Nov-15-21

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 15, 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

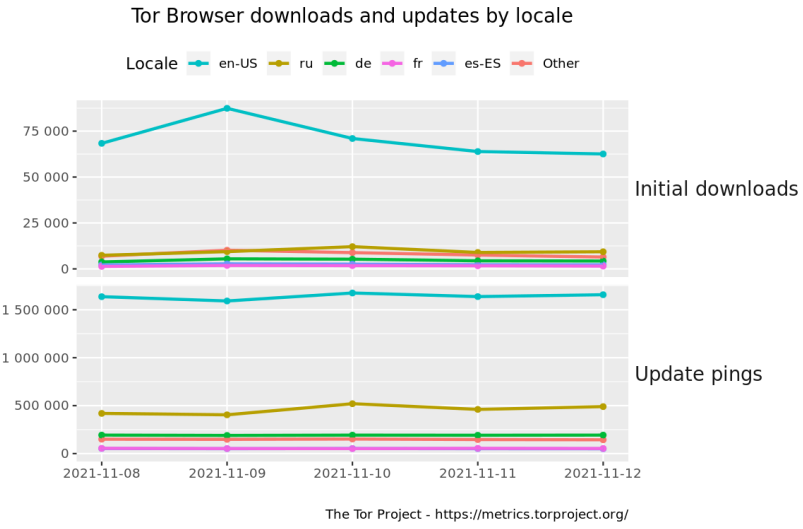
Internet Storm Center Infocon Status

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

* Subscribe to this OSINT resource to recieve it in in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

* The newest issue in the Cyber Secrets series (#6) - Incident Response: Evidence Preservation and Collection is now availible on Amazon!! This issue Incident Responce and Threat Hunting topics. Great for any security team.

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

Index of Sections

Packet Storm Security

* Back-To-Back PlayStation 5 Hacks Hit On The Same Day
* Analyzing A Watering Hole Campaign Using macOS Exploits
* Booking.com Was Reportedly Hacked By A US Intel Agency But Never Told Customers
* Alan Paller, Founder Of The SANS Institute, Passes Away At 76
* Tiny Font Size Fools Email Filters In BEC Phishing
* USA Finally Signs Paris Call For Trust And Security In Cyberspace
* Massive Zero-Day Hole Found In Palo Alto Security Appliances
* Critical Citrix DDoS Bug Shuts Down Network, Cloud App Access
* Ransomware Attack Delays Comic Book Distributor Shipments
* Fresh Scrutiny For Mexico After Arrest Of Suspect In NSO Spyware Case
* New Android Spyware Poses Pegasus-Like Threat
* Microsoft November Patch Tuesday Fixes Six Zero-Days, 55 Bugs
* Hack Leaves Fertility Clinic Medical Data At Risk
* Hacking Group Claims It Found Encryption Keys Needed To Unlock PS5
* Here's What A COD Vanguard Account Boosting Farm Looks Like
* Robinhood Trading Platform Data Breach Hits 7 Million Customers
* US Charges Ukrainian And Russian Nationals Over Ransomware Attacks
* Zoho Password Manager Flaw Torched By Godzilla Webshell
* Forecast: Cloudy With A Chance Of 404
* Hostage-Style Bitcoin Scam Videos Spread On Instagram
* Palestinian Activists' Mobile Phones Hacked Using NSO Spyware
* Fishing Gear Seller Caught In Hacker's Net
* Suspect REvil Ransomware Affiliates Arrested
* Apple's Federighi Delivers Dramatic Speech On Dangers Of Sideloading
* Beijing Fingers Foreign Spies For Data Mischief

Krebs on Security

* 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
* 'Trojan Source' Bug Threatens the Security of All Code
* Zales.com Leaked Customer Data, Just Like Sister Firms Jared, Kay Jewelers Did in 2018
* FBI Raids Chinese Point-of-Sale Giant PAX Technology
* Conti Ransom Gang Starts Selling Access to Victims

Dark Reading

* MSPAlliance Leadership Council Forms Vendor Council to Address Managed Services Supply Chain Risk
* BT to Deploy 'Epidemiological AI' Based on the Spread of Viruses in Humans to Combat Cyberattacks
* Ankura Launches Brooklyn Cyber Center
* Emerging Security Tools Tackle GraphQL Security
* Open Source Project Aims to Detect Living-Off-the-Land Attacks
* Follow the Leaders: A Blueprint for Software Security Success
* How to Hire - and Retain - Effective Threat Hunters
* In Appreciation: Alan Paller
* 'Lyceum' Threat Group Broadens Focus to ISPs
* Google Open Sources ClusterFuzzLite
* How Do I Know It's Time to Consider a SASE Migration?
* What Happens If Time Gets Hacked
* Cloud Attack Analysis Unearths Lessons for Security Pros
* Third-Party Software Risks Grow, but So Do Solutions
* Insider IP Theft Is Surging - and Most Can't Stop It
* Should Our Security Controls Be More Like North Korea or Norway?
* New Application Security Toolkit Uncovers Dependency Confusion Attacks
* Hacker-for-Hire Group Spied on More Than 3,500 Targets in 18 Months
* ChaosDB: Researchers Share Technical Details of Azure Flaw
* Firms Will Struggle to Secure Extended Attack Surface in 2022

The Hacker News

* North Korean Hackers Target Cybersecurity Researchers with Trojanized IDA Pro
* How to Tackle SaaS Security Misconfigurations
* FBI's Email System Hacked to Send Out Fake Cyber Security Alert to Thousands
* Hackers Increasingly Using HTML Smuggling in Malware and Phishing Attacks
* Abcbot - A New Evolving Wormable Botnet Malware Targeting Linux
* Hackers Exploit macOS Zero-Day to Hack Hong Kong Users with new Implant
* Researchers Uncover Hacker-for-Hire Group That's Active Since 2015
* TrickBot Operators Partner with Shathak Attackers for Conti Ransomware
* Navigating The Threat Landscape 2021 - From Ransomware to Botnets
* Iran's Lyceum Hackers Target Telecoms, ISPs in Israel, Saudi Arabia, and Africa
* Palo Alto Warns of Zero-Day Bug in Firewalls Using GlobalProtect Portal VPN
* Researchers Discover PhoneSpy Malware Spying on South Korean Citizens
* 13 New Flaws in Siemens Nucleus TCP/IP Stack Impact Safety-Critical Equipment
* 14 New Security Flaws Found in BusyBox Linux Utility for Embedded Devices
* Microsoft Issues Patches for Actively Exploited Excel, Exchange Server 0-Day Bugs

Security Week

* IoT Protocol Used by NASA, Siemens and Volkswagen Can Be Exploited by Hackers
* Network Security Company Netography Raises $45 Million
* Four Things Your CISO Wants Your Board to Know
* Fake Emails Sent From FBI Address via Compromised Law Enforcement Portal
* Intel, AMD Patch High Severity Security Flaws
* 'BotenaGo' Malware Targets Routers, IoT Devices with Over 30 Exploits
* Zoom Patches High-Risk Flaws in Meeting Connector, Keybase Client
* Researcher Shows Windows Flaw More Serious After Microsoft Releases Incomplete Patch
* HPE Says Customer Data Compromised in Aruba Data Breach
* Google, Adobe Announce New Open Source Security Tools
* macOS Zero-Day Exploited to Deliver Malware to Users in Hong Kong
* Indonesia, UK Discuss Future Technology and Cybersecurity
* Enlisting Employees to Fight Cyber Threats
* The Wild West of the Nascent Cyber Insurance Industry
* U.S. Gov Announces Support for 'Paris Call' Cybersecurity Effort
* Nearly 100 TCP/IP Stack Vulnerabilities Found During 18-Month Research Project
* Contrast Security Raises $150 Million at 'Unicorn' Valuation
* Remote Code Execution Flaw in Palo Alto GlobalProtect VPN
* VMware Working on Patches for Serious vCenter Server Vulnerability
* Critical Flaw in WordPress Plugin Leads to Database Wipe
* South Korean Users Targeted with Android Spyware 'PhoneSpy'
* RPC Firewall Dubbed 'Ransomware Kill Switch' Released to Open Source
* Citrix Patches Critical Vulnerability in ADC, Gateway
* ICS, OT Cybersecurity Incidents Cost Some U.S. Firms Over $100 Million: Survey
* Socure Raises $450 Million at $4.5 Billion Valuation

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* One-Fifth of U.K. Residents Have Experienced a 'Proof of Vaccination' Attack
* "Customer Complaint" May Get Your Attention
* Will Ransomware Extortion Tactics Ever Stop Evolving?
* Use of Ransomware Data Leak Sites Begin to Slow Down?
* Bait Attacks as Reconnaissance
* Phishing Attacks Aimed at Social Accounts Now in the Top Three Targeted Sectors
* Business Email Compromise-as-a-Service Emerges as Attempted Fraud Soars to as High as $6 Million
* The TodayZoo Phishing Kit Has All the Obfuscation and Impersonation Needed to Fool Your Users
* Median Ransomware Payment Jumps 50% as Mid-Market Becomes More Targeted
* CyberheistNews Vol 11 #44 [Heads Up] Multi-Stage Vishing Attacks Are Coming to an Inbox Near You

ISC2.org Blog

* Rookies Needed - Experience Required
* CCSP vs. Symantec Certified Cloud Credentials: How Do They Compare?
* (ISC)² Security Congress Goes West - Las Vegas Here We Come!
* The Dawn of True IoT Security
* (ISC)² Cybersecurity Entry-Level Certification Exam Topics Announced

HackRead

* How big data analytics helps enterprises improve cybersecurity
* 3D Printing and Engineering; an Overview
* BotenaGo botnet malware targeting millions of IoT devices
* How to Securely Access Remote Desktop?
* Critical WordPress plugin vulnerability allowed wiping databases
* Watch out as new PhoneSpy spyware hits Android devices
* How Artificial intelligence (AI) Stops Cybercriminals

Koddos

* How big data analytics helps enterprises improve cybersecurity
* 3D Printing and Engineering; an Overview
* BotenaGo botnet malware targeting millions of IoT devices
* How to Securely Access Remote Desktop?
* Critical WordPress plugin vulnerability allowed wiping databases
* Watch out as new PhoneSpy spyware hits Android devices
* How Artificial intelligence (AI) Stops Cybercriminals

Naked Security

* DHS warning about hackers in your network? Don't panic!
* Samba update patches plaintext password plundering problem
* S3 Ep58: Faces on Facebook, scams that pose as complaints, and a Kaseya bust [Podcast]
* Patch Tuesday updates the Win 7 updater… for at most 1 more year of updates
* Sophos 2022 Threat Report: Malware, Mobile, Machine learning and more!
* Kaseya ransomware suspect nabbed in Poland, $6m seized from absent colleague
* "Customer complaint" email scam preys on your fear of getting into trouble at work
* S3 Ep57: Europol v. Ransomware, Shrootless bug, and Linux browser flamewars [Podcast]
* Facebook to throw out face recognition, delete all template data
* Europol announces "targeting" of 12 suspects in ransomware attacks

Threat Post

* Threat from Organized Cybercrime Syndicates Is Rising
* Costco Confirms: A Data Skimmer's Been Ripping Off Customers
* Top 10 Cybersecurity Best Practices to Combat Ransomware
* Windows 10 Privilege-Escalation Zero-Day Gets an Unofficial Fix
* Mac Zero Day Targets Apple Devices in Hong Kong
* Millions of Routers, IoT Devices at Risk from New Open-Source Malware
* Invest in These 3 Key Security Technologies to Fight Ransomware
* Back-to-Back PlayStation 5 Hacks Hit on the Same Day
* Cyber-Mercenary Group Void Balaur Attacks High-Profile Targets for Cash
* Congress Mulls Ban on Big Ransom Payouts Unless Victims Get Official Say-So

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 Attackers Exploit the Remote Desktop Protocol
* SASE and Zero Trust: What's the Connection?
* Non-Traditional Cybersecurity Career Paths: How to Find Your Own Way
* Roundup: Government Data Security Threats in 2021
* Breach and Attack Simulation: Hack Yourself to a More Secure Future
* Designing a BYOD Approach for the Future
* A New Cybersecurity Executive Order Puts the Heat on Critical Infrastructure Suppliers
* A Journey in Organizational Resilience: Supply Chain and Third Parties
* Zero Trust: What NIST's Guidelines Mean for Your Resources
* How to Deal With Unpatched Software Vulnerabilities Right Now

InfoWorld

* Elastic keeps ticking
* 3 reasons devops must integrate agile and ITSM tools
* Why AI investments fail to deliver
* Deno improves JSX transform, WebAssembly support
* Visual Studio Code 1.62 brings workbench enhancements
* Abstracting public clouds down to common services
* Ruby tees up new JIT compiler
* How to resolve dependencies in ASP.NET Core
* Svelte creator: Web development should be more fun
* Microsoft's C# 10 promises 'prettier' code

C4ISRNET - Media for the Intelligence Age Military

* Emirati conglomerate unveils two drones and a weapons system
* The Army is looking for industry to help shape its future SATCOM needs
* IAI unveils Scorpius electronic warfare system for multi-threat confrontations
* Pentagon wants industry's help to bolster allies and partners' cybersecurity
* Soldiers won't always be able to rely on contractors for coders, says Army Software Factory director
* Cyber Marines could be empowered to act boldly under commandant's future force vision
* The cyber battlefield against China and Russia is constantly shifting. Here's how the NSA is trying t
* Pentagon 'zero trust' cyber office coming in December
* US Cyber Command publishes concept for integrating new capabilities
* At second Project Convergence, US Army experiments with joint operations in the Arizona desert

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.

* MetaRed International CTF 2021 - 4th STAGE
* HTB Uni CTF 2021 - Quals
* Hackfest CTF 13th Edition - Competitive
* Hackfest CTF 13th Edition - Casual
* N1CTF 2021
* Square CTF 2021
* Balsn CTF 2021
* CTF Russian Cup 2021
* LLM CTF
* Damncon 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

* GNUnet P2P Framework 0.15.3
* Faraday 3.18.1
* Clam AntiVirus Toolkit 0.104.1
* GRAudit Grep Auditing Tool 3.2
* TOR Virtual Network Tunneling Tool 0.4.6.8
* Zeek 4.1.1
* GNU Privacy Guard 2.3.3
* GNU Privacy Guard 2.2.32
* Faraday 3.18.0
* AntiRansom 5

Kali Linux Tutorials

* DonPAPI : Dumping DPAPI Credz Remotely
* Clash : A Rule-Based Tunnel In Go
* Keeweb : Free Cross-Platform Password Manager Compatible With KeePass
* Lorsrf : SSRF Parameter Bruteforce
* Mediator : An Extensible, End-To-End Encrypted Reverse Shell With A Novel Approach To Its Architectur
* VECTR : A Tool That Facilitates Tracking Of Your Red And Blue Team Testing Activities To Measure Dete
* Cloudflare CDN: What Is It and How Can You Benefit from It?
* Webdiscover : The Purpose Of This Script Is To Automate The Web Enumeration Process And Search For Ex
* SysFlow : Cloud-native System Telemetry Pipeline
* ThreadStackSpoofer : PoC For An Advanced In-Memory Evasion Technique

GBHackers Analysis

* 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
* Two European Men Sentenced for Providing 'Bulletproof Hosting' to Hackers
* Iranian Hackers Attack the US & Israeli Defense Technology - Microsoft Warns

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Fundamentos de Lógicas de Detección Basadas en Data
* Full Circle Detection: From Hunting to Actionable Detection
* Hunting Malicious Office Macros
* Mining The Shadows with ZoidbergStrike: A Scanner for Cobalt Strike

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

* CircuitPython Setup On The ESP32s2 | HakByte
* Facebook to Delete Facial Recognition Records for 1 Billion Users - ThreatWire
* Free CAD Programs for Makers and Hackers w/ Glytch

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* COVID BOOSTER REQUIRED in FRANCE
* SPIDER-MAN SHOULD BE GAY- or you're a homophobe
* COVID SURGE in States with HIGH VACCINATION RATES
* INSANE CALIFORNIA CRIME - Car Window Glass SHORTAGE

Security Now

* Bluetooth Fingerprinting - Pwn2Own Austin, Unpatched GitLab Servers, Cisco's DEFAULT SSH Key
* "Trojan Source” - Chrome 0-days, Windows 11 confusion, VoIP DDos attacks, Dune

Troy Hunt

* Weekly Update 269

Intel Techniques: The Privacy, Security, & OSINT Show

* Announcement: Listener Questions Show
* 240-Privacy, Security, & OSINT Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Aerohive NetConfig 10.0r8a Local File Inclusion / Remote Code Execution
* WordPress AccessPress Social Icons 1.8.2 Cross Site Scripting
* Xlight FTP 3.9.3.1 Buffer Overflow
* WordPress WP Symposium Pro 2021.10 Cross Site Scripting
* Microsoft Windows MultiPoint Server 2011 SP1 Local Privilege Escalation
* Mumara Classic 2.93 SQL Injection
* Microsoft Windows WSAQuerySocketSecurity AppContainer Privilege Escalation
* Apache HTTP Server 2.4.50 Remote Code Execution
* AbsoluteTelnet 11.24 Denial Of Service
* YeaLink SIP-TXXXP 53.84.0.15 Command Injection
* FormaLMS 2.4.4 Authentication Bypass
* Win32k NtGdiResetDC Use-After-Free / Local Privilege Escalation
* Microsoft OMI Management Interface Authentication Bypass
* Dolibarr ERP / CRM 13.0.2 Remote Code Execution
* Dolibarr ERP / CRM 13.0.2 Cross Site Scripting
* Employee Daily Task Management System 1.0 Cross Site Scripting
* Employee And Visitor Gate Pass Logging System 1.0 Cross Site Scripting
* Google Assistant Authentication Bypass
* Movable Type 7 r.5002 XMLRPC API Remote Command Injection
* Email-Worm.Win32.Plexus.b Code Execution
* Trojan.Win32.SkynetRef.y Unauthenticated Open Proxy
* Trojan.Win32.SkynetRef.x Unauthenticated Open Proxy
* Simple Client Management System 1.0 Cross Site Scripting
* Trojan.Win32.Servstar.poa Unquoted Service Path
* Kmaleon 1.1.0.205 SQL Injection

CXSecurity

* Xlight FTP 3.9.3.1 Buffer Overflow
* AbsoluteTelnet 11.24 Denial Of Service
* FormaLMS 2.4.4 Authentication Bypass
* FusionPBX 4.5.29 Remote Code Execution
* Fuel CMS 1.4.1 Remote Code Execution
* GitLab Unauthenticated Remote ExifTool Command Injection
* Opencart 3 Extension TMD Vendor System SQL Injection

Proof of Concept (PoC) & Exploits

Exploit Database

* [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
* [webapps] Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)
* [webapps] Simple Subscription Website 1.0 - SQLi Authentication Bypass
* [webapps] KONGA 0.14.9 - Privilege Escalation
* [webapps] WordPress Plugin WPSchoolPress 2.1.16 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Mumara Classic 2.93 - 'license' SQL Injection (Unauthenticated)
* [local] Windows MultiPoint Server 2011 SP1 - RpcEptMapper and Dnschade Local Privilege Escalation
* [dos] Xlight FTP 3.9.3.1 - Buffer Overflow (PoC)
* [webapps] WordPress Plugin AccessPress Social Icons 1.8.2 - 'icon title' Stored Cross-Site Scripting
* [webapps] WordPress Plugin WP Symposium Pro 2021.10 - 'wps_admin_forum_add_name' Stored Cross-Site Sc
* [webapps] FormaLMS 2.4.4 - Authentication Bypass
* [webapps] Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)
* [dos] AbsoluteTelnet 11.24 - 'Phone' Denial of Service (PoC)
* [dos] AbsoluteTelnet 11.24 - 'Username' Denial of Service (PoC)
* [webapps] YeaLink SIP-TXXXP 53.84.0.15 - 'cmd' Command Injection (Authenticated)
* [webapps] Employee and Visitor Gate Pass Logging System 1.0 - 'name' Stored Cross-Site Scripting (XSS
* [webapps] Employee Daily Task Management System 1.0 - 'Name' Stored Cross-Site Scripting (XSS)
* [webapps] FusionPBX 4.5.29 - Remote Code Execution (RCE) (Authenticated)
* [local] zlog 1.2.15 - Buffer Overflow
* [webapps] WordPress Plugin Backup and Restore 1.0.3 - Arbitrary File Deletion
* [webapps] Froxlor 0.10.29.1 - SQL Injection (Authenticated)
* [webapps] Money Transfer Management System 1.0 - Authentication Bypass
* [webapps] Kmaleon 1.1.0.205 - 'tipocomb' SQL Injection (Authenticated)
* [webapps] Simple Client Management System 1.0 - 'multiple' Stored Cross-Site Scripting (XSS)

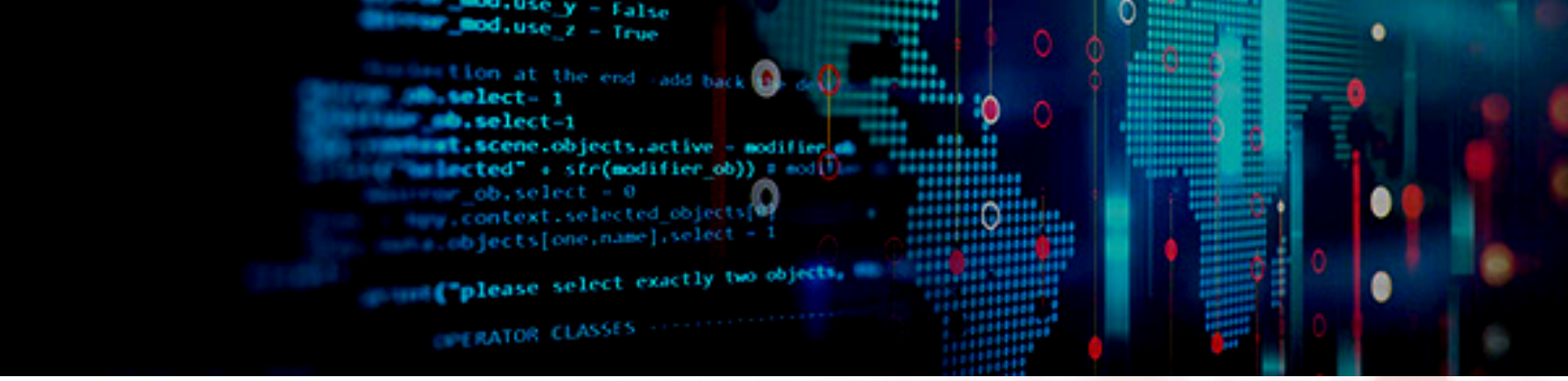
Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is

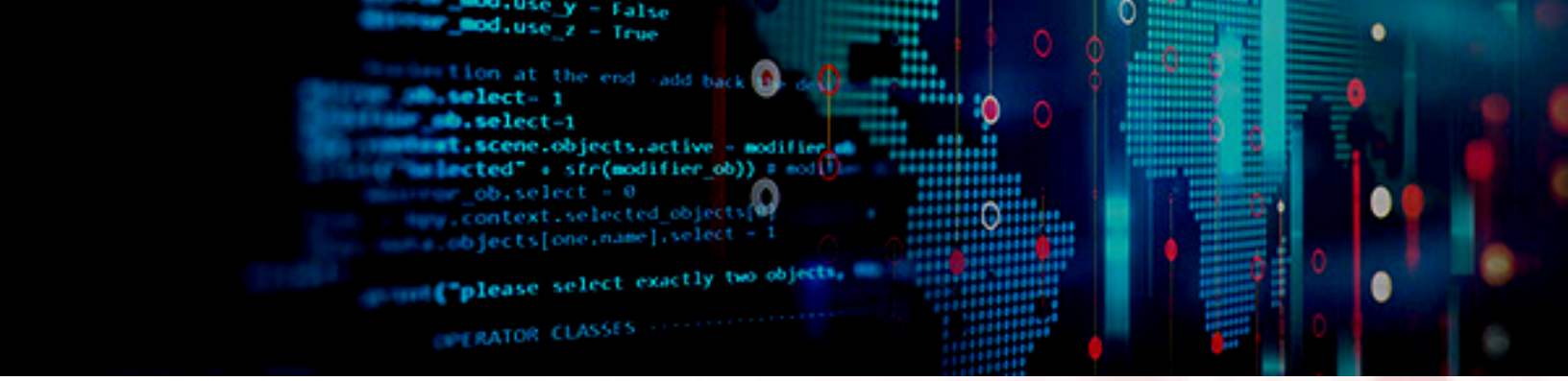
also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://ngrayun.ponorogo.go.id/lucy.txt
http://ngrayun.ponorogo.go.id/lucy.txt notified by luxe
https://www.vcn.gov.ng/slep.html
https://www.vcn.gov.ng/slep.html notified by Mr.Kro0oz.305
https://infosaude.gov.mz/krdsec.html
https://infosaude.gov.mz/krdsec.html notified by 0x1998
https://csrecm.gov.mz/krdsec.html
https://csrecm.gov.mz/krdsec.html notified by 0x1998
https://crepn.gov.mz/krdsec.html
https://crepn.gov.mz/krdsec.html notified by 0x1998
https://crepman.gov.mz/krdsec.html
https://crepman.gov.mz/krdsec.html notified by KrdSec
http://sikkim-culture.gov.in/ks.html
http://sikkim-culture.gov.in/ks.html notified by KrdSec
https://sipac.ufla.br/shared/
https://sipac.ufla.br/shared/ notified by dock0d1
https://sigrh.ufla.br/shared/
https://sigrh.ufla.br/shared/ notified by dock0d1
https://sigpp.ufla.br/shared/
https://sigpp.ufla.br/shared/ notified by dock0d1
https://sigadmin.ufla.br/shared/
https://sigadmin.ufla.br/shared/ notified by dock0d1
https://sigaa.ufla.br/shared/
https://sigaa.ufla.br/shared/ notified by dock0d1
http://cienciaetecnologia.al.gov.br//images/krz.txt
http://cienciaetecnologia.al.gov.br//images/krz.txt notified by Mr.Kro0oz.305
https://www.mozambiqueexpo2020.gov.mz/krd.html
https://www.mozambiqueexpo2020.gov.mz/krd.html notified by 0x1998
http://btdkt.hochiminhcity.gov.vn/index.html
http://btdkt.hochiminhcity.gov.vn/index.html notified by 1877
https://ath.gov.pk
https://ath.gov.pk notified by 1877
https://gobiernosde.gob.ar/krd.html
https://gobiernosde.gob.ar/krd.html notified by 0x1998



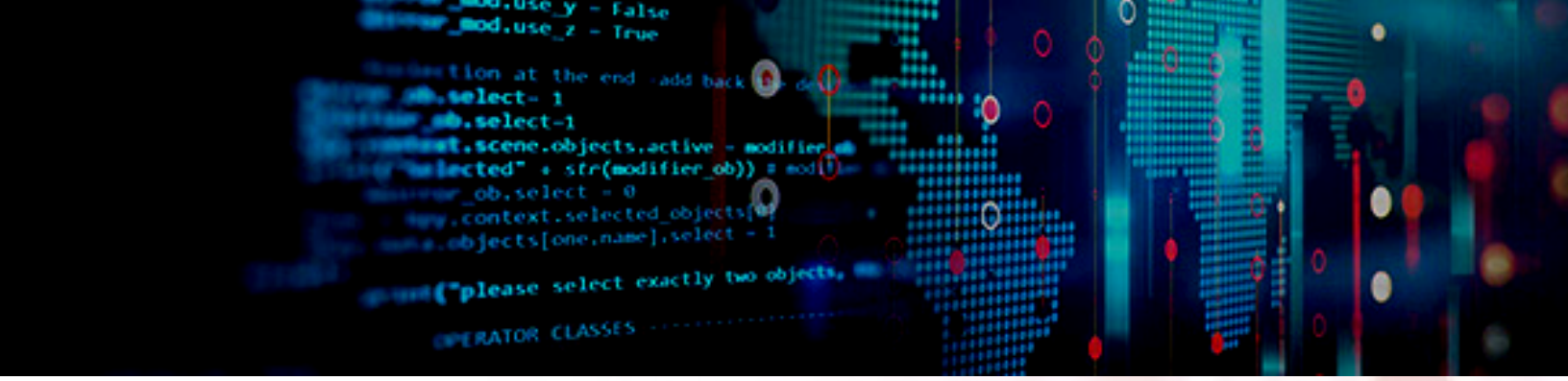
Dark Web News

Darknet Live

Heroin Vendor "Bestman365" Sentenced to Prison
A Maryland man was sentenced to seven years in prison for selling heroin through a vendor account on the darkweb. (via darknetlive.com)
Australian Man Charged for Attempting to Import Meth
Authorities in Australia arrested and charged a man for allegedly importing four kilograms of methamphetamine from Canada. (via darknetlive.com)
Wallstreet Vendor "RaptureReloaded" Sentenced to Prison
A federal judge sentenced Joanna De Alba, 40, to eight years in prison for selling drugs through Wallstreet Market. (via darknetlive.com)
West Virginia Man Sentenced to Prison for Reselling Meth
A West Virginia man was sentenced to 120 months in prison for selling methamphetamine purchased on the darkweb. (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

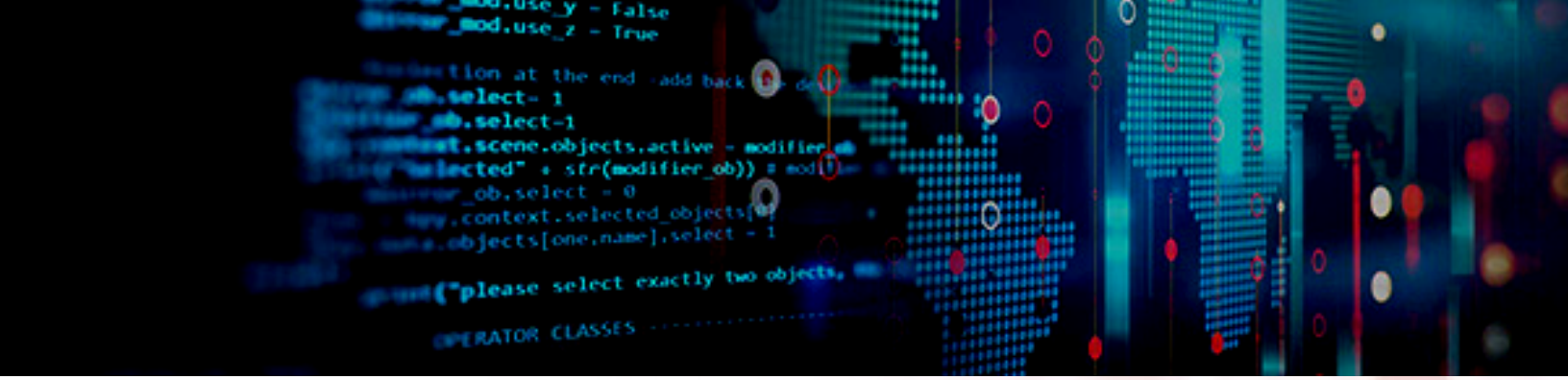
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing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

* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* 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
* Flowspec Bulletproof Services Enable Cybercrime Worldwide
* RiskIQ Analysis Links EITest and Gootloader Campaigns, Once Thought to Be Disparate
* Introducing Next-Gen Vulnerability Intelligence to Identify and Prioritize CVEs in Real-time

FireEye

* Metasploit Wrap-Up
* Hands-On IoT Hacking: Rapid7 at DefCon 29 IoT Village, Part 4
* Time to Act: Bridging the Gap in Cloud Automation Adoption
* Update to GLBA Security Requirements for Financial Institutions
* [Security Nation] Michael Powell on Being a Cyber Envoy
* CVE-2021-43287 Allows Pre-Authenticated Build Takeover of GoCD Pipelines
* tCell by Rapid7 Supports the Newly Released .NET 6.0
* Opportunistic Exploitation of Zoho ManageEngine and Sitecore CVEs
* InsightIDR Was XDR Before XDR Was Even a Thing: An Origin Story
* OWASP Top 10 Deep Dive: Getting a Clear View on Vulnerable and Outdated Components



Advisories

US-Cert Alerts & bulletins

* VMware Releases Security Update for Tanzu Application Service for VMs
* CISA Releases Advisory on Vulnerabilities in Multiple Data Distribution Service Implementations
* Palo Alto Networks Release Security Updates for PAN-OS
* VMware Releases Security Advisory
* Apple Releases Security Update for iCloud for Windows 13
* Microsoft Releases November 2021 Security Updates
* Samba Releases Security Updates
* Citrix Releases Security Updates
* AA21-291A: BlackMatter Ransomware
* AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems
* Vulnerability Summary for the Week of November 1, 2021
* Vulnerability Summary for the Week of October 25, 2021

Zero Day Initiative Advisories

ZDI-CAN-15943: 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: 2021-11-10, 5 days ago. The vendor is given until 2022-03-10 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-15731: 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 'kdot' was reported to the affected vendor on: 2021-11-10, 5 days ago. The vendor is given until 2022-03-10 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-15528: Ivanti
A CVSS score 9.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-11-10, 5 days ago. The vendor is given until 2022-03-10 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-15493: Ivanti
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-11-10, 5 days ago. The vendor is given until 2022-03-10 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-15769: TP-Link
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Bien Pham (@bienpnn) from Team Orca of Sea Security (security.sea.com)' was reported to the affected vendor on:

2021-11-08, 7 days ago. The vendor is given until 2022-03-08 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-15800: Lexmark

A CVSS score 9.6 (AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H) severity vulnerability discovered by 'David BERARD (@_p0ly_), Vincent FARGUES (@Karion_), Thomas IMBERT (@masthoon), from @Synacktiv' was reported to the affected vendor on: 2021-11-08, 7 days ago. The vendor is given until 2022-03-08 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-15670: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15671: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15667: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15449: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15448: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15665: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15668: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15669: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15664: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15666: 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: 2021-10-29, 17 days ago. The vendor is given until 2022-02-26 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-15296: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15587: Microsoft

A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15187: 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: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15446: Microsoft

A CVSS score 4.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15522: 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 'Anonymous' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15443: 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 'Thomas Bouzerar (@MajorTomSec) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15047: Trend Micro

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L) severity vulnerability discovered by 'Elias Martinez (filenotfound - https://www.linkedin.com/in/eli-martinez07/)' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 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-15585: Microsoft

A CVSS score 2.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-10-27, 19 days ago. The vendor is given until 2022-02-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-4531-01

Red Hat Security Advisory 2021-4531-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for Windows serves as the initial Windows release of OpenJDK 17. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-4532-01

Red Hat Security Advisory 2021-4532-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for portable Linux serves as the initial portable Linux release of OpenJDK 17. For further information, refer to the release notes linked to in the References section.

Ubuntu Security Notice USN-5144-1

Ubuntu Security Notice 5144-1 - It was discovered that OpenEXR incorrectly handled certain EXR image files. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Kernel Live Patch Security Notice LSN-0082-1

Jann Horn discovered that the tty subsystem of the Linux kernel did not use consistent locking in some situations, leading to a read-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information (kernel memory). De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker could use this to expose sensitive information (kernel memory) or possibly execute arbitrary code. Various other vulnerabilities were also addressed.

Red Hat Security Advisory 2021-4618-01

Red Hat Security Advisory 2021-4618-01 - Red Hat Advanced Cluster Management for Kubernetes 2.4.0 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 fix several bugs and security issues. Issues addressed include buffer overflow, denial of service, information leakage, integer overflow, out of bounds read, and path sanitization vulnerabilities.

Red Hat Security Advisory 2021-4621-01

Red Hat Security Advisory 2021-4621-01 - FreeRDP is a free implementation of the Remote Desktop Protocol, released under the Apache license. The xfreerdp client can connect to RDP servers such as Microsoft Windows machines, xrdp, and VirtualBox.

Red Hat Security Advisory 2021-4622-04

Red Hat Security Advisory 2021-4622-04 - FreeRDP is a free implementation of the Remote Desktop Protocol, released under the Apache license. The xfreerdp client can connect to RDP servers such as Microsoft Windows machines, xrdp, and VirtualBox.

Ubuntu Security Notice USN-5142-1

Ubuntu Security Notice 5142-1 - Stefan Metzmacher discovered that Samba incorrectly handled SMB1 client connections. A remote attacker could possibly use this issue to downgrade connections to plaintext authentication. Andrew Bartlett discovered that Samba incorrectly mapping domain users to local users. An authenticated attacker could possibly use this issue to become root on domain members. Andrew Bartlett discovered that Samba did not correctly sandbox Kerberos tickets issues by an RODC. An RODC could print administrator tickets, contrary to expectations. Various other issues were also addressed.

Ubuntu Security Notice USN-5141-1

Ubuntu Security Notice 5141-1 - Roman Fiedler discovered that a race condition existed in Firejail when using OverlayFS to prevent writes to the underlying file system. A local attacker could use this to gain administrative

privileges. Note: this update disables support for OverlayFS in Firejail.

Red Hat Security Advisory 2021-4118-01

Red Hat Security Advisory 2021-4118-01 - 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 4.9.6.

Ubuntu Security Notice USN-5137-2

Ubuntu Security Notice 5137-2 - It was discovered that the f2fs file system in the Linux kernel did not properly validate metadata in some situations. An attacker could use this to construct a malicious f2fs image that, when mounted and operated on, could cause a denial of service or possibly execute arbitrary code. It was discovered that the Infiniband RDMA userspace connection manager implementation in the Linux kernel contained a race condition leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possible execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5140-1

Ubuntu Security Notice 5140-1 - It was discovered that the AMD Cryptographic Coprocessor driver in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service. It was discovered that an integer overflow could be triggered in the eBPF implementation in the Linux kernel when preallocating objects for stack maps. A privileged local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-3959-01

Red Hat Security Advisory 2021-3959-01 - This release of Red Hat build of Eclipse Vert.x 4.1.5 includes security updates, bug fixes, and enhancements.

Ubuntu Security Notice USN-5139-1

Ubuntu Security Notice 5139-1 - Ilja Van Sprundel discovered that the SCTP implementation in the Linux kernel did not properly perform size validations on incoming packets in some situations. An attacker could possibly use this to expose sensitive information. It was discovered that the AMD Cryptographic Coprocessor driver in the Linux kernel did not properly deallocate memory in some error conditions. A local attacker could use this to cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-4623-01

Red Hat Security Advisory 2021-4623-01 - FreeRDP is a free implementation of the Remote Desktop Protocol, released under the Apache license. The xfreerdp client can connect to RDP servers such as Microsoft Windows machines, xrdp, and VirtualBox.

Red Hat Security Advisory 2021-4620-01

Red Hat Security Advisory 2021-4620-01 - FreeRDP is a free implementation of the Remote Desktop Protocol, released under the Apache license. The xfreerdp client can connect to RDP servers such as Microsoft Windows machines, xrdp, and VirtualBox.

Red Hat Security Advisory 2021-4619-01

Red Hat Security Advisory 2021-4619-01 - FreeRDP is a free implementation of the Remote Desktop Protocol, released under the Apache license. The xfreerdp client can connect to RDP servers such as Microsoft Windows machines, xrdp, and VirtualBox.

Ubuntu Security Notice USN-5138-1

Ubuntu Security Notice 5138-1 - The py.path.svnwc component of py through v1.9.0 contains a regular expression with an ambiguous subpattern that is susceptible to catastrophic backtracing. This could be used by attackers to cause a compute-time denial of service attack by supplying malicious input to the blame functionality.

Red Hat Security Advisory 2021-4613-01

Red Hat Security Advisory 2021-4613-01 - Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience. This release adds the new Apache HTTP

Server 2.4.37 Service Pack 10 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 9 and includes bug fixes and enhancements. Issues addressed include buffer over-read, heap overflow, integer overflow, and null pointer vulnerabilities.

Red Hat Security Advisory 2021-4614-01

Red Hat Security Advisory 2021-4614-01 - This release adds the new Apache HTTP Server 2.4.37 Service Pack 10 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 9 and includes bug fixes and enhancements. Issues addressed include buffer over-read, heap overflow, integer overflow, and null pointer vulnerabilities.

Red Hat Security Advisory 2021-4593-04

Red Hat Security Advisory 2021-4593-04 - Annobin provides a compiler plugin to annotate and tools to examine compiled binary files.

Red Hat Security Advisory 2021-4589-03

Red Hat Security Advisory 2021-4589-03 - Annobin provides a compiler plugin to annotate and tools to examine compiled binary files.

Red Hat Security Advisory 2021-4586-03

Red Hat Security Advisory 2021-4586-03 - The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

Red Hat Security Advisory 2021-4585-03

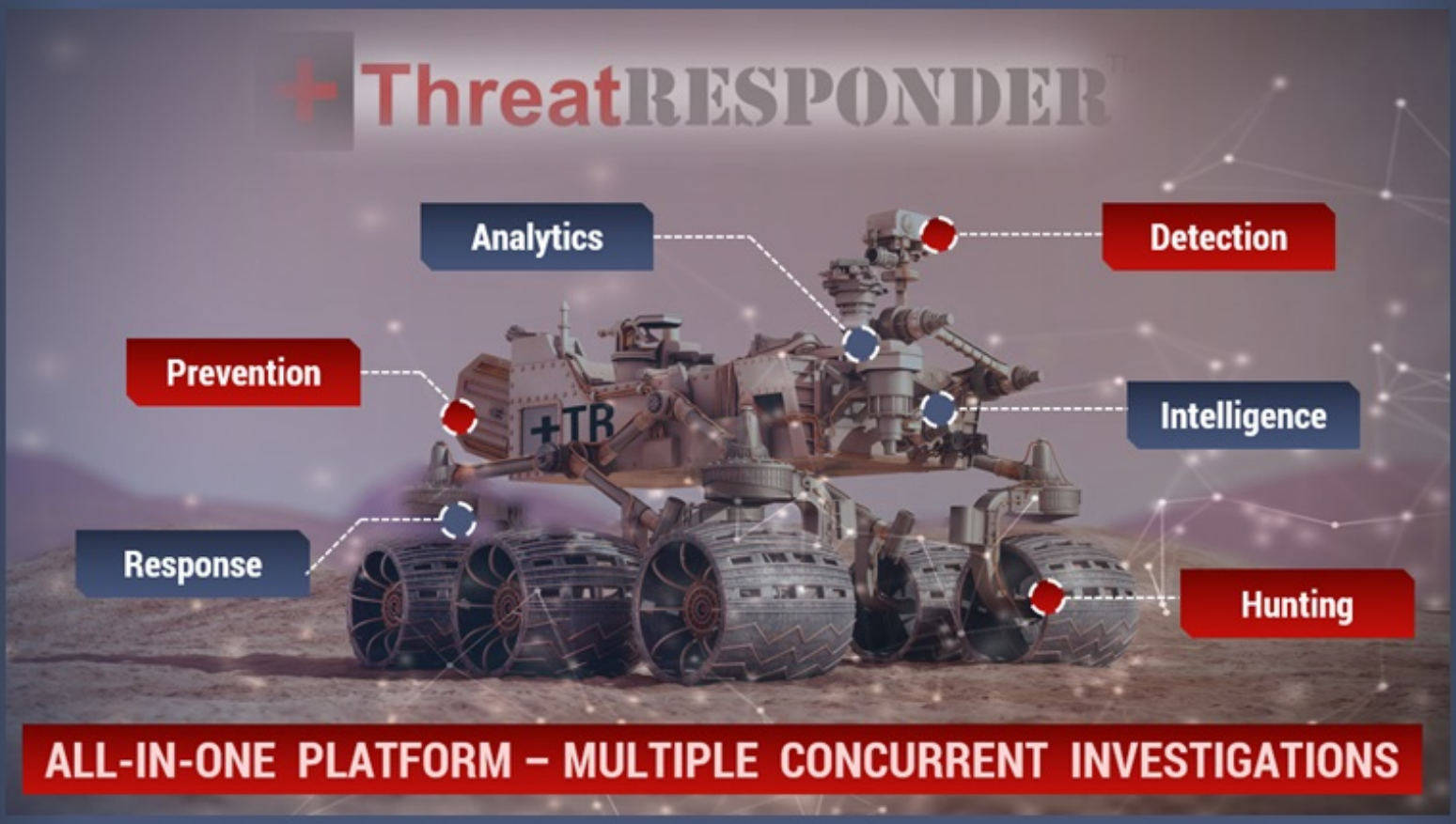
Red Hat Security Advisory 2021-4585-03 - The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

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



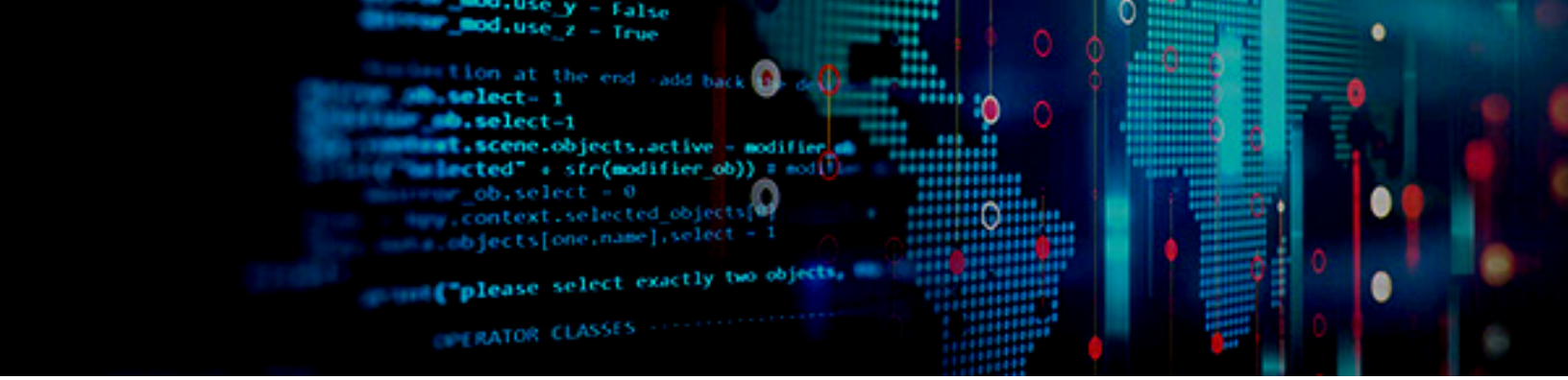
The Solution – ThreatResponder® Platform

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

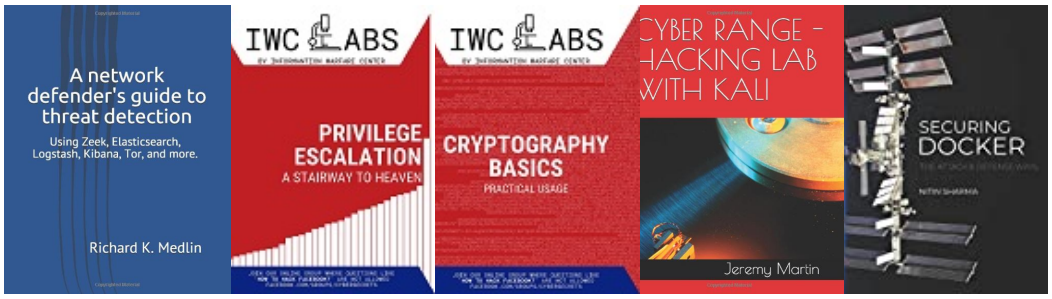


The Cyber Secrets publications on Amazon

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