Aug-09-21

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

CYBER WEEKLY AWARENESS REPORT

August 9, 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

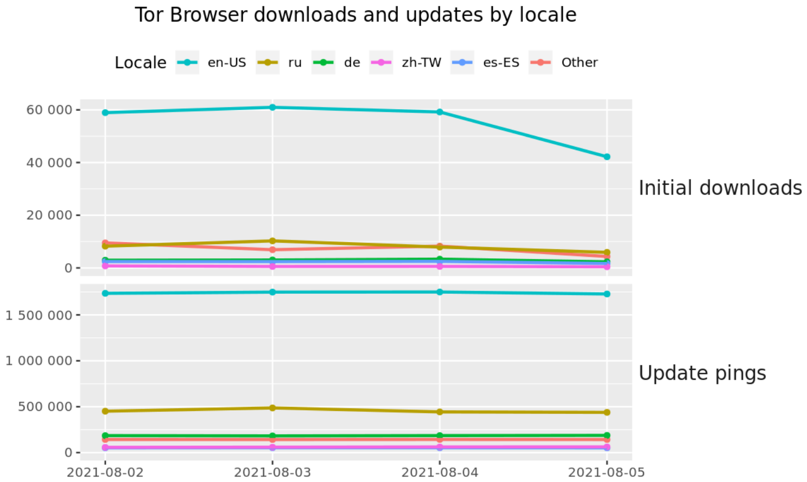
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

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



Tor Browser downloads and updates by locale

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

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

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* StarHub Suffers Data Breach, But Says No System Was Compromised
* Apple Plans To Scan US iPhones For Child Sexual Abuse Images
* South Korea To Test Grenade Launching Drones
* MacOS Flaw In Telegram Retrieves Deleted Messages
* Black Hat: BadAlloc Bugs Expose Millions Of IoT Devices To Hijack
* Critical Cobalt Strike Bug Leaves Botnet Servers Vulnerable To Takedown
* Black Hat: Let's All Help Cyber Immunize Each Other
* Black Hat: Security Bugs Allow Takeover Of Capsule Hotel Rooms
* TechScape: Why Hacker Summer Camp And Pandemics Don't Mix
* Raccoon Stealer Bundles Malware, Propagates Via Google SEO
* Four US Agencies Earned A D In Cybersecurity
* SEC Chair Wants To Regulate Cryptocurrency
* Iranian APT Lures Defense Contractor In Catfishing-Malware Scam
* Supply Chain Attacks Are Getting Worse, And You Are Not Ready For Them
* DeadRinger: Chinese APTs Strike Major Telecom Companies
* Check Out The Newly Discovered Tetraquark
* PwnedPiper Outlines Devastating Bugs In More Than 80% Of Hospital Pneumatics
* CISA Launches Own Vulnerability Disclosure Program
* Microsoft Warns Of Sneakier Than Usual Phishing Attack
* SolarWinds Attackers Breached Email Of US Prosecutors, Says Department Of Justice
* Novel Meteor Wiper Used In Attack That Crippled Iranian Train System
* Vultur Bank Malware Infests Thousands Of Devices
* Cisco Researchers Spotlight Solarmarker Malware
* Security Team Finds Crimea Manifesto Buried In VBA Rat
* Inside The Bitcoin Mine With Its Own Power Plant

Krebs on Security

* Ransomware Gangs and the Name Game Distraction
* The Life Cycle of a Breached Database
* PlugwalkJoe Does the Perp Walk
* Serial Swatter Who Caused Death Gets Five Years in Prison
* Spam Kingpin Peter Levashov Gets Time Served
* Don't Wanna Pay Ransom Gangs? Test Your Backups.
* Microsoft Patch Tuesday, July 2021 Edition
* Spike in "Chain Gang" Destructive Attacks on ATMs
* Kaseya Left Customer Portal Vulnerable to 2015 Flaw in its Own Software
* Microsoft Issues Emergency Patch for Windows Flaw

LATEST NEWS

Dark Reading

* FragAttacks Foil 2 Decades of Wireless Security
* Researchers Call for 'CVE' Approach for Cloud Vulnerabilities
* HTTP/2 Implementation Errors Exposing Websites to Serious Risks
* CISA Launches JCDC, the Joint Cyber Defense Collaborative
* Incident Responders Explore Microsoft 365 Attacks in the Wild
* Researchers Find Significant Vulnerabilities in macOS Privacy Protections
* A New Approach to Securing Authentication Systems' Core Secrets
* Organizations Still Struggle to Hire & Retain Infosec Employees: Report
* Why Supply Chain Attacks Are Destined to Escalate
* New Normal Demands New Security Leadership Structure
* Multiple Zero-Day Flaws Discovered in Popular Hospital Pneumatic Tube System
* 8 Security Tools to be Unveiled at Black Hat USA
* Biden Administration Responds to Geopolitical Cyber Threats
* 7 Hot Cyber Threat Trends to Expect at Black Hat
* Law Firm for Ford, Pfizer, Exxon Discloses Ransomware Attack
* US Accuses China of Using Criminal Hackers in Cyber Espionage Operations
* How Gaming Attack Data Aids Defenders Across Industries
* NSO Group Spyware Used On Journalists & Activists Worldwide
* When Ransomware Comes to (Your) Town
* 7 Ways AI and ML Are Helping and Hurting Cybersecurity

The Hacker News

* Pulse Secure VPNs Get New Urgent Update for Poorly Patched Critical Flaw
* Apple to Scan Every Device for Child Abuse Content - But Experts Fear for Privacy
* New Amazon Kindle Bug Could've Let Attackers Hijack Your eBook Reader
* India's Koo, a Twitter-like Service, Found Vulnerable to Critical Worm Attacks
* VMware Issues Patches to Fix Critical Bugs Affecting Multiple Products
* Salesforce Release Updates - A Cautionary Tale for Security Teams
* A Wide Range of Cyber Attacks Leveraging Prometheus TDS Malware Service
* Unpatched Security Flaws Expose Mitsubishi Safety PLCs to Remote Attacks
* Cisco Issues Critical Security Patches to Fix Small Business VPN Router Bugs
* Several Malware Families Targeting IIS Web Servers With Malicious Modules
* Russian Federal Agencies Were Attacked With Chinese Webdav-O Virus
* New Chinese Spyware Being Used in Widespread Cyber Espionage Attacks
* Critical Flaws Affect Embedded TCP/IP Stack Widely Used in Industrial Control Devices
* Chinese Hackers Target Major Southeast Asian Telecom Companies
* Cynet Empowers IT Resellers and Service Providers to Become Fully Qualified MSSPs

LATEST NEWS

Security Week

- * Threat Detection Provider ReversingLabs Raises $56 Million
- * New DNS Attack Enables 'Nation-State Level Spying' via Domain Registration
- * VMware Patches Severe Vulnerability in Workspace ONE Access, Identity Manager
- * Black Hat 2021: Microsoft Wins Worst of Pwnie Awards
- * Critical Code Execution Vulnerability Patched in Pulse Connect Secure
- * Prometheus TDS - Underground Service Distributing Several Malware Families
- * Analysis of ICS Exploits Can Help Defenders Prioritize Vulnerability Remediation
- * 'Sophisticated Group' Behind Alaska Cyberattack, Agency Says
- * Black Hat 2021: New CISA Boss Unveils Anti-Ransomware Collab With Big Tech
- * Tech Titans Join US Cyber Team to Fight Ransomware
- * U.S. Infrastructure Bill Allocates $2 Billion to Cybersecurity
- * Microsoft Launches JIT-Free 'Super Duper Secure Mode' Edge Browser Experiment
- * Iran-Linked Hackers Expand Arsenal With New Android Backdoor
- * Cisco Patches Critical Vulnerability in Small Business VPN Routers
- * China-Linked Cyberespionage Operation Suggests Interest in SCADA Systems
- * Security is a Big Data Problem, and It's Getting Bigger
- * Researchers Analyze Chinese Malware Used Against Russian Government
- * Oregon Examines Spyware Investment Amid Controversy
- * Black Hat Keynote: Mobile Platforms 'Actively Obstructing' Zero-Day Malware Hunters
- * Senate Report: Federal Agencies Still Have Poor Cybersecurity Practices
- * Advanced Technology Ventures Discloses Ransomware Attack
- * New CISA and NSA Guidance Details Steps to Harden Kubernetes Systems
- * ICS Vendors Address Vulnerabilities Affecting Widely Used Licensing Product
- * Chinese Cyberspy Group APT31 Starts Targeting Russia

Infosecurity Magazine

Unfortunately, at the time of this report, the Infosecuroty Magazine resource was not availible.

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Your KnowBe4 Fresh Content Updates from July
* 12 Steps to a Security Ignorance Program
* BEC Attacks Are Targeting Lower-Level Employees
* Open Source Intelligence (OSINT): Learn the Methods Bad Actors Use to Hack Your Organization
* 79% of Employees Have Knowingly Engaged in Risky Online Activities in the Past Year
* You Knew It Would Eventually Happen: Ransomware Lawsuits
* Egress: 73% of Orgs Were Victims of Phishing Attacks in the Last Year
* CyberheistNews Vol 11 #30 [Eye Opener] Image Inversion as a New Phishing Technique
* Ransomware Extortion Attacks Continue to Rise in Frequency as Ransom Payments Decrease by 40%
* Phishing Attacks Target IT Professionals More Than Any Other Organizational Role

ISC2.org Blog

* Cybersecurity Leaders: Think in Business Terms
* READY To Celebrate Global Achievement Award Winners?
* READY for What's New at (ISC)&sup2; Security Congress in 2021?
* Relevance Requires More than Just Paying Attention
* The Role of Culture in Compliance

HackRead

* Apple's neuralMatch tool will scan iPhones for child abuse content
* Someone pubished Conti ransomware gang's sensitive insider data online
* Lead generation firm exposed household data of 63 million Americans
* How to Protect Your CRM Information from Security Threats
* Defunct marketing firm exposed 32GB worth of records, customers data
* WhatsApp Introduces View Once Feature for Videos and Photos
* Fake Brave browser website dropped malware, thanks to Google Ads

Koddos

* Apple's neuralMatch tool will scan iPhones for child abuse content
* Someone pubished Conti ransomware gang's sensitive insider data online
* Lead generation firm exposed household data of 63 million Americans
* How to Protect Your CRM Information from Security Threats
* Defunct marketing firm exposed 32GB worth of records, customers data
* WhatsApp Introduces View Once Feature for Videos and Photos
* Fake Brave browser website dropped malware, thanks to Google Ads

LATEST NEWS

Naked Security

* S3 Ep44: Unreported holes, retro computing, and tech support for malware [Podcast]
* Conti ransomware affiliate goes rogue, leaks "gang data"
* "Cobalt Strike" network attack tool patches crashtastic server bug
* BazarCaller - the malware gang that talks you into infecting yourself
* S3 Ep43: Apple 0-day, pygmy hippos, hive nightmares and Twitter hacker bust [Podcast]
* Microsoft researcher found Apple 0-day in March, didn't report it
* Apple emergency zero-day fix for iPhones and Macs - get it now!
* Windows "PetitPotam" network attack - how to protect against it
* US court gets UK Twitter hack suspect arrested in Spain
* S3 Ep42: Viruses, Nightmares, patches, rewards and scammers [Podcast]

Threat Post

* Golang Cryptomining Worm Offers 15% Speed Boost
* Amazon Kindle Vulnerable to Malicious EBooks
* Critical Cisco Bug in VPN Routers Allows Remote Takeover
* Zoom Settlement: An $85M Business Case for Security Investment
* Angry Affiliate Leaks Conti Ransomware Gang Playbook
* Black Hat: New CISA Head Woos Crowd With Public-Private Task Force
* Auditors: Feds' Cybersecurity Gets the Dunce Cap
* MacOS Flaw in Telegram Retrieves Deleted Messages
* Black Hat: Microsoft's Patch for Windows Hello Bypass Bug is Faulty, Researchers Say
* Black Hat: Charming Kitten Leaves More Paw Prints

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

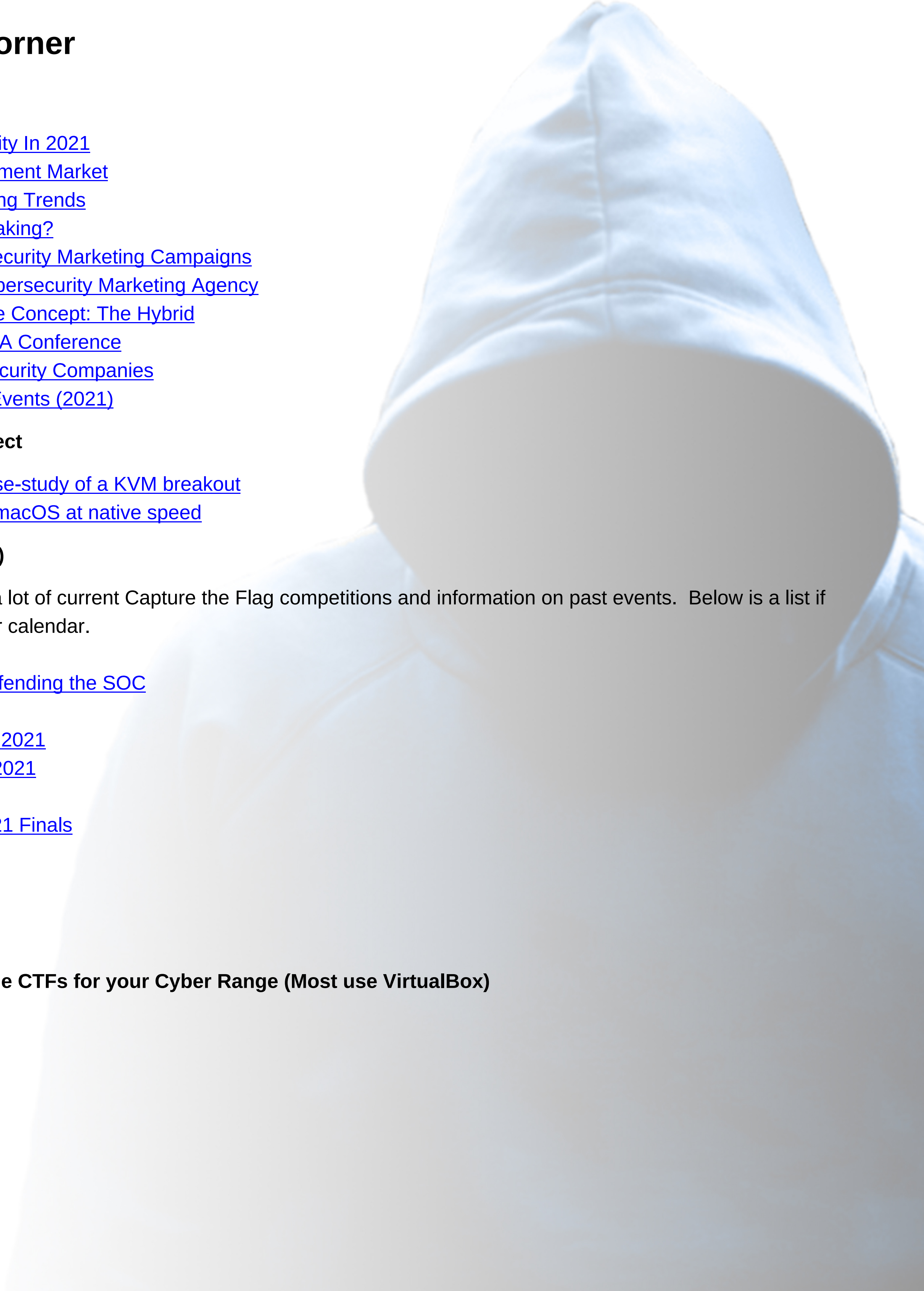
* Spend Wisely (Not Just More) to Become Cyber Resilient
* ITG18: Operational Security Errors Continue to Plague Sizable Iranian Threat Group
* 5 Ways to Increase Password Safety
* Building Effective Business Cases to Cover Cybersecurity Costs
* July 2021 Security Intelligence Roundup: Ransomware, Security by Design and How to Analyze in Windows
* Data Breach Costs at Record High, Zero Trust, AI and Automation Help Reduce Costs
* What's New in the 2021 Cost of a Data Breach Report
* Double Encryption: When Ransomware Recovery Gets Complicated
* How AI Will Transform Data Security
* API Abuse Is a Data Security Issue Here to Stay

InfoWorld

* How to screw up data migration to the cloud
* JDK 17: The new features in Java 17
* What's new in Rust 1.54
* What's new in Kubernetes 1.22
* Developers love Rust and Svelte, dread AngularJS, Stack Overflow survey says
* How to work with Azure Queue Storage in C#
* How to choose a cloud database
* Oracle launches Verrazzano container platform for Kubernetes
* Debugging concurrent code with Coyote
* Eclipse Temurin Java SE binaries debut

C4ISRNET - Media for the Intelligence Age Military

* Commandant calls on senior Marines to stop 'shackling' junior leaders
* Corps' sergeant major calls for improved treatment, care of junior Marines
* Space-based optical communications: updating SATCOM for the information age
* Is expeditionary foraging in the Corps' future?
* Northrop Grumman, Ball Aerospace clear milestone for missile warning payload
* Autonomous systems to help NATO examine climate change effects in Arctic waters
* DoD pledges militarywide alignment on electromagnetic spectrum ops
* Putin's push for isolated internet will shift the Russian cyber landscape
* The Space Force wants to manage acquisitions by portfolio
* US Coast Guard updates cyber plans to reflect rapid threat changes



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

* 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.

* RCTS CERT 2021 Defending the SOC
* InCTF 2021
* Really Awesome CTF 2021
* Hacker's Playground 2021
* corCTF 2021
* Midnight Sun CTF 2021 Finals
* YauzaCTF 2021
* FwordCTF 2021
* WORMCON 0x01
* ALLES! CTF 2021

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

* Hack Me Please: 1
* Corrosion: 1
* ContainMe: 1
* Hms?: 1
* doli: 1

Tools & Techniques

Packet Storm Security Tools Links

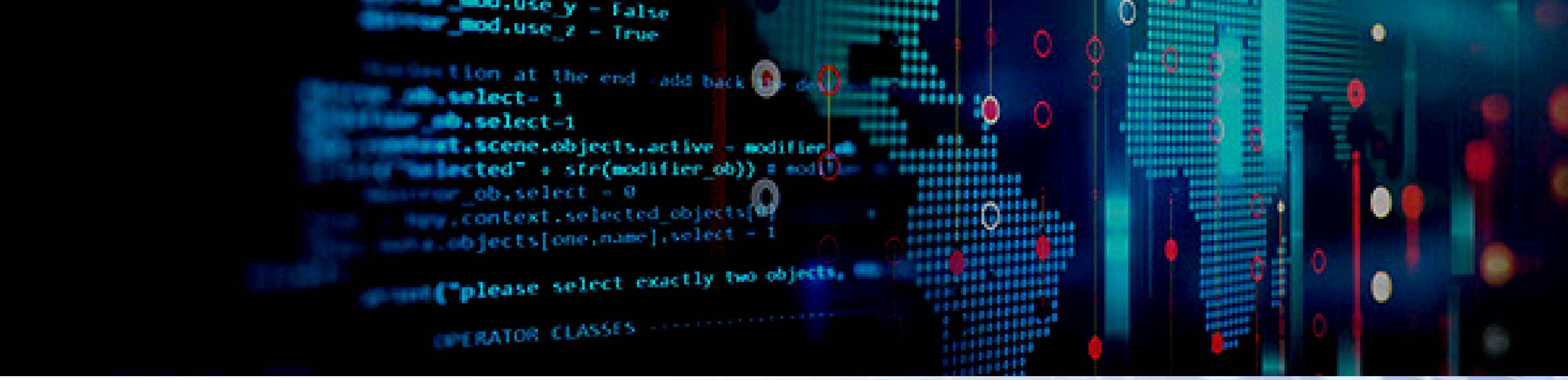
* SQLMAP - Automatic SQL Injection Tool 1.5.8
* Logwatch 7.5.6
* Lynis Auditing Tool 3.0.6
* American Fuzzy Lop plus plus 3.14c
* Hashcat Advanced Password Recovery 6.2.3 Source Code
* Hashcat Advanced Password Recovery 6.2.3 Binary Release
* Wireshark Analyzer 3.4.7
* UFONet 1.7
* Global Socket 1.4.33
* Zeek 4.0.3

Kali Linux Tutorials

* Uchihash : A Small Utility To Deal With Malware Embedded Hashes
* SharpLAPS : Retrieve LAPS Password From LDAP
* Doldrums : A Flutter/Dart Reverse Engineering Tool
* Rz-Ghidra : Deep Ghidra Decompiler And Sleigh Disassembler Integration For Rizin
* Domhttpx : A Google Search Engine Dorker With HTTP Toolkit Built With Python, Can Make It Easier For
* PowerShell Armoury : A PowerShell Armoury For Security Guys And Girls
* TSharkVM : TShark + ELK Analytics Virtual Machine
* CSIRT-Collect : PowerShell Script To Collect Memory And (Triage) Disk Forensics
* Cerbrutus : Network Brute Force Tool, Written In Python
* Ruse : Mobile Camera-Based Application That Attempts To Alter Photos To Preserve Their Utility To Hum

GBHackers Analysis

* SolarWinds Actors Hacked 27 State Attorneys' Offices in the U.S.
* Critical Oracle Weblogic Flaw Let Remote Attacker Take Control of The System
* Millions of Printers Worldwide Vulnerable To The 16-Year-Old Bug
* Russian APT Hackers Launched A Mass Global Brute Force Attack to Hack Enterprise & Cloud Networks
* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Getting started in DFIR: Testing 1,2,3
* DFIR Summit 2021
* STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign
* FOR585: Smartphone Forensic Analysis In-Depth

Defcon Conference

* DEF CON 29 - Vivek Nair - Time Turner Hacking RF Attendance Systems To Be in Two Places at Once
* DEF CON 29 - Hao Xing, Zekai Wu - How I use a JSON 0day to Steal Your Money on the Blockchain
* DEF CON 29 - Rion Carter - Why does my security camera scream like a Banshee?
* DEF CON 29 - Jeff Dileo - Instrument and Find Out: Parasitic Tracers for High Level Languages

Hak5

* Chat with the OMG Dev Team
* Hak5 LIVE: 16th Anniversary Celebration
* HakByte: Capture Wi-Fi Passwords From Smartphones with a Half-Handshake Attack

The PC Security Channel [TPSC]

* Discord Ransomware
* Windows 11: Better Security?

Eli the Computer Guy

* eBeggar Wednesday - HEMAN is a BLACK WOMAN edition
* Cyber Security Introduction
* Hacking Introduction
* "Easy" Computer Speech Recognition with Azure Cognitive Services and Python

Security Now

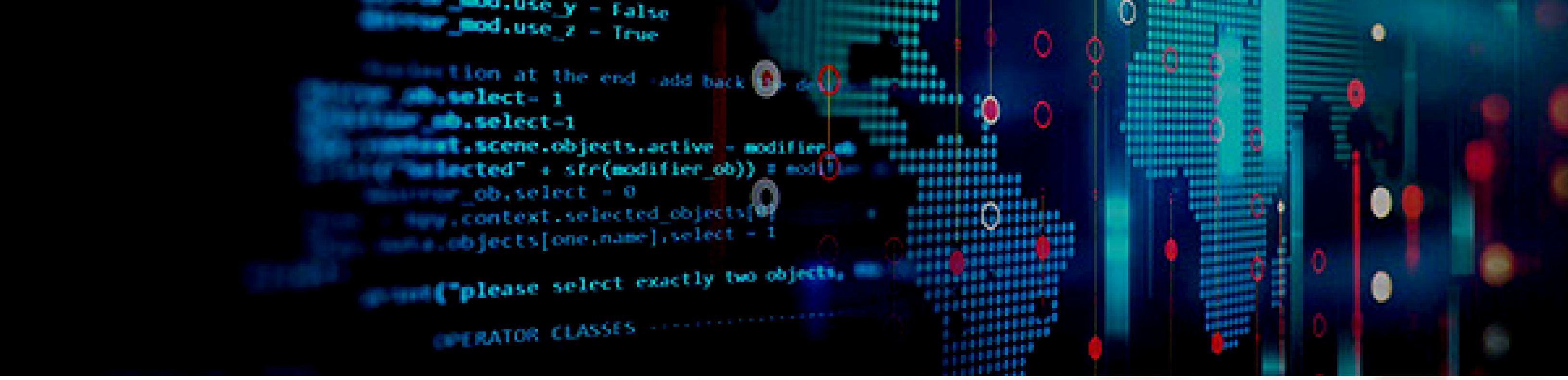
* The BlackMatter Interview - Bad News for Firefox, DarkSide Return, Tailscale, Google to Assume HTTPS
* SeriousSAM & PetitPotam - Kaseya Universal Decryptor, Window's Process Hacker, Chrome 92

Troy Hunt

* Weekly Update 255

Intel Techniques: The Privacy, Security, & OSINT Show

* 228-New Privacy & OSINT Strategies
* 227-Eleven Topics



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

* Bear Tracks: Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers
* New Analysis Shows XAMPP Serving Agent Tesla and Formbook Malware
* Taking a Closer Look at a Malicious Infrastructure Mogul
* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* 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

FireEye

* Metasploit Wrap-Up
* Black Hat 2021: Rapid7 Experts Share Key Day 2 Takeaways
* Slot Machines and Cybercrime: Why Ransomware Won't Quit Pulling Our Lever
* Black Hat 2021: Rapid7 Experts Share Key Day 1 Takeaways
* [Security Nation] Richard Kaufmann on Cybersecurity in Home Healthcare
* PetitPotam: Novel Attack Chain Can Fully Compromise Windows Domains Running AD CS
* The Ransomware Task Force: A New Approach to Fighting Ransomware
* [The Lost Bots] Episode 2: Extended Detection and Response (XDR)
* 3 Steps to Integrate Rapid7 Products Into the DevSecOps Cycle
* Metasploit Wrap-Up

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Backdoor.Win32.Zaratustra Remote File Write / Code Execution
* Backdoor.Win32.Zdemon.126 Remote Command Execution
* Backdoor.Win32.Zdemon.10 Remote Command Execution
* Trojan-Dropper.Win32.Small.fp Unauthenticated Open Proxy
* Constructor.Win32.SS.11.c Unauthenticated Open Proxy
* Amica Prodigy 1.7 Privilege Escalation
* GFI Mail Archiver 15.1 Arbitrary File Upload
* Moodle 3.9 Remote Code Execution
* CMSuno 1.7 Cross Site Scripting
* qdPM 9.2 Information Disclosure
* Client Management System 1.1 Cross Site Scripting
* Riak Insecure Default Configuration / Remote Command Execution
* WordPress WP Customize Login 1.1 Cross Site Scripting
* Apache OfBiz 17.12.01 Remote Command Execution
* Hotel Management System 1.0 Cross Site Scripting / Shell Upload
* Packet Storm New Exploits For July, 2021
* Online Hotel Reservation System 1.0 Cross Site Scripting
* Neo4j 3.4.18 Remote Code Execution
* Men Salon Management System 1.0 SQL Injection
* Pi-Hole Remove Commands Linux Privilege Escalation
* Panasonic Sanyo CCTV Network Camera 2.03-0x Cross Site Request Forgery
* ObjectPlanet Opinio 7.13 Shell Upload
* ObjectPlanet Opinio 7.13 Expression Language Injection
* ObjectPlanet Opinio 7.13 / 7.14 XML Injection
* Microsoft Exchange AD Schema Misconfiguration Privilege Escalation

CXSecurity

* GFI Mail Archiver 15.1 Telerik UI Component Arbitrary File Upload (Unauthenticated)
* GFI Mail Archiver 15.1 Arbitrary File Upload
* Moodle 3.9 Remote Code Execution
* ApacheOfBiz 17.12.01 Remote Command Execution
* Pi-Hole Remove Commands Linux Privilege Escalation
* PHP 7.3.15-3 PHP_SESSION_UPLOAD_PROGRESS Session Data Injection
* NoteBurner 2.35 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

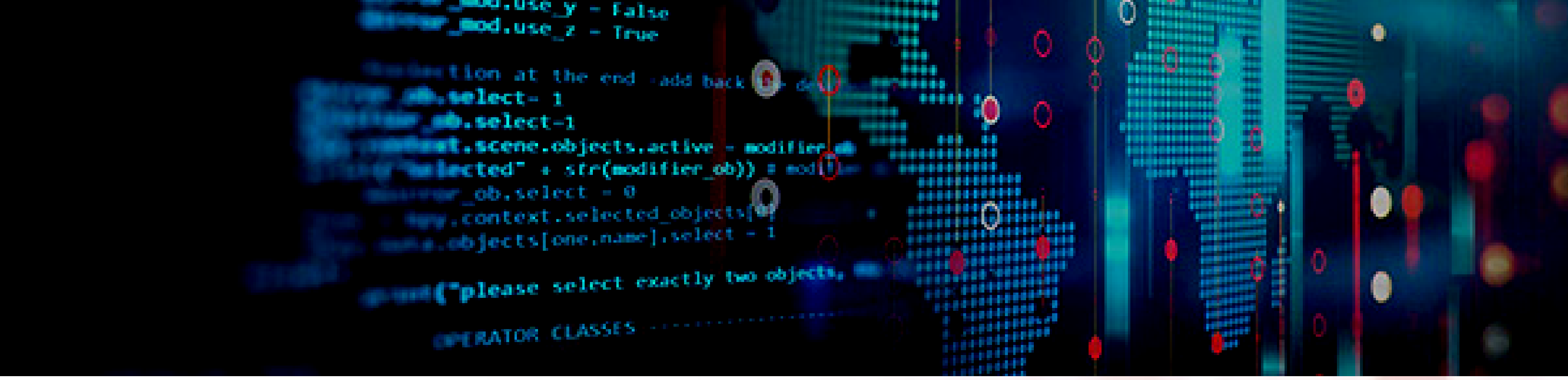
* [webapps] GFI Mail Archiver 15.1 - Telerik UI Component Arbitrary File Upload (Unauthenticated)
* [webapps] Moodle 3.9 - Remote Code Execution (RCE) (Authenticated)
* [webapps] CMSuno 1.7 - 'tgo' Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] ApacheOfBiz 17.12.01 - Remote Command Execution (RCE) via Unsafe Deserialization of XMLRPC
* [webapps] Client Management System 1.1 - 'cname' Stored Cross-site scripting (XSS)
* [webapps] qdPM 9.2 - DB Connection String and Password Exposure (Unauthenticated)
* [webapps] qdPM 9.1 - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin WP Customize Login 1.1 - 'Change Logo Title' Stored Cross-Site Scripting (
* [webapps] Hotel Management System 1.0 - Cross-Site Scripting (XSS) Arbitrary File Upload Remote Code
* [webapps] Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CS
* [webapps] Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)
* [remote] Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)
* [webapps] Men Salon Management System 1.0 - SQL Injection Authentication Bypass
* [webapps] Oracle Fatwire 6.3 - Multiple Vulnerabilities
* [webapps] CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)
* [webapps] Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection
* [webapps] IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration
* [webapps] Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download
* [webapps] Denver IP Camera SHO-110 - Unauthenticated Snapshot
* [webapps] TripSpark VEO Transportation - Blind SQL Injection
* [remote] Denver Smart Wifi Camera SHC-150 - 'Telnet' Remote Code Execution (RCE)
* [webapps] Event Registration System with QR Code 1.0 - Authentication Bypass & RCE
* [webapps] Customer Relationship Management System (CRM) 1.0 - Sql Injection Authentication Bypass
* [webapps] PHP 7.3.15-3 - 'PHP_SESSION_UPLOAD_PROGRESS' Session Data Injection

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
```

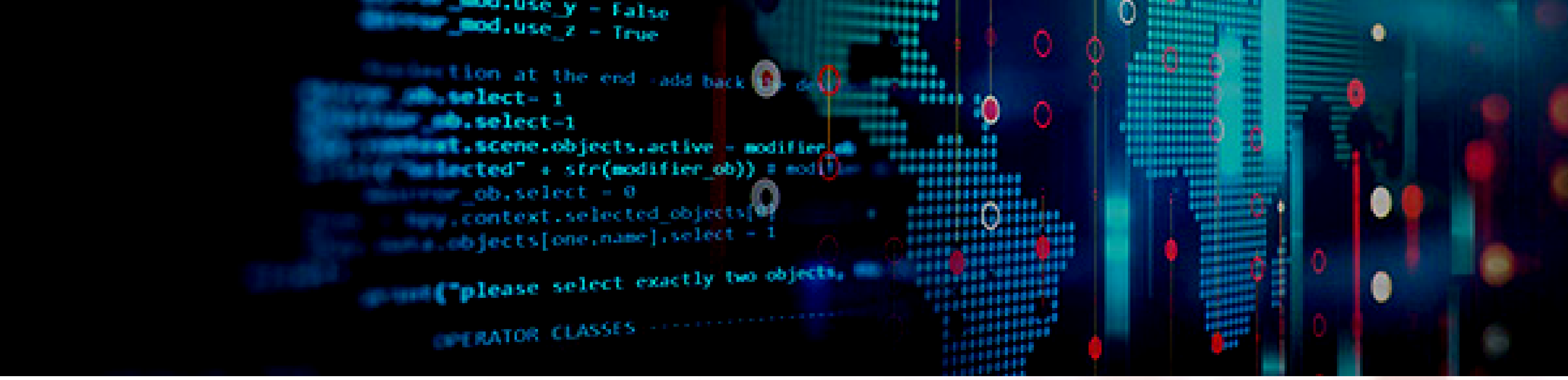
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

Unfortunately, at the time of this report, the Zone-H.org last hacked feed was not availible.


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

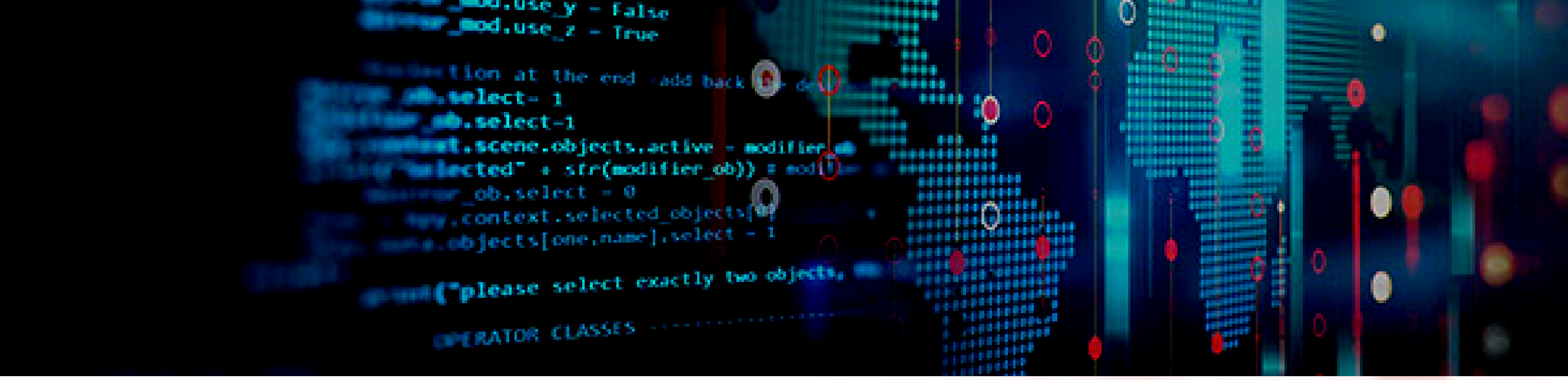
Dark Web News

Darknet Live

Apple to Scan iPhones for Child Abuse Content
The concern is that governments will eventually use this to catch their ideological opponents (or drug users). (via darknetlive.com)
Prescription Vendor "Pillpusher" Pleads Guilty to Drug Charges
A Georgia man pleaded guilty to distributing prescription drugs through the darkweb under the username "Pillpusher.&rdquo; (via darknetlive.com)
Opioid Vendor "Fentmaster" Sentenced to 15 Years in Prison
The infamous AlphaBay vendor "Fentmaster&rdquo; will spend the next 180 months in prison for selling opioids through the darkweb. (via darknetlive.com)
Student Caught with 23 Kilos of MDMA Heads to Prison
A master's student in France is heading to prison for selling MDMA to customers on darkweb markets. (via darknetlive.com)

Dark Web Link

Data Laundering Fakes Security, Privacy Risks
Data laundering, just like money laundering, is the process of obtaining data through illegal means, such as the dark web or a stolen/hacked database, and then passing it through a legitimate business or process to make it appear authentic. There are more avenues to gather and force data as both companies and customer bases familiarise [...] The post Data Laundering Fakes Security, Privacy Risks appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Fake Covid Passport, The Newest Call For Dark Web Criminals
The law was followed, and the snare was set. We first saw it during pandemics with the illegal sale of masks and medical supplies. Then there were drugs ostensibly effective against the coronavirus, as well as the sale of ostensibly effective vaccines on the dark web. Now it's the covid passport's turn. Countries from Europe [...] The post Fake Covid Passport, The Newest Call For Dark Web Criminals appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Coronavirus: How The Black Market Of Covid Certificates Works
The first tourist to visit our country this year was a 65-year-old Russian who was treated in a Coronavirus Intensive Care Unit.He arrived in Greece on May 29 with a 72-hour negative PCR test, as required by current legislation; however, the fact that he developed symptoms the same day he arrived and was hospitalised three [...] The post Coronavirus: How The Black Market Of Covid Certificates Works appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


.select-1
.scene.objects.active = modifier_ob
_ob.select = 0
("please select exactly two objects,
OPERATOR CLASSES

Advisories

US-Cert Alerts & bulletins

* Ivanti Releases Security Update for Pulse Connect Secure
* CISA Releases Security Advisory for InterNiche Products
* VMware Releases Security Updates for Multiple Products
* Cisco Releases Security Updates&#8239;
* Google Releases Security Updates for Chrome
* CISA Releases Security Advisory for Swisslog Healthcare
* CISA and NSA Release Kubernetes Hardening Guidance
* CISA Announces Vulnerability Disclosure Policy (VDP) Platform
* AA21-209A: Top Routinely Exploited Vulnerabilities
* AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013
* Vulnerability Summary for the Week of July 26, 2021
* Vulnerability Summary for the Week of July 19, 2021

Zero Day Initiative Advisories

ZDI-CAN-14539: NetBSD
A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14695: Bentley
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 'Francis Provencher {PRL}' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14808: NetBSD
A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14538: FreeBSD
A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14807: NetBSD
A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the

release of a public advisory.

ZDI-CAN-14809: NetBSD

A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-09, 0 days ago. The vendor is given until 2021-12-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14571: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14574: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14420: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14572: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14421: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14573: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14413: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14422: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14423: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14658: 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 'ZhangJiaxing(@r0fm1a) from Codesafe Team of Legendsec at Qi'anxin Group' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14419: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14408: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14569: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14417: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14411: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14410: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14886: Microsoft

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N) severity vulnerability discovered by 'Simon Zuckerbraun - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-14570: WECON

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-05, 4 days ago. The vendor is given until 2021-12-03 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-5032-1
Ubuntu Security Notice 5032-1 - Several vulnerabilities were fixed in Docker. This update provides a new upstream version that fixed them.

Red Hat Security Advisory 2021-3020-01
Red Hat Security Advisory 2021-3020-01 - 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 code execution vulnerability.

Red Hat Security Advisory 2021-3015-01
Red Hat Security Advisory 2021-3015-01 - Go Toolset provides the Go programming language tools and libraries. Go is alternatively known as golang. The go-toolset packages have been updated to version 1.15.14.

Ubuntu Security Notice USN-5031-1
Ubuntu Security Notice 5031-1 - It was discovered that openCryptoki incorrectly handled certain EC keys. An attacker could possibly use this issue to cause a invalid curve attack.

Ubuntu Security Notice USN-5027-2
Ubuntu Security Notice 5027-2 - USN-5027-1 fixed a vulnerability in PEAR. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5030-1
Ubuntu Security Notice 5030-1 - It was discovered that the Perl DBI module incorrectly opened files outside of the folder specified in the data source name. A remote attacker could possibly use this issue to obtain sensitive information. It was discovered that the Perl DBI module incorrectly handled certain long strings. A local attacker could possibly use this issue to cause the DBI module to crash, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. Various other issues were also addressed.

Red Hat Security Advisory 2021-3001-01
Red Hat Security Advisory 2021-3001-01 - Windows Container Support for Red Hat OpenShift allows you to deploy Windows container workloads running on Windows Server containers.

Red Hat Security Advisory 2021-2998-01
Red Hat Security Advisory 2021-2998-01 - The glibc packages provide the standard C libraries, POSIX thread libraries, standard math libraries, and the name service cache daemon used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2993-01
Red Hat Security Advisory 2021-2993-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2021-2992-01
Red Hat Security Advisory 2021-2992-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. Issues addressed include bypass, null pointer, and server-side request forgery vulnerabilities.

Ubuntu Security Notice USN-5029-1
Ubuntu Security Notice 5029-1 - It was discovered that GnuTLS incorrectly handled sending certain extensions when being used as a client. A remote attacker could use this issue to cause GnuTLS to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5028-1
Ubuntu Security Notice 5028-1 - It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2021-2989-01
Red Hat Security Advisory 2021-2989-01 - The lasso packages provide the Lasso library that implements the Liberty Alliance Single Sign-On standards, including the SAML and SAML2 specifications. It allows handling of the whole life-cycle of SAML-based federations and provides bindings for multiple languages.

Red Hat Security Advisory 2021-2988-01

Red Hat Security Advisory 2021-2988-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Ubuntu Security Notice USN-5026-2

Ubuntu Security Notice 5026-2 - USN-5026-1 fixed several vulnerabilities in QPDF. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to consume resources, resulting in a denial of service. It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2965-01

Red Hat Security Advisory 2021-2965-01 - Red Hat Single Sign-On 7.4 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.4.8 serves as a replacement for Red Hat Single Sign-On 7.4.7, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a cross site scripting vulnerability.

Ubuntu Security Notice USN-5026-1

Ubuntu Security Notice 5026-1 - It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to consume resources, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5027-1

Ubuntu Security Notice 5027-1 - It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5025-2

Ubuntu Security Notice 5025-2 - USN-5025-1 fixed a vulnerability in libsndfile. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5025-1

Ubuntu Security Notice 5025-1 - It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-4944-2

Ubuntu Security Notice 4944-2 - USN-4944-1 fixed vulnerabilities in MariaDB. It caused a regression. This update fixes the problem. Ubuntu 20.04 has been updated to MariaDB 10.3.30.

Ubuntu Security Notice USN-5024-1

Ubuntu Security Notice 5024-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Red Hat Security Advisory 2021-2932-01

Red Hat Security Advisory 2021-2932-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, and out of bounds read vulnerabilities.

Red Hat Security Advisory 2021-2931-01

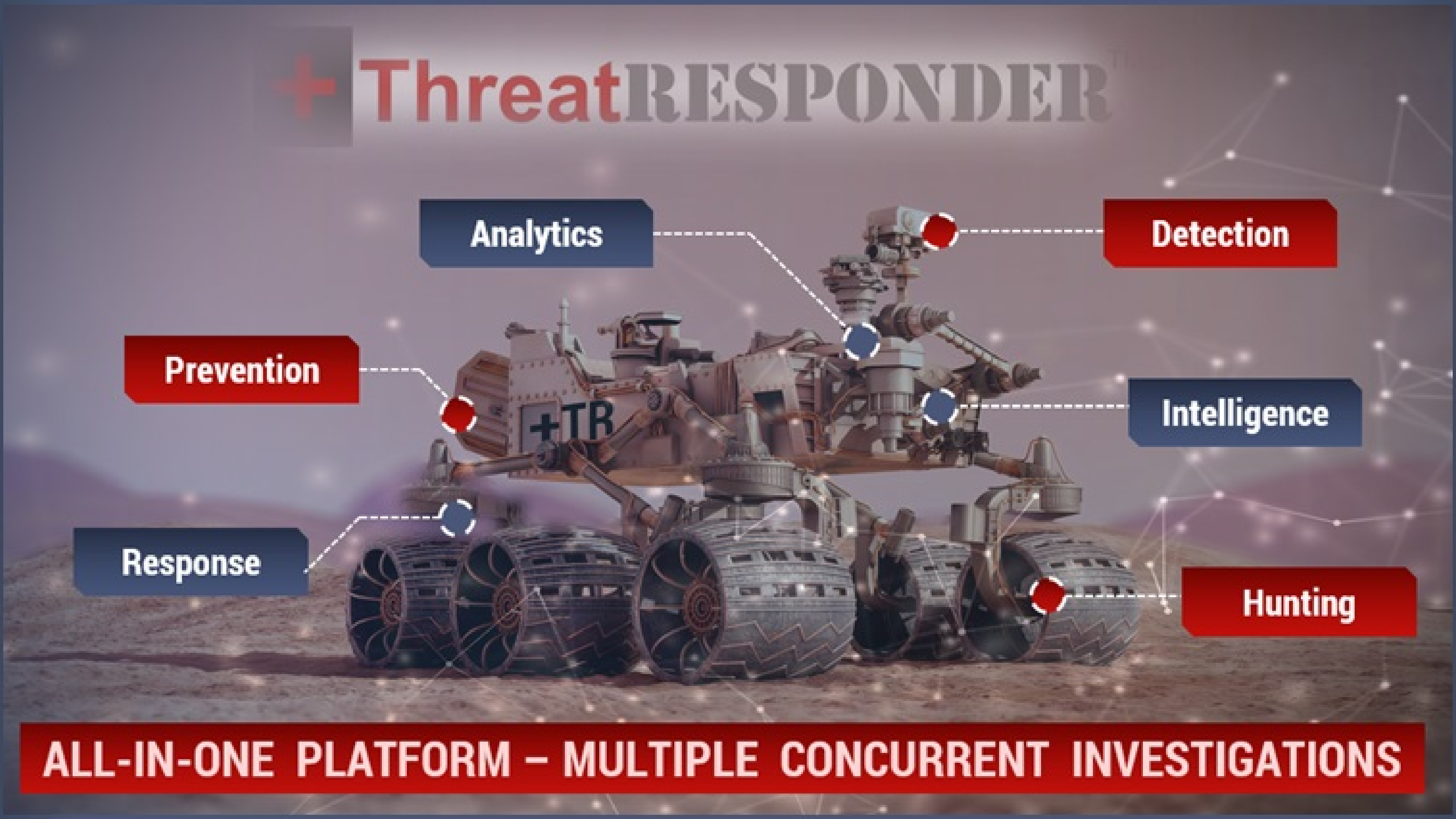
Red Hat Security Advisory 2021-2931-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, and out of bounds read vulnerabilities.

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

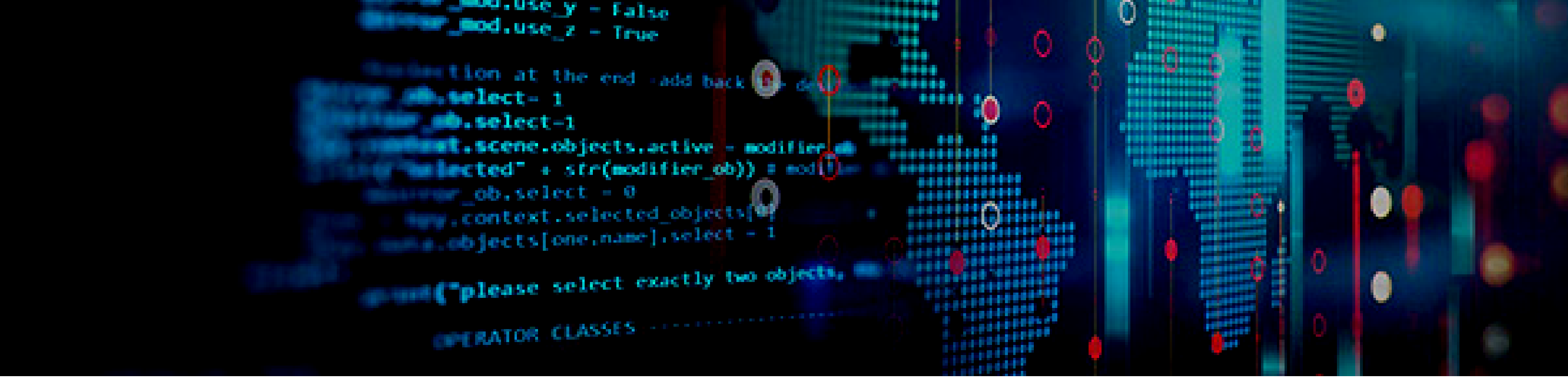
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

* Cyber Secrets on Amazon - amzn.to/2UuIG9B

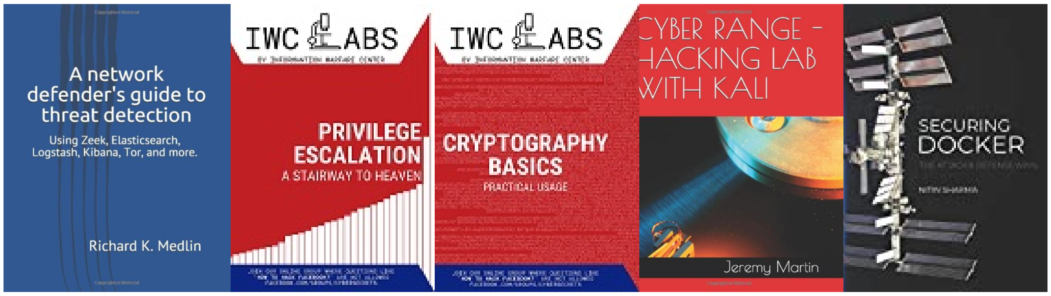


The Cyber Secrets publications on Amazon

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