Dec-06-21

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

December 6, 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

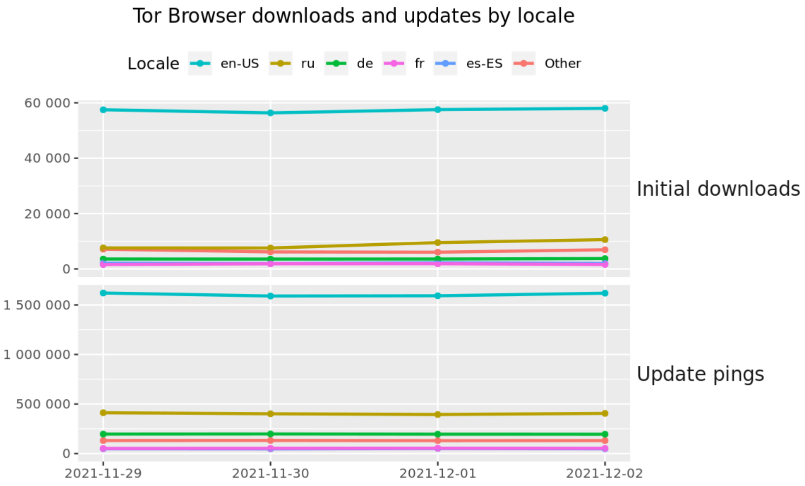
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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.



The Tor Project - https://metrics.torproject.org/

Interesting News

* **Cyber Monday:** Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case. This is a prerequizite for all other courses CSI Linux offers.

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

Index of Sections

Current News

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

The Hacker Corner:

* Security Conferences
* Google Zero Day Project

Cyber Range Content

* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques

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

InfoSec Media for the Week

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

Exploits and Proof of Concepts

* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified

* CyberCrime-Tracker

Advisories

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

Information Warfare Center Products

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

LATEST NEWS

Packet Storm Security

* US Rejects Calls For Regulating Or Banning Killer Robots
* Researcher Found Way To Brute Force Verizon Customer PINs
* Hackers Steal $119 Million From Web3 Crypto Project With Old School Attack
* Ransomware Attack On Planned Parenthood Steals Data Of 400k Patients
* Stealthy WIRTE Gang Targets Middle Eastern Governments
* Facebook To Mandate High Security Program For Politicians, Journalists
* Really Stupid "Smart Contract" Bug Let Hackers Steal $31 Million In Digital Coin
* Is KAX17 Performing De-Anonymization Attacks Against Tor Users?
* More Than 1/3 Of The World Has Never Used The Internet, Says UN
* These Researchers Wanted To Test Cloud Security. They Were Shocked By What They Found
* Twitch Unleashes AI Tool To Spot Banned Users
* DNA Testing Center Admits To Breach Of Data For 2 Million People
* Thousands Of AT&T Customers In The US Infected By New Data Stealing Malware
* Yanluowang Ransomware Tied To Thieflock Threat Actor
* IKEA Hit By Email Reply Chain Cyber Attack
* Printing Shellz: Critical Bugs Impacting 150 HP Printer Models Patched
* Zoom Owes Everyone $25 For Giving Their Data To Facebook
* MI6 Must Adapt To New Technology To Survive, Says Spy Chief
* Google Play Apps Downloaded 300,000 Times Stole Bank Credentials
* Chinese Could Hack Data For Future Quantum Decryption, Report Warns
* What The SEC Requires From Businesses After A Data Breach
* Panasonic Confirms Data Breach After Hackers Access Internal Network
* 1,000 Arrests Made In Online Fraud Crackdown, Says Interpol
* This Stealthy Malware Hides Behind An Impossible Date
* Mr Goxx, The Cryptocurrency Trading Hamster, Dies

Krebs on Security

* Who Is the Network Access Broker 'Babam'?
* Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach"
* The Internet is Held Together With Spit & Baling Wire
* Arrest in 'Ransom Your Employer' Email Scheme
* The 'Zelle Fraud' Scam: How it Works, How to Fight Back
* Tech CEO Pleads to Wire Fraud in IP Address Scheme
* Hoax Email Blast Abused Poor Coding in FBI Website
* SMS About Bank Fraud as a Pretext for Voice Phishing
* Microsoft Patch Tuesday, November 2021 Edition
* REvil Ransom Arrest, $6M Seizure, and $10M Reward

LATEST NEWS

Dark Reading

* One-Third of Black Friday Shoppers Were Bots, Fake Users
* NSO Group Spyware Used to Breach US State Dept. Phones
* IGI Cybersecurity Introduces CISO Team-as-a-Service
* How Criminals Are Using Synthetic Identities for Fraud
* Logiq.ai Tackles Observability Problem With LogFlow
* USB Devices the Common Denominator in All Attacks on Air-Gapped Systems
* An Insider's Account of Disclosing Vulnerabilities
* Ransomware, Carding, and Initial Access Brokers: Group-IB Presents Report on Trending Crimes
* Darktrace Reports 30% More Ransomware Attacks Targeting Organizations During the Holiday Period
* Remote Browser Isolation Stars in Content Protection Role
* Top 5 Reasons to Get 'SASE' With Security
* Planned Parenthood LA Breach Compromises 400,000 Patients' Data
* Develop 'Foursight' - Keep Your Post-COVID Transformation on Track
* Key Characteristics of Malicious Domains: Report
* When Will a Cloud Infrastructure Heavyweight Launch a SASE?
* Breaking the Black Mirror and Other Lessons From Day of Shecurity
* Military Vets Share Lessons That Helped Them Build Infosec Startups
* APT Groups Adopt New Phishing Method. Will Cybercriminals Follow?
* Russian Man Sentenced to 60 Months in Prison for Running 'Bulletproof' Hosting for Cybercrime
* Neustar Security Services Spins Out as Own Company

The Hacker News

* Malicious KMSPico Windows Activator Stealing Users' Cryptocurrency Wallets
* Vulnerability Scanning Frequency Best Practices
* Hackers Steal $200 Million Worth of Cryptocurrency Tokens from BitMart Exchange
* 14 New XS-Leaks (Cross-Site Leaks) Attacks Affect All Modern Web Browsers
* Pegasus Spyware Reportedly Hacked iPhones of U.S. State Department and Diplomats
* Warning: Yet Another Zoho ManageEngine Product Found Under Active Attacks
* Researchers Detail How Pakistani Hackers Targeting Indian and Afghan Governments
* New Malvertising Campaigns Spreading Backdoors, Malicious Chrome Extensions
* Why Everyone Needs to Take the Latest CISA Directive Seriously
* New Payment Data Stealing Malware Hides in Nginx Process on Linux Servers
* CISA Warns of Actively Exploited Critical Zoho ManageEngine ServiceDesk Vulnerability
* Meta Expands Facebook Protect Program to Activists, Journalists, Government Officials
* Researches Detail 17 Malicious Frameworks Used to Attack Air-Gapped Networks
* Let there be light: Ensuring visibility across the entire API lifecycle
* Researchers Warn Iranian Users of Widespread SMS Phishing Campaigns

LATEST NEWS

Security Week

* Hackers Steal $150 Million Worth of Cryptocurrency From BitMart
* Cyberattack Causes Significant Disruption at Colorado Electric Utility
* Pegasus Maker Probes Reports its Spyware Targeted US Diplomats
* Researchers Find 226 Vulnerabilities in Nine Wi-Fi Routers
* Iranians Charged for Cryptojacking After U.S. Firm Gets $760,000 Cloud Bill
* CISA Informs Organizations About Vulnerabilities in Hitachi Energy Products
* Facebook, Twitter Take Down More State-Linked Accounts
* 17 Malware Frameworks Target Air-Gapped Systems for Espionage
* TSA Requires Rail and Airports to Strengthen Cybersecurity
* Facebook Expands Advanced Security Program to More Countries
* Security Analytics Startup Panther Labs Scores $120M Investment
* CISA Adds Zoho, Qualcomm, Mikrotik Flaws to 'Must-Patch' List
* Webinar Today: CISO Fireside Chat With Steve Katz, World's First Known CISO
* Karamba Security Raises $10 Million to Protect Connected Devices
* Blockchain Security Provider CertiK Raises $80 Million
* Critical Flaw in NSS Cryptographic Library Affects Several Popular Applications
* Russian Administrator of Bulletproof Hosting Sentenced to Prison in U.S.
* Data Hacked for 400,000 Planned Parenthood LA Patients
* Former Employee Accused of Being Behind Ubiquiti Hack
* CyCognito Snags $100M Investment for Attack Surface Management
* Prediction Season: What's in Store for Cybersecurity in 2022?
* Aqua Security Acquires Software Development Security Firm Argon
* Critical Vulnerability Found in More Than 150 HP Printer Models
* VirusTotal Introduces 'Collections' to Simplify IoC Sharing
* Cybersecurity M&A Roundup: 40 Deals Announced in November 2021

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Your KnowBe4 Fresh Content Updates from November 2021
* [Heads Up] First Omicron Phishing Attack Spotted In The UK
* Morgan Stanley Warns Against "Brushing Scam"
* Ingenious New Attack Technique Uses Windows Store to Install Malware
* 91% of All Baiting Attacks Use Gmail to Collect Intel on Potential Victims
* When Cybercriminals Hide in Plain Sight: Hacking Platforms You Know and Trust
* Holiday Shopping and Phishing-as-a-Service
* Bitcoin Scam Videos on Instagram are Part of an Elaborate Account Takeover Scam
* Phishing Attacks Smash All Records in Q3 2021 With the Highest Monthly Number of Attacks Ever
* Mobile Phishing Attacks Surge 161% in the Energy Industry

ISC2.org Blog

* Poll Data: What CEOs Need to Know About Cybersecurity Going into 2022
* Data Consistency Storage in the Cloud
* CISSPs from Around the Globe: An Interview with Chinyelu Philomena Karibi-Whyte
* A Safe and Secure Way to Decommission
* How to Prepare for CISSP Exam Day

HackRead

* BitMart Exchange hacked as hackers steal $150 million
* Malvertising attack distributes malicious Chrome extensions, backdoors
* Hackers steal $120m from Badger Defi and $30m from MonoX
* Planned Parenthood data breach: Hackers steal 400,000 patients' data
* Development of Corporate Applications Based on Artificial Intelligence
* DNA testing service data breach impacting 2.1 million users
* 300,000 Android users impacted by malware apps on Play Store

Koddos

* BitMart Exchange hacked as hackers steal $150 million
* Malvertising attack distributes malicious Chrome extensions, backdoors
* Hackers steal $120m from Badger Defi and $30m from MonoX
* Planned Parenthood data breach: Hackers steal 400,000 patients' data
* Development of Corporate Applications Based on Artificial Intelligence
* DNA testing service data breach impacting 2.1 million users
* 300,000 Android users impacted by malware apps on Play Store

LATEST NEWS

Naked Security

* Mozilla patches critical "BigSig" cryptographic bug: Here's how to track it down and fix it
* S3 Ep61: Call scammers, cloud insecurity, and facial recognition creepiness [Podcast]
* IoT devices must "protect consumers from cyberharm", says UK government
* Clearview AI face-matching service set to be fined over $20m
* Cloud Security: Don't wait until your next bill to find out about an attack!
* S3 Ep60: Exchange exploit, GoDaddy breach and cookies made public [Podcast]
* US government securities watchdog spoofed by investment scammers - don't fall for it!
* Check your patches - public exploit now out for critical Exchange bug
* GoDaddy admits to password breach: check your Managed WordPress site!
* Black Friday and Cyber Monday - here's what you REALLY need to do!

Threat Post

* Pandemic-Influenced Car Shopping: Just Use the Manufacturer API
* Omicron Phishing Scam Already Spotted in UK
* What Are Your Top Cloud Security Challenges? Threatpost Poll
* Threat Group Takes Aim Again at Cloud Platform Provider Zoho
* 'Double-Extortion' Ransomware Damage Skyrockets 935%
* Planned Parenthood Breach Opens Patients to Follow-On Attacks
* AT&T Takes Steps to Mitigate Botnet Found Inside Its Network
* 80K Retail WooCommerce Sites Exposed by Plugin XSS Bug
* Stealthy 'WIRTE' Gang Targets Middle Eastern Governments
* Widespread 'Smishing' Campaign Defrauds Iranian Android Users

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

LATEST NEWS

IBM Security Intelligence

* What the Internet Bug Bounty Teaches About Open-Source Software Security
* Technical Problem or Cyber Crime? How to Tell the Difference
* Data Security: Defending Against the Cache Poisoning Vulnerability
* "Trusted Partner" in Cybersecurity: Clich&eacute; or Necessity?
* Why the Future Needs Passwordless Authentication
* How to Cut Down on Data Breach Stress and Fatigue
* X-Force Threat Intelligence: Monthly Malware Roundup
* Roundup: Ransomware, the Future of the Cloud and Cyber Careers
* How Do You Plan to Celebrate National Computer Security Day?
* Understanding the Adversary: How Ransomware Attacks Happen

InfoWorld

* How CentOS changes the cloud Linux game
* Review: Document parsing in AWS, Azure, and Google Cloud
* A cure for complexity in software development
* Top developer takeaways from AWS re:Invent 2021
* AWS updates databases, AI and serverless offerings at re:Invent
* JetBrains launches cross-platform UI framework for Kotlin
* Why the cloud computing hangover?
* AWS brings no-code to Amazon SageMaker machine learning
* Hands-on with SolidJS
* "Do More with R" video tutorials

C4ISRNET - Media for the Intelligence Age Military

* French defense minister: Shifting from a new frontier to a new front
* IISS analysts: Fiscal constraints drive the state of South America's defense
* NRO director: Innovation is the key to America's advantage in space
* US military tech leads: Achieving all-domain decision advantage through JADC2
* CYBERCOM and NSA chief: Cybersecurity is a team sport
* Almaz-Antey director: Air and space capabilities will decide tomorrow's conflicts
* Cyberwarriors will soon have access to more training tools
* US should expect cyberattacks in any struggle for Taiwan
* Egyptian defense expo highlights homemade tech to counter small drones
* Department of Defense orders $316 million more in anti-jam GPS devices

The Hacker Corner

Conferences

* Marketing Cybersecurity In 2021
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

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

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* OverTheWire Advent Bonanza 2021
* Capture The TI_eRx
* NITECTF
* X-MAS CTF 2021 First Weekend
* idekCTF 2021
* SECCON CTF 2021
* Hack-A-Sat 2 Finals
* CTF Internacional MetaRed 2021 - 5th STAGE
* hxp CTF 2021
* STAY ~/ CTF 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

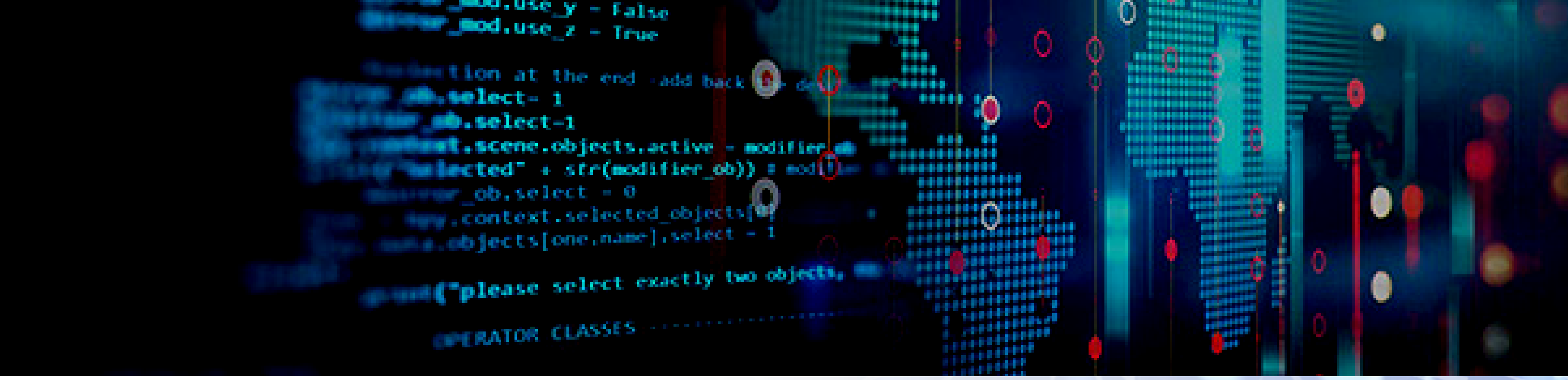
* I2P 1.6.1
* Wapiti Web Application Vulnerability Scanner 3.0.8
* Stegano 0.10.1
* Photon OSINT Crawler 1.3.2
* OpenStego Free Steganography Solution 0.8.2
* GNU Privacy Guard 2.2.33
* Wireshark Analyzer 3.6.0
* OpenStego Free Steganography Solution 0.8.1
* Hashcat Advanced Password Recovery 6.2.5 Source Code
* Hashcat Advanced Password Recovery 6.2.5 Binary Release

Kali Linux Tutorials

* Smuggler : An HTTP Request Smuggling / Desync Testing Tool
* Certipy : Python Implementation For Active Directory Certificate Abuse
* Tor-Rootkit : A Python 3 Standalone Windows 10 / Linux Rootkit Using Tor
* PyRDP : RDP Monster-In-The-Middle (Mitm) And Library For Python With The Ability To Watch Connections
* Androidqf : (Android Quick Forensics) Helps Quickly Gathering Forensic Evidence From Android Devices,
* If You Need Academic Help, Here's Where You Can Get It
* How to Protect Small and Medium-Sized Businesses From Cyberattacks
* LDAPmonitor : Monitor Creation, Deletion And Changes To LDAP Objects Live During Your Pentest Or Syst
* TIWAP : Totally Insecure Web Application Project
* Cybersecurity Tips For Startups

GBHackers Analysis

* Printing Shellz - New Vulnerabilities That Affects 150 Different Multifunction Printers
* North Korean Hackers Group Posed as Samsung Recruiters To Target Security Firms
* Two Iranian Hackers Charged For Gaining Access to Confidential Voter Information
* Void Balaur - Hacker-for-Hire Group Stealing Emails & Sensitive Data From More Than 3,500 Targets
* Hackers Exploit Microsoft Exchange Vulnerabilities To Drop Babuk Ransomware



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Wrap Up Panel
* Open Threat Research - The Hunt for Red Apples: How to threat hunt and emulate Ocean Lotus on macOS
* Hunting Beacon Activity with Fourier Transforms
* Common misconceptions and mistakes made in Threat Hunting

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelg&auml;nger Your H&auml;x 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

* Making a Hardware WiFi Recon Tool with the ESP8266 | HakByte
* Android Eavesdropping Vulnerability Patched by MediaTek; GoDaddy Hacked - ThreatWire
* What parts should you use for a 3d printed drone

The PC Security Channel [TPSC]

* Phobos Ransomware
* Windows 11 vs Ransomware

Eli the Computer Guy

* APPLE FAIL - BIGGER PROBLEMS THAN SUPPLY CHAIN
* BIDEN SURRENDERS ON UNCONSTITUTIONAL COVID MANDATES
* DESANTIS CREATING SECRET POLICE for FLORIDA - copying new york and california
* REPUBLICANS KILLING BIDEN VACCINE MANDATE using debt ceiling

Security Now

* Bogons Begone! - 0-Day Windows Exploit, Major MediaTek Flaw, Super Duper Secure Mode
* HTTP Request Smuggling - NetGear Routers 0-Day, The Most Brute Forced Passwords, GoDaddy Breach

Troy Hunt

* Weekly Update 272

Intel Techniques: The Privacy, Security, & OSINT Show

* 242-Privacy News & Updates
* 241-Listener Questions

Proof of Concept (PoC) & Exploits

Packet Storm Security

* OrbiTeam BSCW Server XSS / LFI / User Enumeration
* Backdoor.Win32.WinShell.50 Hardcoded Password
* WordPress All-In-One Video Gallery 2.4.9 Local File Inclusion
* Ubuntu Overlayfs Local Privilege Escalation
* WordPress Slider By Soliloquy 2.6.2 Cross Site Scripting
* Backdoor.Win32.WinShell.50 Hardcoded Password
* WordPress DZS Zoomsounds 6.45 Arbitrary File Read
* Online Magazine Management System 1.0 SQL Injection
* Backdoor.Win32.Bionet.10 Authentication Bypass / Code Execution
* Backdoor.Win32.Vernet.axt Insecure Permissions
* M-Files Web Denial Of Service
* Online Pre-Owned / Used Car Showroom Management System 1.0 SQL Injection
* Trojan.Win32.Mucc.ivk Unquoted Service Path
* DuckDuckGo 7.64.4 Address Bar Spoofing
* Android vold Unsafe Mounting
* Packet Storm New Exploits For November, 2021
* MilleGPG5 5.7.2 Luglio 2021 Privilege Escalation
* NSS Signature Validation Memory Corruption
* Advanced Comment System 1.0 Remote Command Execution
* Online Enrollment Management System In PHP And PayPal 1.0 Cross Site Scripting
* Laundry Booking Management System 1.0 Remote Code Execution
* Orangescrum 1.8.0 Privilege Escalation
* Orangescrum 1.8.0 SQL Injection
* Orangescrum 1.8.0 Cross Site Scripting
* Opencart 3.0.3.8 Session Injection

CXSecurity

* Ubuntu Overlayfs Local Privilege Escalation
* Advanced Comment System 1.0 Remote Command Execution
* Pinkie 2.15 TFTP Remote Buffer Overflow (PoC)
* Nextar C472 POS DLL Hijacking
* D-Link DSL-3782 Pre-Authentication Remote Root
* CMSimple 5.4 Local File Inclusion / Remote Code Execution
* Apache HTTP Server 2.4.50 Remote Code Execution Py ver

Proof of Concept (PoC) & Exploits

Exploit Database

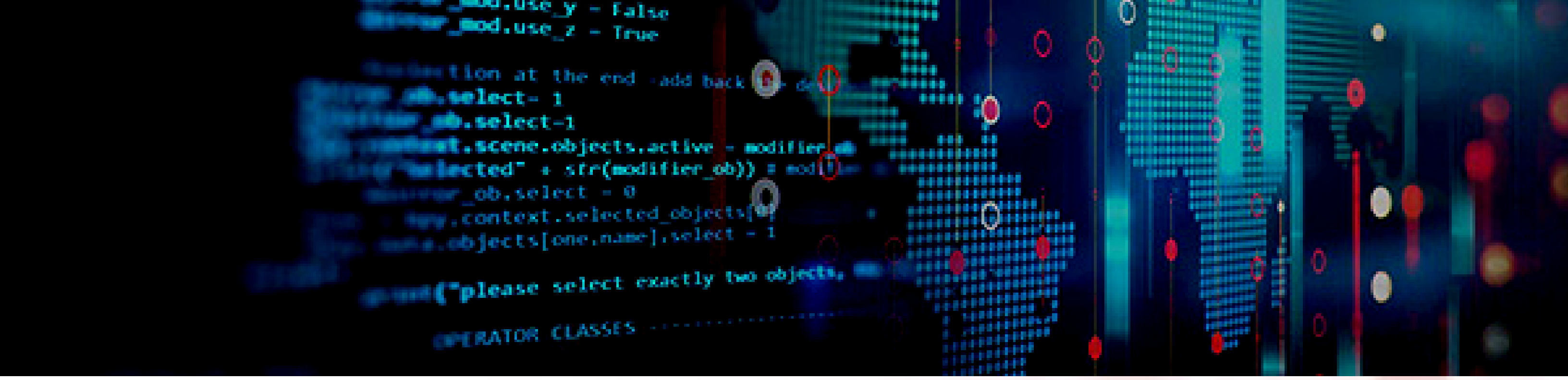
* [webapps] Croogo 3.0.2 - Remote Code Execution (Authenticated)
* [remote] Auerswald COMpact 8.0B - Multiple Backdoors
* [remote] Auerswald COMpact 8.0B - Arbitrary File Disclosure
* [remote] Auerswald COMpact 8.0B - Privilege Escalation
* [local] HCL Lotus Notes V12 - Unquoted Service Path
* [remote] Auerswald COMfortel 2.8F - Authentication Bypass
* [webapps] WordPress Plugin DZS Zoomsounds 6.45 - Arbitrary File Read (Unauthenticated)
* [webapps] WordPress Plugin Slider by Soliloquy 2.6.2 - 'title' Stored Cross Site Scripting (XSS) (Aut
* [webapps] WordPress Plugin All-in-One Video Gallery plugin 2.4.9 - Local File Inclusion (LFI)
* [webapps] Online Magazine Management System 1.0 - SQLi Authentication Bypass
* [webapps] Online Pre-owned/Used Car Showroom Management System 1.0 - SQLi Authentication Bypass
* [local] MilleGPG5 5.7.2 Luglio 2021 - Local Privilege Escalation
* [webapps] Online Enrollment Management System in PHP and PayPal 1.0 - 'U_NAME' Stored Cross-Site Scri
* [webapps] Laundry Booking Management System 1.0 - Remote Code Execution (RCE)
* [webapps] opencart 3.0.3.8 - Sessjion Injection
* [webapps] orangescrum 1.8.0 - 'Multiple' Cross-Site Scripting (XSS) (Authenticated)
* [webapps] orangescrum 1.8.0 - 'Multiple' SQL Injection (Authenticated)
* [webapps] orangescrum 1.8.0 - Privilege escalation (Authenticated)
* [webapps] Bagisto 1.3.3 - Client-Side Template Injection
* [webapps] CMSimple 5.4 - Local file inclusion (LFI) to Remote code execution (RCE) (Authenticated)
* [local] HTTPDebuggerPro 9.11 - Unquoted Service Path
* [webapps] FLEX 1085 Web 1.6.0 - HTML Injection
* [webapps] Bus Pass Management System 1.0 - 'Search' SQL injection
* [webapps] Webrun 3.6.0.42 - 'P_0' SQL Injection
* [local] Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2)

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
```

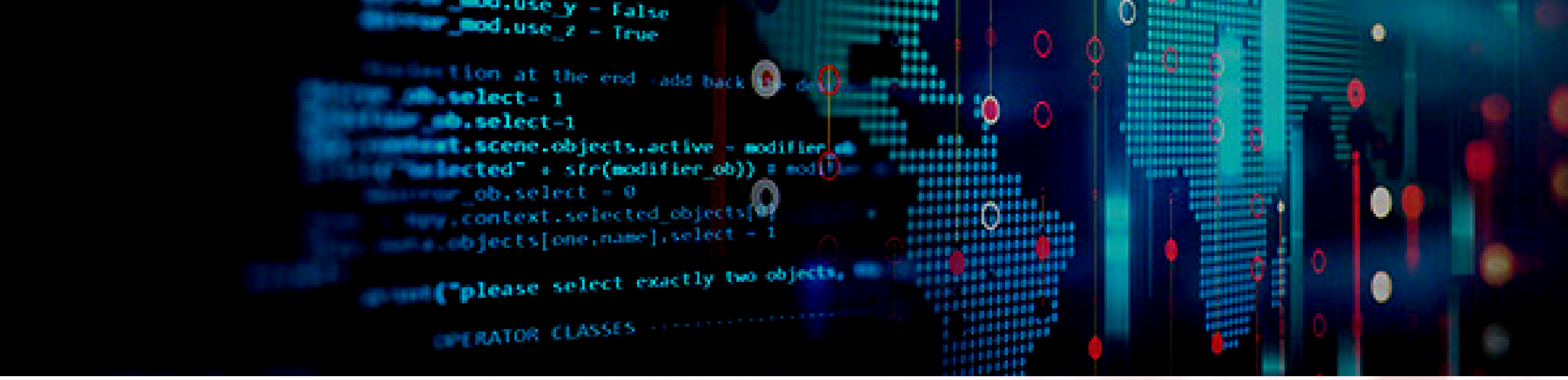
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.anticorruption.m-society.go.th
http://www.anticorruption.m-society.go.th notified by Mr.Kro0oz.305
https://dindik.ponorogo.go.id
https://dindik.ponorogo.go.id notified by Mr.Kro0oz.305
https://badegan.ponorogo.go.id
https://badegan.ponorogo.go.id notified by Mr.Kro0oz.305
https://dgec.gob.ar/readme.html
https://dgec.gob.ar/readme.html notified by 0x1998
https://www.irupi.es.gov.br
https://www.irupi.es.gov.br notified by Paran&aacute; Cyber Mafia
http://421.cd.gov.mn
http://421.cd.gov.mn notified by 0x1998
http://429.cd.gov.mn
http://429.cd.gov.mn notified by 0x1998
https://history.cd.gov.mn
https://history.cd.gov.mn notified by 0x1998
https://zavkhan.cd.gov.mn/index.php
https://zavkhan.cd.gov.mn/index.php notified by 0x1998
https://capilladelmonte.gob.ar/b4.html
https://capilladelmonte.gob.ar/b4.html notified by 0x1998
https://capilladelmonte.gov.ar/b4.html
https://capilladelmonte.gov.ar/b4.html notified by 0x1998
https://zaragoza.gob.gt/m.txt
https://zaragoza.gob.gt/m.txt notified by Panataran
https://munizaragoza.gob.gt/m.txt
https://munizaragoza.gob.gt/m.txt notified by Panataran
https://lapalma.gob.sv/m.txt
https://lapalma.gob.sv/m.txt notified by Panataran
https://chiltiupan.gob.sv/m.txt
https://chiltiupan.gob.sv/m.txt notified by Panataran
https://registrodelapropiedadpedromoncayo.gob.ec/m.txt
https://registrodelapropiedadpedromoncayo.gob.ec/m.txt notified by Panataran
http://dprd.kapuaskab.go.id/b4.html
http://dprd.kapuaskab.go.id/b4.html notified by 0x1998



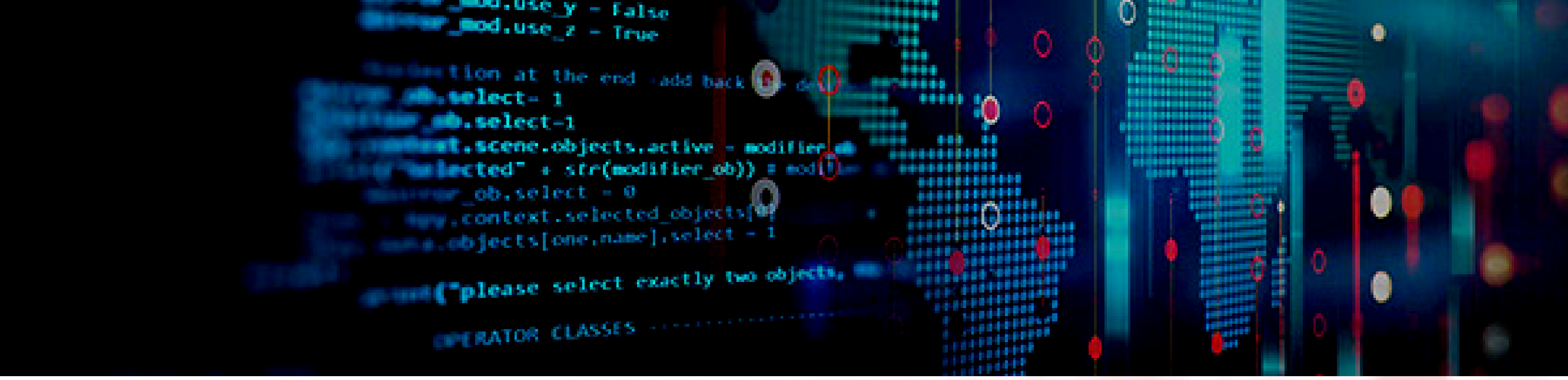
Dark Web News

Darknet Live

Three Sentenced to Prison for Selling Counterfeit Oxy Pills
Three Seattle men were sentenced to prison for producing and selling counterfeit oxycodone pills laced with fentanyl. (via darknetlive.com)
FBI Doc Highlights the Benefits of End-to-End Encryption
The FBI can obtain limited access to iMessage and WhatsApp but only metadata from other services such as Signal, according to an internal document. (via darknetlive.com)
Cannazon Market is Retiring
Cannazon, a popular marketplace for marijuana enthusiasts, will be shutting down this month. (via darknetlive.com)
Parallel Construction: The DEA Once "Stole" a Dealer's Car
This is an old tale of how the U.S. Drug Enforcement Administration used parallel construction to arrest a drug trafficker after secretly intercepting his phone calls. (via darknetlive.com)

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 &#8220;Dark web&#8221; persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that &#8220;you didn't take any shit from anyone.&#8221; During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug
Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

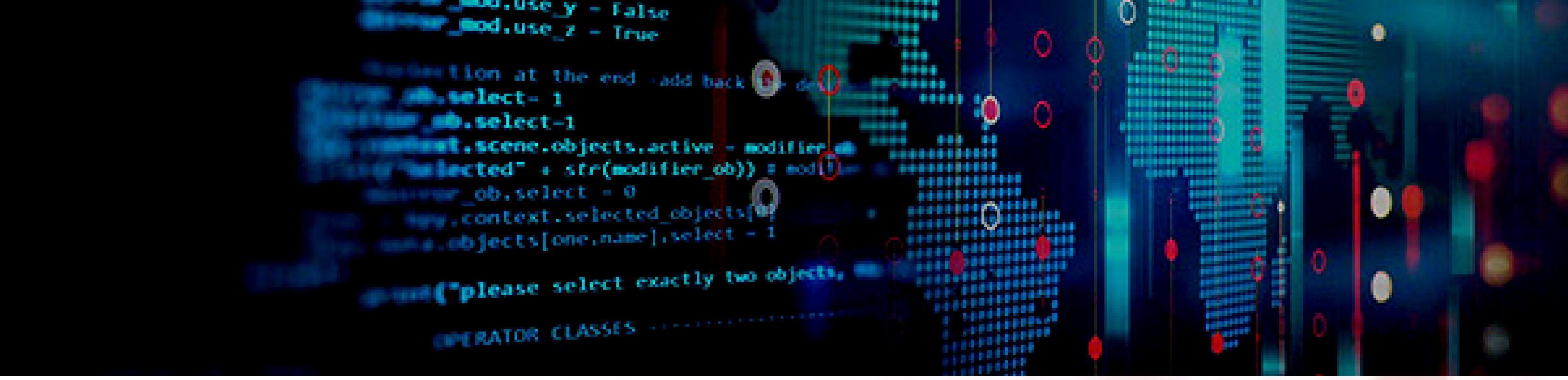
* [Our New Blog]
* [How Unsecure gRPC Implementations Can Compromise APIs, Applications]
* [XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages]
* [August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild]
* [Water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

RiskIQ

* [New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season]
* [New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses]
* [The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing]
* [Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management]
* [Discord CDN Abuse Found to Deliver 27 Unique Malware Types]
* [The Threat Landscape is Dynamic and Ever-Changing - Can You Keep Up?]
* [Mana Tools: A Malware C2 Panel with a Past]
* [What 10,000 Analysts Showed Us About the State of Threat Hunting]
* ["Bom" Skimmer is Magecart Group 7's Latest Model]
* [Untangling the Spider Web]

FireEye

* [Metasploit Wrap-Up]
* [Hacky Holidays From Rapid7! Announcing Our New Festive Blog Series]
* [OWASP Top 10 Deep Dive: Identification and Authentication Failures]
* [Ongoing Exploitation of Windows Installer CVE-2021-41379]
* [Active Exploitation of Apache HTTP Server CVE-2021-40438]
* [Metasploit Wrap-Up]
* [[Security Nation] Chris John Riley on Minimum Viable Secure Product (MVSP)]
* [OWASP Top 10 Deep Dive: Defending Against Server-Side Request Forgery]
* [The End of the Cybersecurity Skills Crisis (Maybe?)]
* [Metasploit Wrap-Up]


.use_y = False
_mod.use_z = True
tion at the end -add back
.select= 1
.select=1
.scene.objects.active = modifier
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Advisories

US-Cert Alerts & bulletins

* CISA and FBI Release Alert on Active Exploitation of CVE-2021-44077 in Zoho ManageEngine ServiceDesk
* Mozilla Releases Security Updates for Network Security Services
* NSA and CISA Release Part III of Guidance on Securing 5G Cloud Infrastructures
* CISA Adds Five Known Exploited Vulnerabilities to Catalog
* CISA Releases Capacity Enhancement Guides to Enhance Mobile Device Cybersecurity for Consumers and Or
* VMware Releases Security Updates
* Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends
* Updated: APT Exploitation of ManageEngine ADSelfService Plus Vulnerability
* AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus
* AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet V
* Vulnerability Summary for the Week of November 22, 2021
* Vulnerability Summary for the Week of November 15, 2021

Zero Day Initiative Advisories

ZDI-CAN-16073: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Qi Sun and Robert Ai of Trend Micro' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16076: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16074: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Qi Sun and Robert Ai of Trend Micro' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16075: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16084: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin

(@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15764: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15359: GE

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14733: SAP

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15484: Omron

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15730: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14868: KOYO

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-03, 3 days ago. The vendor is given until 2022-04-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15743: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Rich' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15811: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15702: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Rich' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15744: Foxit

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Rich' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15973: Microsoft]()

A CVSS score 7.8 [(AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'JeongOh Kyea with THEORI' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15586: Adobe]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Rich' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-14780: Fatek Automation]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-14735: SAP]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15903: Adobe]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15901: Adobe]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15900: Adobe]()

A CVSS score 7.8 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)]() severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-15902: 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 'Anonymous' was reported to the affected vendor on: 2021-12-01, 5 days ago. The vendor is given until 2022-03-31 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-14647: Delta Industrial Automation]()

A CVSS score 5.5 [(AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)]() severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-11-24, 12 days ago. The vendor is given until 2022-03-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Red Hat Security Advisory 2021-4827-06

Red Hat Security Advisory 2021-4827-06 - 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 a bypass vulnerability.

Red Hat Security Advisory 2021-4915-02

Red Hat Security Advisory 2021-4915-02 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4919-03

Red Hat Security Advisory 2021-4919-03 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Red Hat Security Advisory 2021-4910-03

Red Hat Security Advisory 2021-4910-03 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.8.3 RPMs.

Red Hat Security Advisory 2021-4916-01

Red Hat Security Advisory 2021-4916-01 - Mailman is a program used to help manage e-mail discussion lists. Issues addressed include bypass and cross site request forgery vulnerabilities.

Red Hat Security Advisory 2021-4799-05

Red Hat Security Advisory 2021-4799-05 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.6.51. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-4914-06

Red Hat Security Advisory 2021-4914-06 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains the following OpenShift Virtualization 4.8.3 images: RHEL-8-CNV-4.8.

Red Hat Security Advisory 2021-4918-03

Red Hat Security Advisory 2021-4918-03 - A minor version update is now available for Red Hat Camel K that includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, denial of service, deserialization, information leakage, privilege escalation, and server-side request forgery vulnerabilities.

CA Network Flow Analysis SQL Injection

CA Technologies is alerting customers to a vulnerability in CA Network Flow Analysis (NFA). A vulnerability exists that can allow an authenticated user to perform SQL injection attacks and access sensitive data. CA published solutions to address this vulnerability and recommends that all affected customers implement these solutions. The vulnerability occurs due to insufficient input validation. An authenticated user can potentially access sensitive data. CA Network Flow Analysis versions 9.3.8, 9.5, 10.0, 10.0.2, 10.0.3, 10.0.4, 10.0.5, 10.0.6, 10.0.7, and 21.2.1 are affected.

Red Hat Security Advisory 2021-4909-03

Red Hat Security Advisory 2021-4909-03 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Red Hat Security Advisory 2021-4907-04

Red Hat Security Advisory 2021-4907-04 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Red Hat Security Advisory 2021-4902-06

Red Hat Security Advisory 2021-4902-06 - The release of RHACS 3.67 provides the following new features, bug fixes, security patches and system changes: OpenShift Dedicated support RHACS 3.67 is thoroughly tested and supported on OpenShift Dedicated on Amazon Web Services and Google Cloud Platform. 1. Use OpenShift OAuth server as an identity provider If you are using RHACS with OpenShift, you can now configure the built-in OpenShift OAuth server as an identity provider for RHACS. Issues addressed include denial of service, information leakage, memory exhaustion, remote shell upload, and traversal vulnerabilities.

Red Hat Security Advisory 2021-4903-05

Red Hat Security Advisory 2021-4903-05 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Red Hat Security Advisory 2021-4904-05

Red Hat Security Advisory 2021-4904-05 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Ubuntu Security Notice USN-5168-3

Ubuntu Security Notice 5168-3 - USN-5168-1 fixed a vulnerability in NSS. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Tavis Ormandy discovered that NSS incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5168-1

Ubuntu Security Notice 5168-1 - Tavis Ormandy discovered that NSS incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause NSS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5168-2

Ubuntu Security Notice 5168-2 - Tavis Ormandy discovered that NSS, included with Thunderbird, incorrectly handled verifying DSA/RSA-PSS signatures. A remote attacker could use this issue to cause Thunderbird to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2021-4801-06

Red Hat Security Advisory 2021-4801-06 - 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 4.7.38. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-5164-1

Ubuntu Security Notice 5164-1 - It was discovered that the Option USB High Speed Mobile device driver in the Linux kernel did not properly handle error conditions. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. 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.

Ubuntu Security Notice USN-5165-1

Ubuntu Security Notice 5165-1 - It was discovered that the NFC subsystem in the Linux kernel contained a use-after-free vulnerability in its NFC Controller Interface implementation. A local attacker could possibly use this to cause a denial of service or execute arbitrary code. It was discovered that the SCTP protocol implementation in the Linux kernel did not properly verify VTAGs in some situations. A remote attacker could possibly use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-5163-1

Ubuntu Security Notice 5163-1 - 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 Option USB High Speed Mobile device driver in the Linux kernel did not properly handle error conditions. A physically proximate 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 2021-4861-06

Red Hat Security Advisory 2021-4861-06 - 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 5.6.0 serves as a replacement for Red Hat JBoss Web Server 5.5.0. This release includes bug fixes, enhancements and component upgrades, which are documented in the Release Notes, linked to in the References. Issues addressed include HTTP request smuggling and denial of service vulnerabilities.

Red Hat Security Advisory 2021-4866-02

Red Hat Security Advisory 2021-4866-02 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Red Hat Security Advisory 2021-4859-03

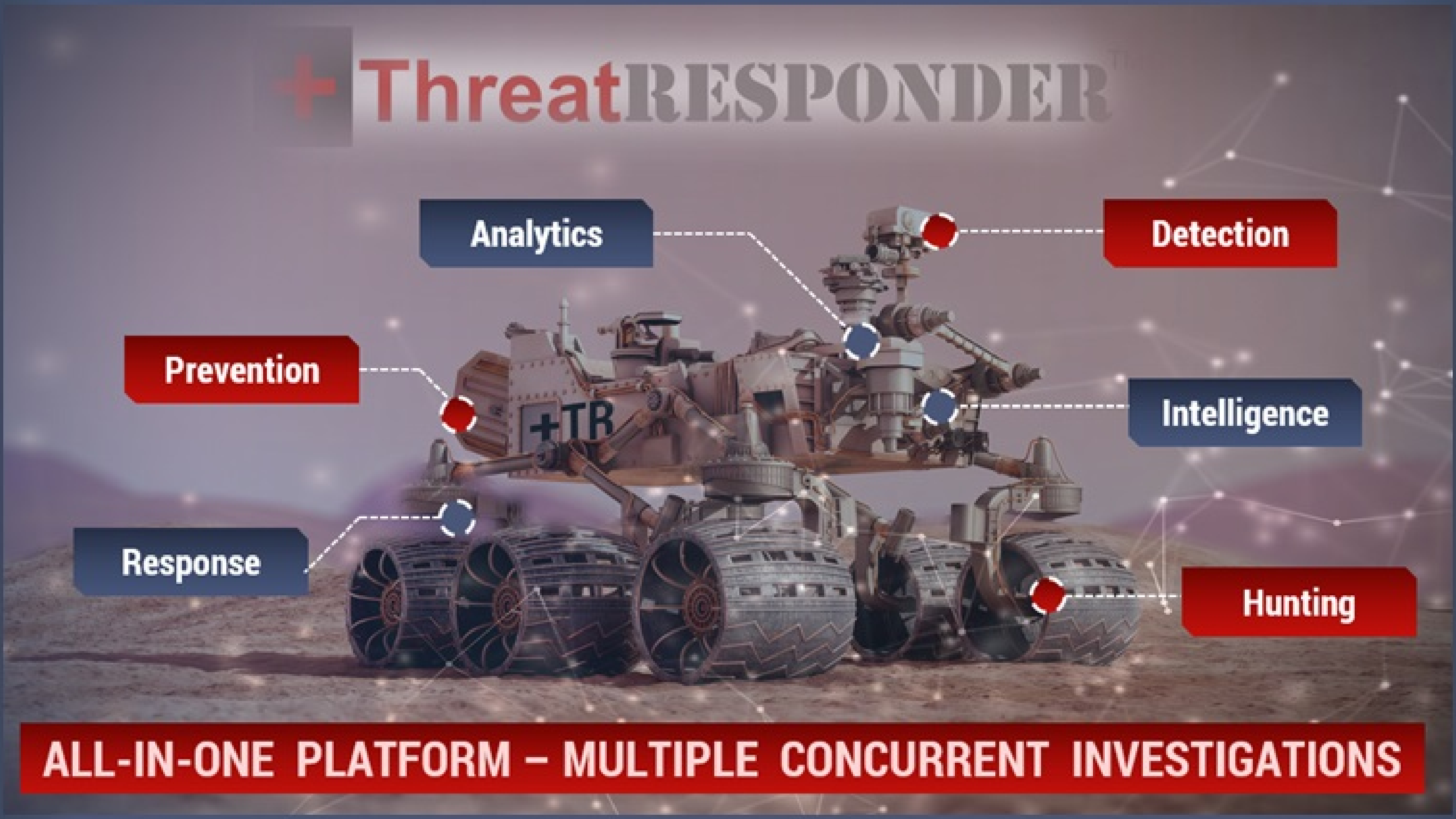
Red Hat Security Advisory 2021-4859-03 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

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



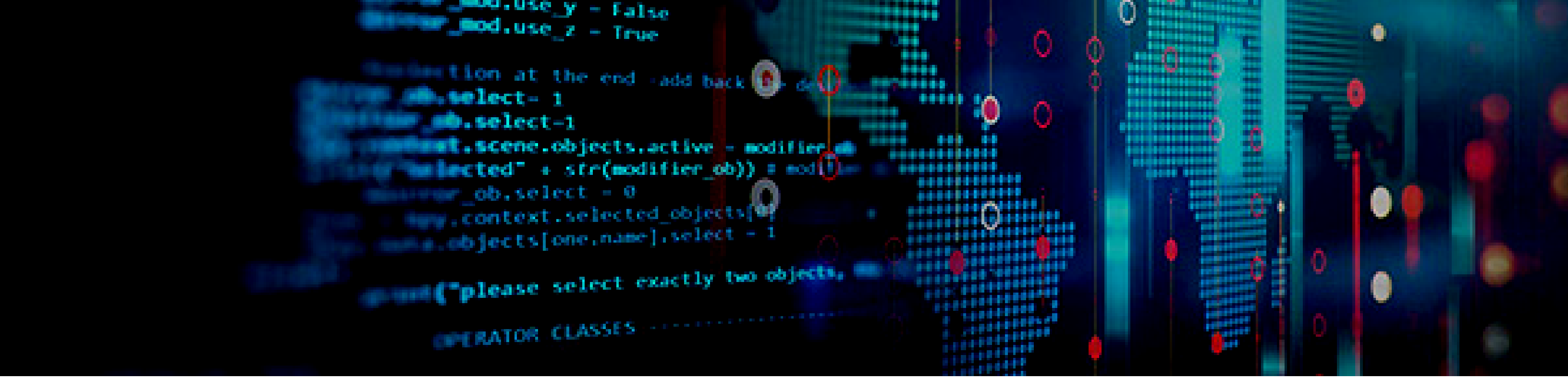
The Solution – ThreatResponder® Platform

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

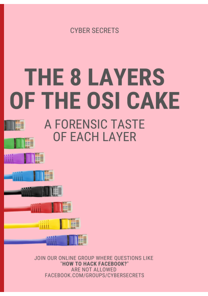


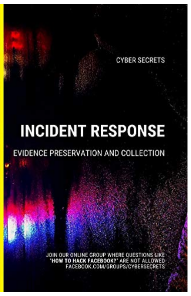
The Cyber Secrets publications on Amazon

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.

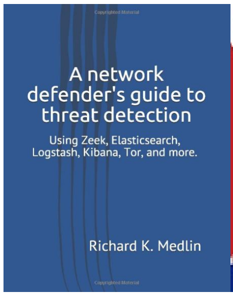
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

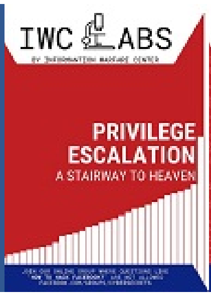
CYBER Secrets
Information Warfare Center
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training

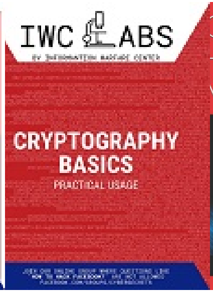


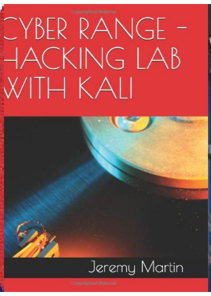


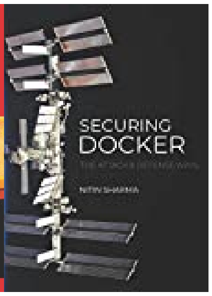
Other Publications from Information Warfare Center











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