
Jul-05-21
CYBER
WEEKLY
AWARENESS
REPORT
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS
netSecurity
INFORMATION WARFARE CENTER
LINUX
ARGOS
APPLIED INTELLIGENCE

July 5, 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

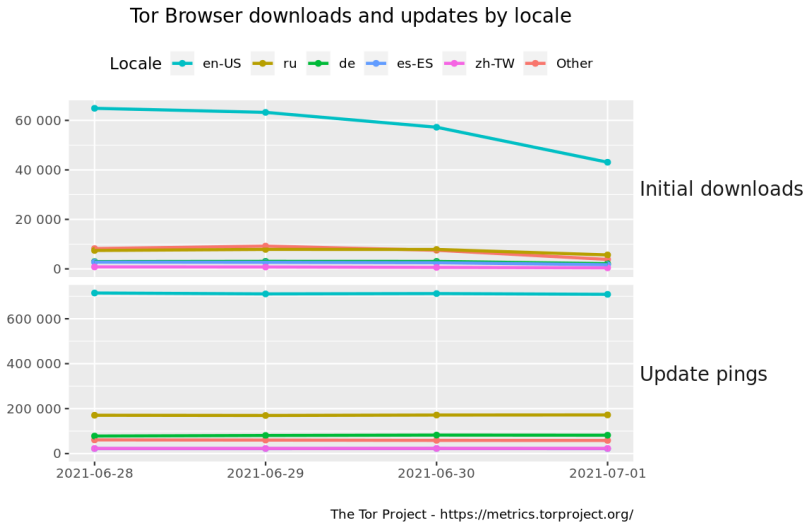
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

Just released!!! Web App Hacking: Carnage & Pwnage



Interesting News

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

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

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

Index of Sections

Packet Storm Security

* Biden Announces Investigation Into International Ransomware Attack
* Ransomware Attacks Driving Cyber Reinsurance Rates Up 40%
* Didi Barred From China App Stores Amidst Government Security Review
* Gang Behind Huge Cyber Attack Demands $70M In Bitcoin
* Ransomware Gangs Taking Aim At Soft Target Industrial Control Systems
* Hacked Data For 69K LimeVPN Users Up For Sale On Dark Web
* Feds File New Charges For Amazon Employee That Leveraged Server Access To Hack Capital One
* China Investigates Didi Over Cyber Security Days After Its IPO
* Russian Military Hackers Have Been On A Worldwide Password Guessing Spree
* Colombia Police Collar Suspected Gozi Trojan Distributor
* XKEYSCORE Spy Program Revealed By Snowden Still A Problem
* Netgear Authentication Bypass Allows Router Takeover
* Lorenz Ransomware Victims Can Recover Files With Free Tool
* Chinese Hacking Group Impersonates Afghan President To Infiltrate Government Agencies
* Microsoft Executive Says U.S. Overuses Secret Orders For Americans' Data
* This VPN Service Used By Ransomware Gangs Was Just Taken Down By Police
* You Can Hijack Google Cloud VMs Using DHCP Floods
* Cobalt Strike Usage Explodes Among Cybercrooks
* Feds Told To Better Manage Facial Recognition
* Microsoft Approved A Windows Driver With Rootkit Malware
* Hackers Exploited 0-Day, Not 2018 Bug, To Mass-Wipe My Book Live Devices
* A Well-Meaning Feature Leaves Millions Of Dell PCs Vulnerable
* Data For 700M LinkedIn Users Posted For Sale
* Using The Android USB Driver To Extract Data As USB Mass Storage Device
* GitHub Bug Bounty Payouts Surge Past $1.5 Million

Krebs on Security

* Another 0-Day Looms for Many Western Digital Users
* Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax
* We Infiltrated a Counterfeit Check Ring! Now What?
* MyBook Users Urged to Unplug Devices from Internet
* How Cyber Sleuths Cracked an ATM Shimmer Gang
* How Cyber Safe is Your Drinking Water Supply?
* First American Financial Pays Farcical $500K Fine
* Ukrainian Police Nab Six Tied to CLOP Ransomware
* How Does One Get Hired by a Top Cybercrime Gang?
* Microsoft Patches Six Zero-Day Security Holes

Dark Reading

* Watch for Cybersecurity Games at the Tokyo Olympics
* Barracuda Agrees to Acquire Skout Cybersecurity
* Secured-Core PCs May Mitigate Firmware Attacks, but Adoption Lags
* Microsoft Issues New CVE for 'PrintNightmare' Flaw
* SOC Investment Improves Detection and Response Times, Data Shows
* 5 Mistakes That Impact a Security Team's Success
* WFH: A Smart Time to Revisit Employee Use of Social Media
* GitHub Unveils AI Tool to Speed Development, but Beware Insecure Code
* CISA Urges Orgs to Disable Windows Print Spooler on Critical Systems
* WhiteHat Security Rebrands as NTT Application Security
* Name That Edge Toon: Security Grill
* CISA Updates CSET Tool for Ransomware Defense
* NSA & CISA Issue Warning About Russian GRU Brute-Force Cyberattacks Against US, Global Orgs
* Why Are There Never Enough Logs During an Incident Response?
* Stop Playing Catchup: Move From Reactive to Proactive to Defeat Cyber Threats
* SentinelOne Starts Trading on NYSE, Raises $1.2B in IPO
* SMB Worm Targeting EternalBlue Vuln Spreads to US
* Impersonation Becomes Top Phishing Technique
* MyBook Investigation Reveals Attackers Exploited Legacy, Zero-Day Vulnerabilities
* Attackers Already Unleashing Malware for Apple macOS M1 Chip

The Hacker News

* Getting Started with Security Testing: A Practical Guide for Startups
* TrickBot Botnet Found Deploying A New Ransomware Called Diavol
* Microsoft Urges Azure Users to Update PowerShell to Patch RCE Flaw
* REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom
* Android Apps with 5.8 million Installs Caught Stealing Users' Facebook Passwords
* Kaseya Supply-Chain Attack Hits Nearly 40 Service Providers With REvil Ransomware
* Learn to Code - Get 2021 Master Bundle of 13 Online Courses @ 99% OFF
* New Mirai-Inspired Botnet Could Be Using Your KGUARD DVRs in Cyber Attacks
* Mongolian Certificate Authority Hacked to Distribute Backdoored CA Software
* New Google Scorecards Tool Scans Open-Source Software for More Security Risks
* NSA, FBI Reveal Hacking Methods Used by Russian Military Hackers
* Microsoft Warns of Critical "PrintNightmare" Flaw Being Exploited in the Wild
* IndigoZebra APT Hacking Campaign Targets the Afghan Government
* Rethinking Application Security in the API-First Era
* Facebook Sues 4 Vietnamese for Hacking Accounts and $36 Million Ad Fraud

Security Week

* Scale, Details of Massive Kaseya Ransomware Attack Emerge
* IT Software Firm Kaseya Hit By Supply Chain Ransomware Attack
* Hackers Compromise Mongolian Certificate Authority to Spread Malware
* Microsoft Tells Azure Users to Update PowerShell to Patch Vulnerability
* New Ransomware 'Diavol' Linked to Notorious Cybercrime Gang
* Microsoft Confirms 'PrintNightmare' is New Windows Security Flaw
* Ferry Agency: No Sensitive Info Compromised in Cyberattack
* Director of Cybersecurity at NSA Gets Dedicated Twitter Account
* DHS Hired 300 Cybersecurity Professionals in Last Two Months
* Vulnerabilities in WAGO Devices Expose Industrial Firms to Remote Attacks
* French Tech Firm Charged Over Libya Cyber-Spying
* Russians Used Brute Force Attacks Against Hundreds of Orgs: Security Agencies
* The VC View: Enabling Business via IT Security
* SASE Provider Versa Networks Raises $84 Million
* Sevco Security Banks $15 Million Series A Funding
* University Medical Center Says Hackers Breached Data Server
* Becoming Elon Musk - the Danger of Artificial Intelligence
* Cybersecurity M&A Roundup: 37 Deals Announced in June 2021
* Critical, Exploitable Flaws in NETGEAR Router Firmware
* Study Finds Insurance Companies Lack Cyber Hygiene
* Google, OpenSSF Update Scorecards Project With New Security Checks
* Twitter Enables Use of Security Keys as Sole Two-Factor Authentication Method
* CISA Adds Ransomware Module to Cyber Security Evaluation Tool
* Vulnerability Found in Industrial Remote Access Product From Claroty

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Important Kaseya Notice! Turn VSA Off. Now. Ransomware. Updated
* [BREAKING] NSA, Partners Release Cybersecurity Advisory on Brute Force Global Cyber Campaign
* New IcedID and QBot Phishing Campaigns Are Running Amuck
* How to Get The Most Out of Your Compliance Platform
* Almost All LinkedIn User's Data Has Been Scraped and is Up for Sale on the Dark Web
* Spear Phishing Impersonation Attacks Take on New Tactics to Become More Convincing and Effective
* Yet Another Disk Image File Format Spotted in the Wild Used to Deliver Malware
* 35% of All Security Incidents are Business Email Compromise Phishing Attacks
* [Eye Opener] The Biggest Bitcoin Heist Ever: A Whopping 3.6 Billion Dollars!
* CyberheistNews Vol 11 #25 [Heads Up] Attackers Abuse Your Google Docs With a New Phishing Angle

ISC2.org Blog

* Igniting Passion for Diversity, Equity and Inclusion (DEI): Cybersecurity Professionals Address Chall
* DoD Adds Two More (ISC)² Certifications to Requirements for Cybersecurity Staff
* NIST Has Come Out With Its Own Ransomware Guidance | #RansomwareWeek
* Six Steps to Protect Your Organization from Ransomware | #RansomwareWeek
* (ISC)² Offers Free Access to Ransomware Education | #RANSOMWAREWEEK

HackRead

* Revil ransomware increases ransom to $70M in Kaseya attack
* 9 apps with 6M installs stole Facebook logins of Android users
* REvil Ransomware targets 1000+ businesses causing holiday havoc
* Spanish telecom giant MasMovil hit by Revil ransomware gang
* Online learning provider New Skills Academy alerts users of data breach
* Colombia arrests suspect wanted by US over Gozi virus
* Domain, server of DoubleVPN used by ransomware gangs seized

Koddos

* Revil ransomware increases ransom to $70M in Kaseya attack
* 9 apps with 6M installs stole Facebook logins of Android users
* REvil Ransomware targets 1000+ businesses causing holiday havoc
* Spanish telecom giant MasMovil hit by Revil ransomware gang
* Online learning provider New Skills Academy alerts users of data breach
* Colombia arrests suspect wanted by US over Gozi virus
* Domain, server of DoubleVPN used by ransomware gangs seized

Naked Security

* Kaseya ransomware attackers say: "Pay $70 million and we'll set everyone free"
* US email hacker gets his "computer trespass" conviction reversed
* S3 Ep39: Paying the date, #SocialMediaDay tips, and a special splintersode [Podcast]
* PrintNightmare, the zero-day hole in Windows - here's what to do
* Colombian police arrest Gozi malware suspect after 8 years at large
* Police warn of WhatsApp scams in time for Social Media Day
* British tourists charged Â£1000s for pier visits in billing blunder
* S3 Ep38: Clop busts, destructive Linux hacking, and rooted bicycles [Podcast]
* Ransomware: What REALLY happens if you pay the crooks?
* Can *YOU* blow a PC speaker using only a Linux kernel driver?

Threat Post

* Ransomware Defense: Top 5 Things to Do Right Now
* TrickBot Spruces Up Its Banking Trojan Module
* Widespread Brute-Force Attacks Tied to Russia's APT28
* Why Healthcare Keeps Falling Prey to Ransomware and Other Cyberattacks
* CISA Offers New Mitigation for PrintNightmare Bug
* Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices
* Defeating Ransomware-as-a-Service? Think Intel-Sharing
* Hacked Data for 69K LimeVPN Users Up for Sale on Dark Web
* Babuk Ransomware Builder Mysteriously Appears in VirusTotal
* Data Exfiltration: What You Should Know to Prevent It

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

* The OSI Model and You Part 7: Stopping Threats at the Application Layer
* Confessions of a Famous Fraudster: How and Why Social Engineering Scams Work
* Hunting for Windows "Features" with Frida: DLL Sideloading
* June 2021 Security Intelligence Roundup: Cybersecurity Certifications, The Problem With New Accounts
* A Fly on ShellBot's Wall: The Risk of Publicly Available Cryptocurrency Miners
* The OSI Model and You Part 6: Stopping Threats at the OSI Presentation Layer
* Cloud Security: Navigating the Cloud Migration Journey Successfully
* Data Security Along Every Stage of the Journey
* Shifting Left With Analytics to Identify Software Supply Chain Anomalies
* Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy

InfoWorld

* How the cloud and big compute are remaking HPC
* How 5 companies got their developers to care about cloud costs
* The problem with sharding
* GitHub unveils AI coding assistant for Visual Studio Code
* Cloud lock-in is real
* Accessibility improvements coming to Visual Studio
* What is MongoDB? A quick guide for developers
* Rethinking data architectures for a cloud world
* Red Hat OpenShift 4.8 shines on CI/CD, serverless functions
* What Windows 11 means for developers

C4ISRNET - Media for the Intelligence Age Military

* Rafael combines AI and automatic target recognition in new Sea Breaker missile
* Big screen to battlefield: How sci-fi can inspire next-generation weaponry
* Robins looks to bring home the BACN under new Air Force proposal
* The Space Development Agency now has demo satellites on orbit. Here's what they'll do.
* Army to set in stone the importance of information advantage, with new capabilities on deck
* Skyborg makes its second flight, this time autonomously piloting General Atomics' Avenger drone
* Virgin Orbit plane launches four US military satellites into space
* Intel agencies, armed services push for more data and capability sharing to win future fights
* Pentagon's top IT official: More coordination needed on weapon systems and critical infrastructure cy
* Pentagon official placed on leave over allegations of unauthorized release of classified info

The Hacker Corner

Conferences

* 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)
* How To Sponsor Cybersecurity Conferences

Google Zero Day Project

* An EPYC escape: Case-study of a KVM breakout
* Fuzzing iOS code on macOS at native speed

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.

* Capture the Signal CTF 2021
* redpwnCTF 2021
* ENOWARS 5
* TyphoonCon CTF 2021
* Google Capture The Flag 2021
* RuCTF 2021
* HTB Business CTF 2021
* ImaginaryCTF 2021
* IJCTF 2021
* CyBRICS CTF 2021

VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* HackathonCTF: 2
* Hackable: II
* VulnCMS: 1
* hacksudo: ProximaCentauri
* Tech_Supp0rt: 1

Tools & Techniques

Packet Storm Security Tools Links

* Suricata IDPE 6.0.3
* nfstream 6.3.3
* Lynis Auditing Tool 3.0.5
* TOR Virtual Network Tunneling Tool 0.4.6.6
* Falco 0.29.1
* Samhain File Integrity Checker 4.4.5
* Global Socket 1.4.32
* Faraday 3.16.0
* Proxmark 4.13441
* Flawfinder 2.0.18

Kali Linux Tutorials

* Shreder : A Powerful Multi-Threaded SSH Protocol Password Bruteforce Tool
* BlobHunter : Find Exposed Data In Azure With This Public Blob Scanner
* SharpHook : Tool Tath Uses Various API Hooks In Order To Give Us The Desired Credentials
* CamRaptor : Tool That Exploits Several Vulnerabilities In Popular DVR Cameras To Obtain Network Camer
* HoneyCreds : Network Credential Injection To Detect Responder And Other Network Poisoners
* Dark Load Library : Load Library For Offensive Operations
* Mythic : A Collaborative, Multi-Platform, Red Teaming Framework
* HashCheck : Tool To Assist In The Search For Leaked Passwords
* Swift-Attack : Unit Tests For Blue Teams To Aid With Building Detections For Some Common macOS Post E
* Xerror : An Automated Penetration Tool

GBHackers Analysis

* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices
* 5 Key Phases of Ethical Hacking
* Researcher Managed to Hack ATMs Using His Phone's NFC & Android App
* 10 Best WiFi Hacking Apps for Android - 2021 Edition
* How to Protect Your Email From Hacking?

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown - Ransomware with guest speaker Ryan Chapman
* Mobile Validation - Working together for the Common Good
* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course

Defcon Conference

* DEF CON China Party 2021 - Keynote Interview Excerpt - Steve Wozniak, The Dark Tangent
* DEF CON China Party 2021 - Whispers Among the Stars - James Pavur
* DEF CON China Party 2021- Wall of Sheep: Hilarious Fails and the Sheep Behind Them - Riverside
* DEF CON China Party - Cooper Quintin- Detecting Fake 4G Base Stations in Real Time

Hak5

* Building DIY Lithium Battery Packs w/Glytch Pt3
* HakByte: Build a Hackable Router with a $5 ESP32
* Introducing the Bash Bunny Mark II - Story Time with @Hak5Darren

The PC Security Channel [TPSC]

* F Secure Total: Test vs Malware and ID Protection
* Windows Defender vs Malware in 2021

Eli the Computer Guy

* How to Become a YouTuber
* How to Become a Tech Professional
* "Easy" SMS with Twilio (Add SMS to Your Coding Projects)
* "Easy" Computer Vision with Azure and AWS

Security Now

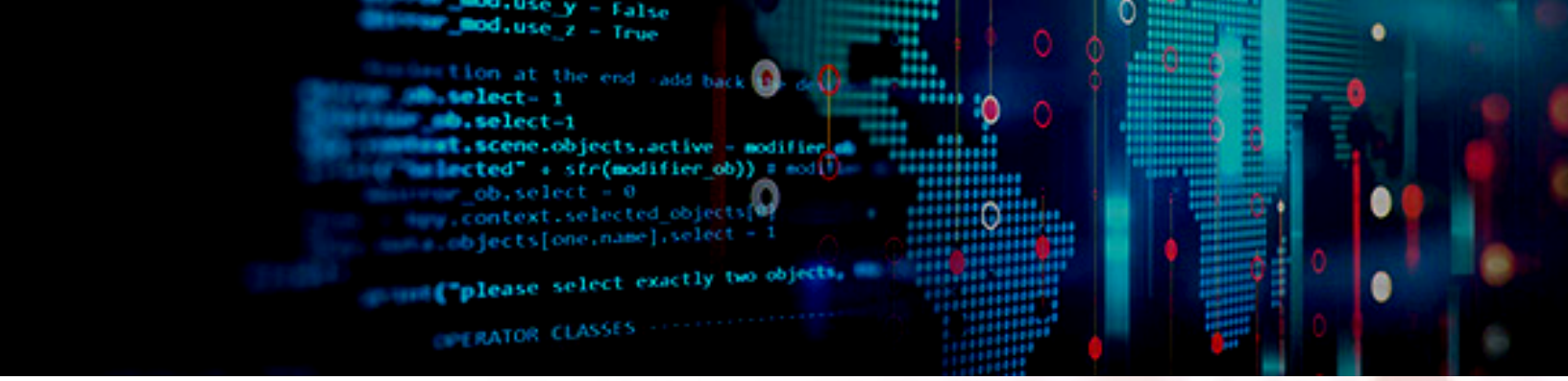
* Halfway Through 2021 - Google's FLoC, $600M Ransomware Attack, Where Will Windows 11 Run?
* Avaddon Ransonomics - Chrome 0-Day, Big Spinrite Update, iOS Wi-Fi Bug, Economics of Ransomware

Troy Hunt

* Weekly Update 250

Intel Techniques: The Privacy, Security, & OSINT Show

* 223-Secure Messaging Woes (and Solutions)
* 222-Spoiler: We all die



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

* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think
* MobileInter: A Popular Magecart Skimmer Redesigned For Your Phone
* DarkSide is Standing Down, But Its Affiliates Live On
* Next-Gen Threat Intelligence: Adding Profound Value to Security and Risk Functions
* TrickBot: Get to Know the Malware That Refuses to Be Killed
* SolarWinds: Illuminating the Hidden Patterns That Advance the Story

FireEye

* Managed Service Providers Used in Coordinated, Mass Ransomware Attack Impacting Hundreds of Companies
* Metasploit Wrap-Up
* CVE-2021-1675 (PrintNightmare) Patch Does Not Remediate Vulnerability
* ForgeRock Access Manager/OpenAM Pre-Auth Remote Code Execution Vulnerability (CVE-2021-35464): What Y
* #Rapid7Life Belfast: Why I Joined
* Automated remediation level 3: Governance and hygiene
* 3 Takeaways From The 2021 VDBIR: It's An Appandemic
* Metasploit Wrap-Up
* Kill Chains: Part 3→What's Next
* CVE-2021-20025: SonicWall Email Security Appliance Backdoor Credential

Proof of Concept (PoC) & Exploits

Packet Storm Security

* PrintNightmare Windows Spooler Service Remote Code Execution
* Garbage Collection Management System 1.0 SQL Injection
* Microsoft PrintNightmare Proof Of Concept
* Scratch Desktop 3.17 Code Execution / Cross Site Scripting
* WordPress Modern Events Calendar 5.16.2 Shell Upload
* WordPress Modern Events Calendar 5.16.2 Information Disclosure
* b2evolution 7.2.2 Cross Site Request Forgery
* AKCP sensorProbe SPX476 Cross Site Scripting
* Packet Storm New Exploits For June, 2021
* Docker Container Escape
* WordPress XCloner 4.2.12 Remote Code Execution
* WinWaste.NET 1.0.6183.16475 Local Privilege Escalation
* Online Voting System 1.0 Remote Code Execution
* Online Voting System 1.0 SQL Injection
* Vianeos OctoPUS 5 SQL Injection
* KVM nested_svm_vmrun Double Fetch
* Apache Superset 1.1.0 Account Enumeration
* Securepoint SSL VPN Client 2.0.30 Local Privilege Escalation
* Doctors Patients Management System 1.0 SQL Injection
* phpAbook 0.9i SQL Injection
* ES File Explorer 4.1.9.7.4 Arbitrary File Read
* WordPress wpDiscuz 7.0.4 Shell Upload
* Constructor.Win32.Bifrose.asc Buffer Overflow / Heap Corruption
* WordPress YOP Polls 6.2.7 Cross Site Scripting
* Personnel Record Management System 1.0 Authentication Bypass / XSS

CXSecurity

* GLPI 9.4.5 Remote Code Execution
* EasyFTP Server 1.7.0.11 Denial Of Service
* KnFTP Server 1.0.0 Denial Of Service
* elFinder 2.0.47 - 'PHP connector' Command Injection
* WordPress Modern Events Calendar 5.16.2 Shell Upload
* rConfig Shell Upload
* Adobe ColdFusion 8 Remote Command Execution

Proof of Concept (PoC) & Exploits

Exploit Database

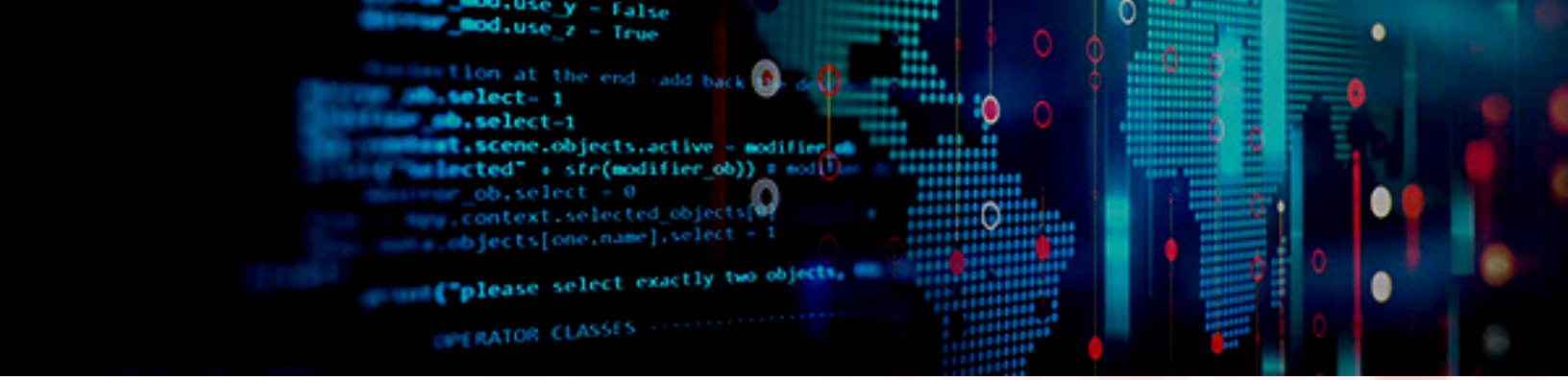
* [webapps] Ricon Industrial Cellular Router S9922XL - Remote Command Execution (RCE)
* [webapps] TextPattern CMS 4.9.0-dev - Remote Command Execution (RCE) (Authenticated)
* [webapps] Simple Client Management System 1.0 - Remote Code Execution (RCE)
* [webapps] Wordpress Plugin Backup Guard 1.5.8 - Remote Code Execution (Authenticated)
* [webapps] Church Management System 1.0 - 'password' SQL Injection (Authentication Bypass)
* [webapps] Church Management System 1.0 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Church Management System 1.0 - Unrestricted File Upload to Remote Code Execution (Authentic
* [webapps] Online Birth Certificate System 1.1 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Online Voting System 1.0 - SQLi (Authentication Bypass) + Remote Code Execution (RCE)
* [webapps] OpenEMR 5.0.1.7 - 'fileName' Path Traversal (Authenticated) (2)
* [webapps] WordPress Plugin WP Learn Manager 1.1.2 - Stored Cross-Site Scripting (XSS)
* [webapps] Garbage Collection Management System 1.0 - SQL Injection (Unauthenticated)
* [webapps] Wordpress Plugin Modern Events Calendar 5.16.2 - Event export (Unauthenticated)
* [local] WinWaste.NET 1.0.6183.16475 - Privilege Escalation due Incorrect Access Control
* [webapps] Wordpress Plugin Modern Events Calendar 5.16.2 - Remote Code Execution (Authenticated)
* [webapps] b2evolution 7.2.2 - 'edit account details' Cross-Site Request Forgery (CSRF)
* [webapps] AKCP sensorProbe SPX476 - 'Multiple' Cross-Site Scripting (XSS)
* [webapps] Scratch Desktop 3.17 - Cross-Site Scripting/Remote Code Execution (XSS/RCE)
* [webapps] Vianeos OctoPUS 5 - 'login_user' SQLi
* [webapps] Wordpress Plugin XCloner 4.2.12 - Remote Code Execution (Authenticated)
* [webapps] Online Voting System 1.0 - Remote Code Execution (Authenticated)
* [webapps] Online Voting System 1.0 - Authentication Bypass (SQLi)
* [webapps] Doctors Patients Management System 1.0 - SQL Injection (Authentication Bypass)
* [webapps] Simple Traffic Offense System 1.0 - 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*

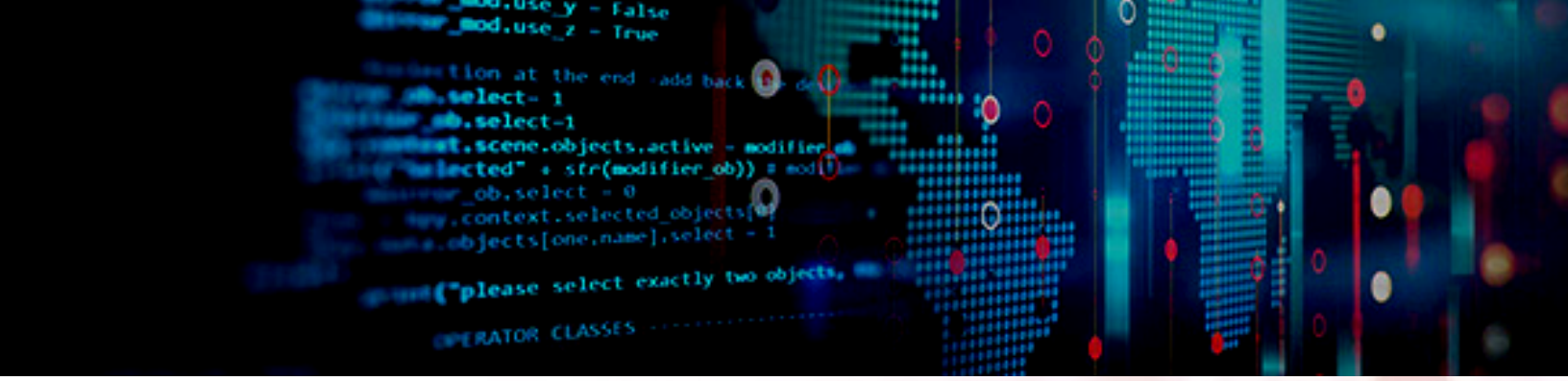
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://pn-pangkalanbalai.go.id/zzz.txt
https://pn-pangkalanbalai.go.id/zzz.txt notified by Family Attack Cyber
http://rajfed.gov.in/rn.html
http://rajfed.gov.in/rn.html notified by Ren4Sploit
https://www.npc.gov.gh/vz.txt
https://www.npc.gov.gh/vz.txt notified by aDriv4
http://centralinvest.gov.vn/rn.html
http://centralinvest.gov.vn/rn.html notified by Ren4Sploit
http://daknongdpi.gov.vn/rn.html
http://daknongdpi.gov.vn/rn.html notified by Ren4Sploit
https://www.ezeiza.gob.ar/noname.html
https://www.ezeiza.gob.ar/noname.html notified by K4TSUY4-GH05T
http://pn-tuban.go.id/readme.html
http://pn-tuban.go.id/readme.html notified by Family Attack Cyber
http://municaceresdelperu.gob.pe/ox.html
http://municaceresdelperu.gob.pe/ox.html notified by F.Z MalaikatHati
http://pta-babel.go.id/hyme.html
http://pta-babel.go.id/hyme.html notified by Family Attack Cyber
https://www.casadeculturapiedradelsol.gov.co/vz.txt
https://www.casadeculturapiedradelsol.gov.co/vz.txt notified by aDriv4
http://zls.go.tz/er.php
http://zls.go.tz/er.php notified by LahBodoAmat
http://erdemlisydv.gov.tr/rn.html
http://erdemlisydv.gov.tr/rn.html notified by Ren4Sploit
http://ataturkarboretumu.gov.tr/rn.html
http://ataturkarboretumu.gov.tr/rn.html notified by Ren4Sploit
http://marsu.gov.tr/rn.html
http://marsu.gov.tr/rn.html notified by Ren4Sploit
http://ataturkolimpiyatstadi.gov.tr/rn.html
http://ataturkolimpiyatstadi.gov.tr/rn.html notified by Ren4Sploit
http://artvinkhb.gov.tr/rn.html
http://artvinkhb.gov.tr/rn.html notified by Ren4Sploit
http://yhsb.gov.tr/rn.html
http://yhsb.gov.tr/rn.html notified by Ren4Sploit



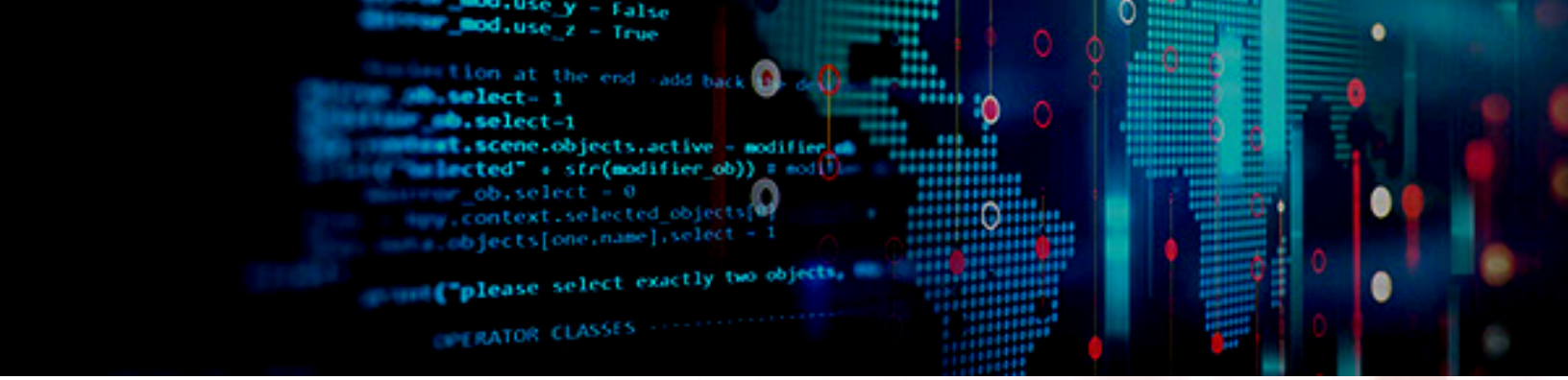
Dark Web News

Darknet Live

[The Majority of Market Admins Don't Get Caught]
Although many high-profile cases involving darkweb market admins make the news, the majority of market creators retire in peace. (via darknetlive.com)
[German Woman Tried to Hire a Hitman on the Darkweb]
A German woman allegedly tried to hire a hitman on the darkweb to murder her ex-husband's girlfriend. (via darknetlive.com)
[PA Man Admits Attempting to Buy Meth on the Darkweb]
A Pennsylvania man faces 40 years in prison for attempting to purchase methamphetamine on the darkweb. (via darknetlive.com)
[Alleged Firearm Vendor and Customers Charged in Germany]
Four Germans allegedly traded firearms and other weapons on the darkweb, according to authorities in Frankfurt. (via darknetlive.com)

Dark Web Link

[Biometric Selfies & Forged Passports On The Dark Web For Sale]
Personal identities are rapidly sold on the dark web, with the recent ones being biometric selfies. Privacy Affairs has published a report named "2021 Dark Web Price Index”, seeing this massive surge. The report details the average prices for various products that include all kinds of selfies bearing IDs. These selfies can be utilized to [...] The post Biometric Selfies & Forged Passports On The Dark Web For Sale appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Brit Paedophile Arrested After 70 Home Security Camera Hack]
A Brit paedophile has been arrested in Benidorm. The man had been under suspicion of hacking over 70 families' home security cameras around the world. Spanish Police stated that the unnamed pedophile had worked as a babysitter and private tutor. He had acquired 1,000 images of the naked children. Apart from this, the Brit paedophile [...] The post Brit Paedophile Arrested After 70 Home Security Camera Hack appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Crypto Coin Exchanges: What Is Happening Right Now?]
The majority of the top cryptocurrencies are lately trading in red, with Ethereum (ETH) and Bitcoin (BTC) down around 3% in the past 24 hours. The global crypto market capitalization is currently at $1.51 trillion, which is a sharp decline of 3.40% over the previous day. The world's largest cryptocurrency, Bitcoin, has dropped as much [...] The post Crypto Coin Exchanges: What Is Happening Right Now? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Att
* Kaseya VSA Supply-Chain Ransomware Attack
* NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign
* PrintNightmare, Critical Windows Print Spooler Vulnerability
* CISA's CSET Tool Sets Sights on Ransomware Threat
* CISA Begins Cataloging Bad Practices that Increase Cyber Risk
* Citrix Releases Security Updates for Hypervisor
* VMware Releases Security Updates
* AA21-148A: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* Vulnerability Summary for the Week of June 28, 2021
* Vulnerability Summary for the Week of June 21, 2021

Zero Day Initiative Advisories

ZDI-CAN-14375: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14372: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14466: 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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14335: Open Design Alliance (ODA)
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14308: Open Design Alliance (ODA)
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: 2021-07-02, 3 days ago. The vendor is given until

2021-10-30 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-14333: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14325: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14314: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14299: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14285: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14353: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14345: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14301: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14351: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14352: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend

Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14331: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14349: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14329: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14337: Open Design Alliance (ODA)

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: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14350: Open Design Alliance (ODA)

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-13796: D-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 'Anonymous' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-14457: Trend Micro

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L) severity vulnerability discovered by 'Simon Zuckerbraun - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-02, 3 days ago. The vendor is given until 2021-10-30 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-13755: Commvault

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Justin Kennedy, Brandon Perry' was reported to the affected vendor on: 2021-06-30, 5 days ago. The vendor is given until 2021-10-28 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-13706: Commvault

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 'Brandon Perry, Justin Kennedy and Steven Seeley of Source Incite' was reported to the affected vendor on: 2021-06-30, 5 days ago. The vendor is given until 2021-10-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-4905-2

Ubuntu Security Notice 4905-2 - USN-4905-1 fixed a vulnerability in X.Org. This update provides the corresponding update for Ubuntu 14.04 ESM. Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain lengths of XInput extension ChangeFeedbackControl requests. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2634-01

Red Hat Security Advisory 2021-2634-01 - Go Toolset provides the Go programming language tools and libraries. Go is alternatively known as golang. Issues addressed include a memory exhaustion vulnerability.

Red Hat Security Advisory 2021-2517-01

Red Hat Security Advisory 2021-2517-01 - 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 3.11.462. Issues addressed include XML injection, cross site request forgery, and denial of service vulnerabilities.

Red Hat Security Advisory 2021-2575-01

Red Hat Security Advisory 2021-2575-01 - The lz4 packages provide support for LZ4, a very fast, lossless compression algorithm that provides compression speeds of 400 MB/s per core and scales with multicore CPUs. It also features an extremely fast decoder that reaches speeds of multiple GB/s per core and typically reaches RAM speed limits on multicore systems. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2566-01

Red Hat Security Advisory 2021-2566-01 - The fwupd packages provide a service that allows session software to update device firmware. Issues addressed include buffer overflow, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2569-01

Red Hat Security Advisory 2021-2569-01 - The libxml2 library is a development toolbox providing the implementation of various XML standards. Issues addressed include buffer overflow, bypass, null pointer, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2574-01

Red Hat Security Advisory 2021-2574-01 - 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 2021-2570-01

Red Hat Security Advisory 2021-2570-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include bypass and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2595-01

Red Hat Security Advisory 2021-2595-01 - 389 Directory Server is an LDAP version 3 compliant server. The base packages include the Lightweight Directory Access Protocol server and command-line utilities for server administration. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2021-2588-01

Red Hat Security Advisory 2021-2588-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include HTTP request smuggling, HTTP response splitting, denial of service, information leakage, and insecure permissions vulnerabilities.

Red Hat Security Advisory 2021-2587-01

Red Hat Security Advisory 2021-2587-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include HTTP request smuggling, HTTP response splitting, denial of service, and information leakage vulnerabilities.

Red Hat Security Advisory 2021-2591-01

Red Hat Security Advisory 2021-2591-01 - EDK is a project to enable UEFI support for Virtual Machines. This package contains a sample 64-bit UEFI firmware for QEMU and KVM. Issues addressed include a heap corruption vulnerability.

Red Hat Security Advisory 2021-2584-01

Red Hat Security Advisory 2021-2584-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has

features to process text files and to perform system management tasks. Issues addressed include a HTTP request smuggling vulnerability.

Red Hat Security Advisory 2021-2583-01

Red Hat Security Advisory 2021-2583-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.

Red Hat Security Advisory 2021-2599-01

Red Hat Security Advisory 2021-2599-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include bypass and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2563-01

Red Hat Security Advisory 2021-2563-01 - 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 2021-2561-01

Red Hat Security Advisory 2021-2561-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache Tomcat Servlet container, JBoss HTTP Connector, the PicketLink Vault extension for Apache Tomcat, and the Tomcat Native library. This release of Red Hat JBoss Web Server 5.5.0 serves as a replacement for Red Hat JBoss Web Server 5.4.2, and includes bug fixes, enhancements and component upgrades, which are documented in the Release Notes, linked to in the References. Issues addressed include a remote SQL injection vulnerability.

Red Hat Security Advisory 2021-2562-01

Red Hat Security Advisory 2021-2562-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache Tomcat Servlet container, JBoss HTTP Connector, the PicketLink Vault extension for Apache Tomcat, and the Tomcat Native library. This release of Red Hat JBoss Web Server 5.5.0 serves as a replacement for Red Hat JBoss Web Server 5.4.2, and includes bug fixes, enhancements and component upgrades, which are documented in the Release Notes, linked to in the References. Issues addressed include a remote SQL injection vulnerability.

Red Hat Security Advisory 2021-2500-01

Red Hat Security Advisory 2021-2500-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-2499-01

Red Hat Security Advisory 2021-2499-01 - 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 4.6.36. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-4997-2

Ubuntu Security Notice 4997-2 - USN-4997-1 fixed vulnerabilities in the Linux kernel for Ubuntu 21.04. This update provides the corresponding updates for the Linux KVM kernel for Ubuntu 21.04. Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5000-2

Ubuntu Security Notice 5000-2 - USN-5000-1 fixed vulnerabilities in the Linux kernel for Ubuntu 20.04 LTS and the Linux HWE kernel for Ubuntu 18.04 LTS. This update provides the corresponding updates for the Linux KVM kernel for Ubuntu 20.04 LTS. Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4998-1

Ubuntu Security Notice 4998-1 - It was discovered that in some situations Ceph logged passwords from the mgr module

in clear text. An attacker could use this to expose sensitive information. Goutham Pacha Ravi, Jahson Babel, and John Garbutt discovered that user credentials in Ceph could be manipulated in certain environments. An attacker could use this to gain unintended access. It was discovered that the Ceph dashboard was susceptible to a cross-site scripting attack. An attacker could use this to expose sensitive information or gain unintended access. Various other issues were also addressed.

Ubuntu Security Notice USN-4995-2

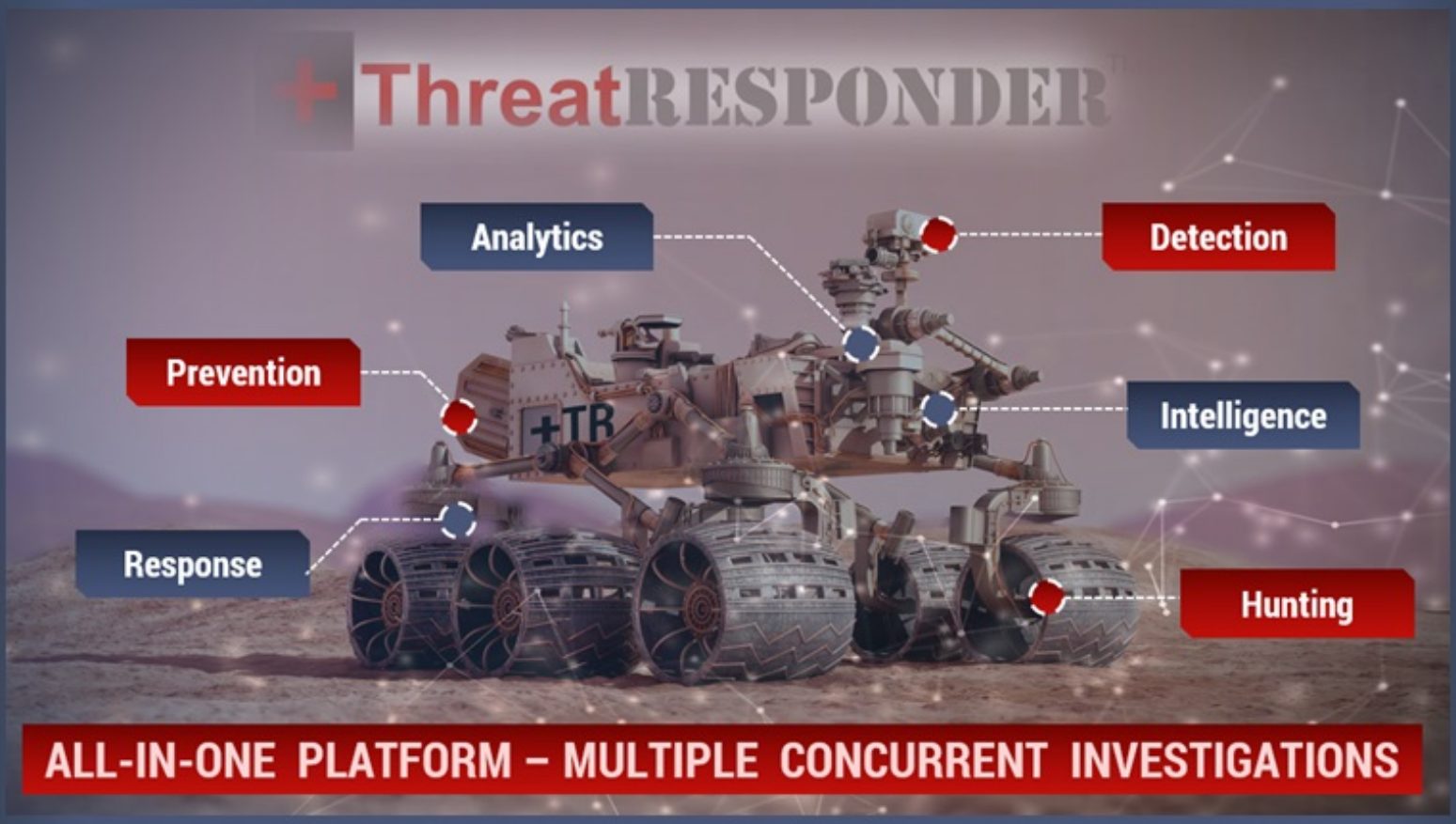
Ubuntu Security Notice 4995-2 - USN-4995-1 fixed vulnerabilities in Thunderbird. This update provides the corresponding updates for Ubuntu 18.04 LTS. Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass security restrictions, or execute arbitrary code. It was discovered that extensions could open popup windows with control of the window title in some circumstances. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to spoof a website and trick the user into providing credentials. Multiple security issues were discovered in Thunderbird's OpenPGP integration. If a user were tricked into importing a specially crafted key in some circumstances, an attacker could potentially exploit this to cause a denial of service or confuse the user. A use-after-free was discovered when Responsive Design Mode was enabled. If a user were tricked into opening a specially crafted website with Responsive Design Mode enabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. It was discovered that Thunderbird mishandled ftp URLs with encoded newline characters. If a user were tricked into clicking on a specially crafted link, an attacker could potentially exploit this to send arbitrary FTP commands. It was discovered that Thunderbird wrote signatures to disk and read them back during verification. A local attacker could potentially exploit this to replace the data with another signature file. It was discovered that Thunderbird might load an alternative OTR library. If a user were tricked into copying a specially crafted library to one of Thunderbird's search paths, an attacker could potentially exploit this to execute arbitrary code. It was discovered that secret keys imported into Thunderbird were stored unencrypted. A local attacker could potentially exploit this to obtain private keys. It was discovered that Thunderbird did not indicate when an inline signed or encrypted message contained additional unprotected parts. Various other issues were also addressed.

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

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

CSI Linux is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux has been rebuilt from the ground up on Ubuntu 20.04 LTS to provide long term support for the backend OS and has become a powerful Investigation environment that comes in both the traditional Virtual Machine option and a bootable image that you can install onto an external drive or USB to use as your daily driver or DFIR triage drive. The SIEM has been given an evolution boost with capability while being encapsulated into a Docker container

CSI Linux Tutorials:

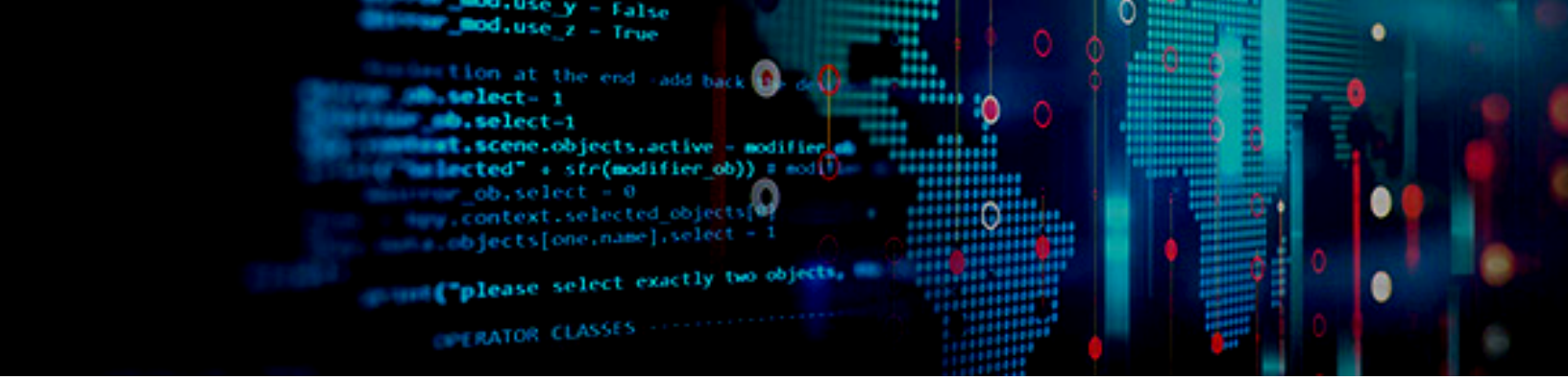
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:
* Amazon FireTV App - amzn.to/30oiUpE
* YouTube - youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg

Printed / Kindle Publications:
* Cyber Secrets on Amazon - amzn.to/2UuIG9B

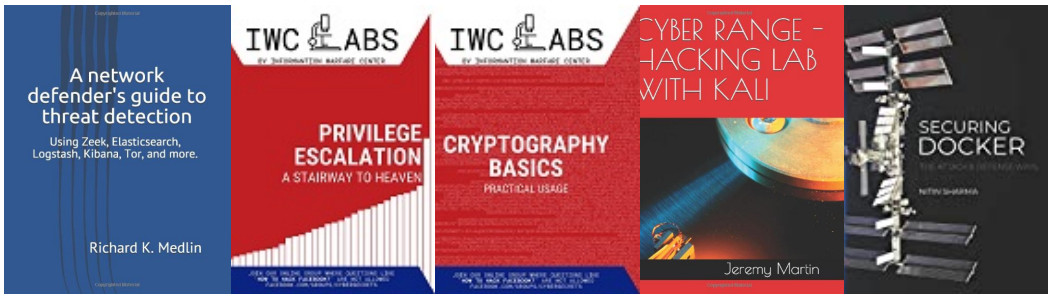


The Cyber Secrets publications on Amazon

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