-4844-01 - 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 2021-4843-01

Red Hat Security Advisory 2021-4843-01 - 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 2021-4833-01

Red Hat Security Advisory 2021-4833-01 - 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 4.9.9. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-5156-1

Ubuntu Security Notice 5156-1 - It was discovered that ICU contains a double free issue. An attacker could use this issue to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2021-4837-02

Red Hat Security Advisory 2021-4837-02 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4838-02

Red Hat Security Advisory 2021-4838-02 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4839-02

Red Hat Security Advisory 2021-4839-02 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4826-02

Red Hat Security Advisory 2021-4826-02 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4774-02

Red Hat Security Advisory 2021-4774-02 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-4788-02

Red Hat Security Advisory 2021-4788-02 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2021-4798-02

Red Hat Security Advisory 2021-4798-02 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-4773-03

Red Hat Security Advisory 2021-4773-03 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-5155-1

Ubuntu Security Notice 5155-1 - It was discovered that BlueZ incorrectly handled the Discoverable status when a device is powered down. This could result in devices being powered up discoverable, contrary to expectations. This issue only affected Ubuntu 20.04 LTS, Ubuntu 21.04, and Ubuntu 21.10. It was discovered

that BlueZ incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause BlueZ to consume resources, leading to a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-4782-01

Red Hat Security Advisory 2021-4782-01 - OpenSSH is an SSH protocol implementation supported by a number of Linux, UNIX, and similar operating systems. It includes the core files necessary for both the OpenSSH client and server. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2021-4785-01

Red Hat Security Advisory 2021-4785-01 - The RPM Package Manager is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-4777-01

Red Hat Security Advisory 2021-4777-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-4779-01

Red Hat Security Advisory 2021-4779-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-5154-1

Ubuntu Security Notice 5154-1 - It was discovered that FreeRDP incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash. It was discovered that FreeRDP incorrectly handled certain connections. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

Red Hat Security Advisory 2021-4765-03

Red Hat Security Advisory 2021-4765-03 - Red Hat OpenShift Serverless Client kn 1.19.0 provides a CLI to interact with Red Hat OpenShift Serverless 1.19.0. The kn CLI is delivered as an RPM package for installation on RHEL platforms, and as binaries for non-Linux platforms.

Red Hat Security Advisory 2021-4766-01

Red Hat Security Advisory 2021-4766-01 - Red Hat OpenShift Serverless release of the OpenShift Serverless Operator. This version of the OpenShift Serverless Operator is supported on Red Hat OpenShift Container Platform versions 4.6, 4.7, 4.8 and 4.9, and includes security and bug fixes and enhancements. For more information, see the documentation listed in the References section.

Red Hat Security Advisory 2021-4767-01

Red Hat Security Advisory 2021-4767-01 - This release of Red Hat Integration - Camel Extensions for Quarkus - 2.2 GA serves as a replacement for tech-preview 2, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include bypass, code execution, denial of service, deserialization, information leakage, resource exhaustion, and server-side request forgery vulnerabilities.

Red Hat Security Advisory 2021-4768-01

Red Hat Security Advisory 2021-4768-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-4771-01

Red Hat Security Advisory 2021-4771-01 - The RPM Package Manager is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2012-4770-01

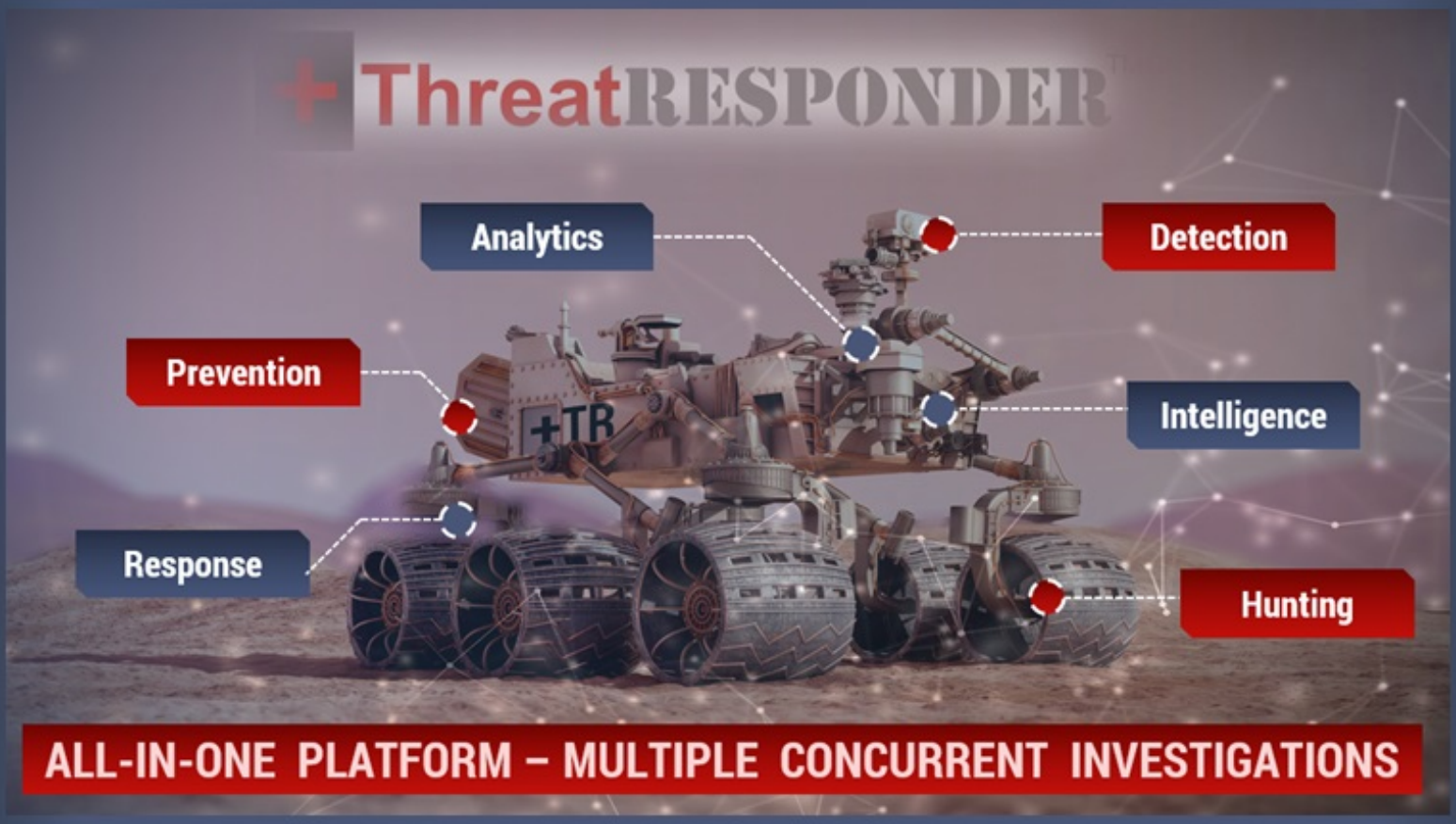
Red Hat Security Advisory 2012-4770-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

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



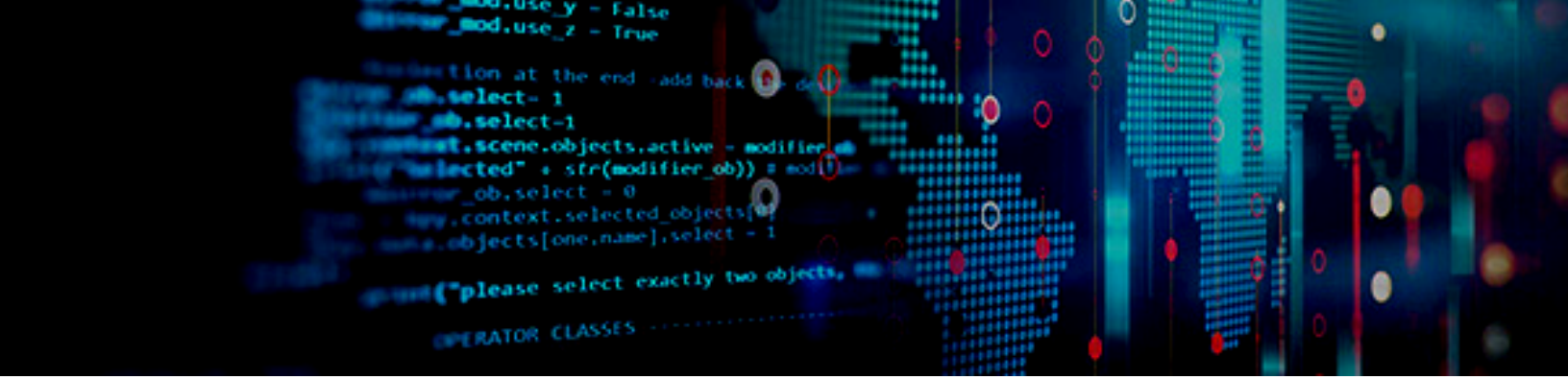
The Solution – ThreatResponder® Platform

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

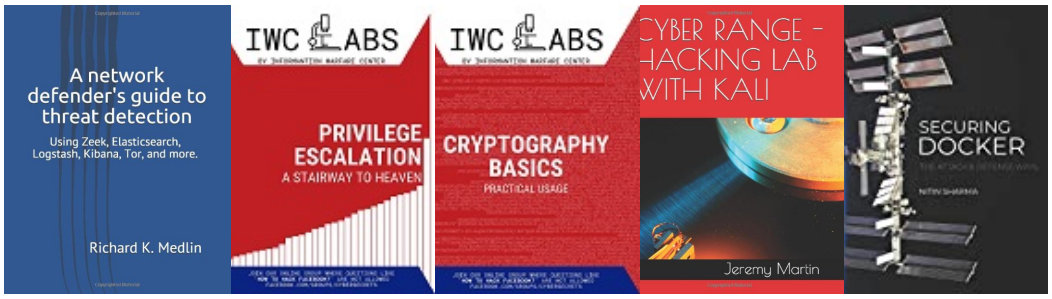


The Cyber Secrets publications on Amazon

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