Sep-13-21

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

Si LINUX

ARGOS
APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

September 13, 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

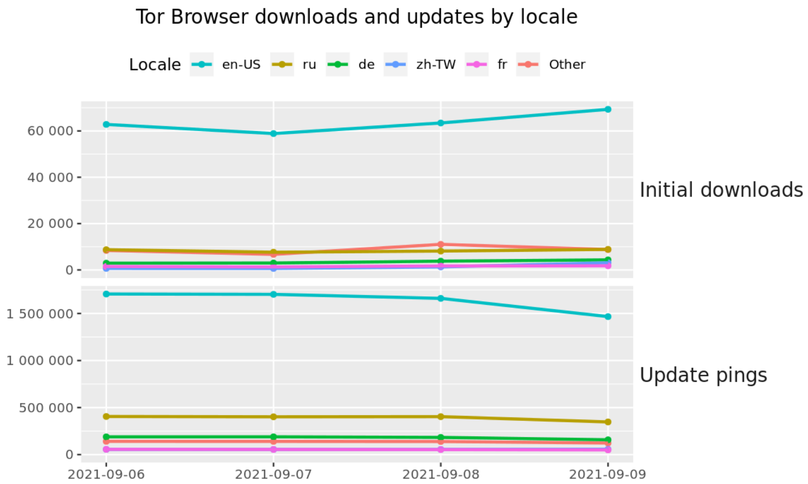
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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



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

* Attackers Exploit MSHTML Browser Engine Via ActiveX Controls
* Thousands Of Fortinet VPN Account Credentials Leaked
* Hacker Lawyer Jay Leiderman Is Dead At 50
* Infosec Researchers Say Apple's Bug Bounty Program Needs Work
* TeamTNT Hacking Group Strikes Thousands Of Victims Worldwide
* Ransomware Attack Hits Howard University
* ProtonMail Under Fire After Police Data Handover
* Netgear Smart Switches Open To Complete Takeover
* Bitcoin Becomes Legal Tender In El Salvador
* IoT Attacks Skyrocket, Doubling In Six Months
* Report: This Is The Perfect Ransomware Victim
* Outlook Shows Real Contact Info For Spoofed IDNs
* Ransomware That Avoids Russian Speakers Gets 90% Of Payments
* Apple Hits Pause On Controversial CSAM Detection Feature
* Banksy Was Warned About Website Flaw Before NFT Hack Scam
* FTC Orders SpyFone To Delete All Of Its Surveillance Data
* NPM Package With 3 Million Weekly Downloads Had A Severe Vuln
* WhatsApp Patches Vulnerability Related To Image Filter Functionality
* Comcast RF Attack Leveraged Remotes For Surveillance
* WhatsApp Issued Second Largest GDPR Fine Of 225 Million Euro
* This Lightning Cable Will Leak Everything You Type
* This Is Why The Mozi Botnet Will Linger On
* Fake Banksy NFT Sold Through Artist's Website For Â£244k
* Cream Finance Platform Pilfered For Over $34 Million In Cryptocurrency
* Feds Warn Of Ransomware Attacks Ahead Of Labor Day

Krebs on Security

* KrebsOnSecurity Hit By Huge New IoT Botnet "Meris"
* Microsoft: Attackers Exploiting Windows Zero-Day Flaw
* "FudCo" Spam Empire Tied to Pakistani Software Firm
* Gift Card Gang Extracts Cash From 100k Inboxes Daily
* 15-Year-Old Malware Proxy Network VIP72 Goes Dark
* Man Robbed of 16 Bitcoin Sues Young Thieves' Parents
* Wanted: Disgruntled Employees to Deploy Ransomware
* T-Mobile: Breach Exposed SSN/DOB of 40M+ People
* T-Mobile Investigating Claims of Massive Data Breach
* New Anti Anti-Money Laundering Services for Crooks

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

* New SpookJs Attack Bypasses Google Chrome's Site Isolation Protection
* M&#275;ris Botnet Hit Russia's Yandex With Massive 22 Million RPS DDoS Attack
* WhatsApp to Finally Let Users Encrypt Their Chat Backups in the Cloud
* Moving Forward After CentOS 8 EOL
* SOVA: New Android Banking Trojan Emerges With Growing Capabilities
* Experts Link Sidewalk Malware Attacks to Grayfly Chinese Hacker Group
* Microsoft Warns of Cross-Account Takeover Bug in Azure Container Instances
* Russian Ransomware Group REvil Back Online After 2-Month Hiatus
* Fighting the Rogue Toaster Army: Why Secure Coding in Embedded Systems is Our Defensive Edge
* Hackers Leak VPN Account Passwords From 87,000 Fortinet FortiGate Devices
* CISA Warns of Actively Exploited Zoho ManageEngine ADSelfService Vulnerability
* 3 Ways to Secure SAP SuccessFactors and Stay Compliant
* HAProxy Found Vulnerable to Critical HTTP Request Smuggling Attack
* Experts Uncover Mobile Spyware Attacks Targeting Kurdish Ethnic Group
* [Ebook] The Guide for Speeding Time to Response for Lean IT Security Teams

LATEST NEWS

Security Week

* Cybersecurity Seen as Rising Risk for Airlines After 9/11
* M&#275;ris Botnet Flexes Muscles With 22 Million RPS DDoS Attack
* Google Introduces Private Compute Services for Android
* ProtonMail (Wrongly?) Criticized for Disclosing User IP to Authorities
* Cisco Patches High-Severity Security Flaws in IOS XR
* HAProxy Vulnerability Leads to HTTP Request Smuggling
* GitHub Patches Security Flaws in Core Node.js Dependencies
* Understanding the Cryptocurrency-Ransomware Connection
* Mastercard to Acquire Blockchain Analytics Firm CipherTrace
* Hacking the Hire: Three Ways to Recruit and Retain Cyber Talent
* Three Ways to Keep Cloud Data Safe From Attackers
* US Gov Seeks Public Feedback on Draft Federal Zero Trust Strategy
* Canadian-US National Sentenced to Prison for Cybercrime Schemes
* Microsoft Warns of Information Leak Flaw in Azure Container Instances
* Get Ready for PYSA Ransomware Attacks Against Linux Systems
* Is the Taliban a Cyber Threat to the West?
* TrueFort Raises $30 Million to Grow Application Protection Platform
* Zoho Confirms Zero-Day Authentication Bypass Attacks
* Howard University Cancels Classes, Shuts Campus After Ransomware Attack
* Google Android Security Update Patches 40 Vulnerabilities
* CISA Reminds of Risks Connected to Managed Service Providers
* The Impact of the Pandemic on Today's Approach to Cybersecurity
* US-built Databases a Potential Tool of Taliban Repression
* Critical Flaw in Pac-Resolver NPM Package Affects 290,000 Repositories

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

* Wanting to Stream the Italian Grand Prix This Weekend? It Might Be a Scam.
* Five Signs of Social Engineering
* A Look at Phishing Keywords
* The Number of Daily Ransomware Attacks Increase Nearly 1000% in 2021
* The Amount of Weekly New Phishing URLs Has Grown Nearly 2.5x Since 2020
* BEC, Fraud, and Ransomware Attacks Are All on the Rise and Costing More Than Ever
* Phishing for the German Bundestag
* [FREE COURSES] Two New Training Modules are Now Available to Support Cybersecurity Awareness Month
* CyberheistNews Vol 11 #35 [Heads Up] When the URL Domain Is Not Enough To Avoid That Phish
* Windows 11 Phishbait by Active Threat Group Now Delivers Malware

ISC2.org Blog

* Are You the Keymaster?
* Mastering Identity and Access Management in the Cloud
* Want a Cybersecurity Job? Keep Up with Industry Developments
* CISSPs from Around the Globe: An Interview with James Wright
* Do You Hire Cyber Pros? Let's Talk!

HackRead

* Experts concerned over emergence of new Android banking trojan S.O.V.A.
* Yandex hit by largest DDoS attack involving 200,000 hacked devices
* What are endpoint security threats, and how can they enter your device?
* Microsoft warns of Azure vulnerability which exposed users to data theft
* Hackers dump login credentials of Fortinet VPN users in plain-text
* Malware droppers for hire targeting users on fake pirated software sites
* REvil ransomware gang is back after disappearing amid Kaseya attack

Koddos

* Experts concerned over emergence of new Android banking trojan S.O.V.A.
* Yandex hit by largest DDoS attack involving 200,000 hacked devices
* What are endpoint security threats, and how can they enter your device?
* Microsoft warns of Azure vulnerability which exposed users to data theft
* Hackers dump login credentials of Fortinet VPN users in plain-text
* Malware droppers for hire targeting users on fake pirated software sites
* REvil ransomware gang is back after disappearing amid Kaseya attack

LATEST NEWS

Naked Security

* S3 Ep49: Poison PACs, pointless alarms and phunky bugs [Podcast]
* Windows zero-day MSHTML attack - how not to get booby trapped!
* Poisoned proxy PACs! The NPM package with a network-wide security hole&hellip;
* S3 Ep48: Cryptographic bugs, cryptocurrency nightmares, and lots of phishing [Podcast]
* Pwned! The home security system that can be hacked with your email address
* Skimming the CREAM - recursive withdrawals loot $13M in cryptocash
* Big bad decryption bug in OpenSSL - but no cause for alarm
* S3 Ep47: Daylight robbery, spaghetti trouble, and mousetastic superpowers [Podcast]
* How a gaming mouse can get you Windows superpowers!
* What's *THAT* on my 3D printer? Cloud bug lets anyone print to everyone

Threat Post

* MyRepublic Data Breach Raises Data-Protection Questions
* Top Steps for Ransomware Recovery and Preparation
* Yandex Pummeled by Potent Meris DDoS Botnet
* SOVA, Worryingly Sophisticated Android Trojan, Takes Flight
* 5 Steps For Securing Your Remote Work Space
* Stolen Credentials Led to Data Theft at United Nations
* Thousands of Fortinet VPN Account Credentials Leaked
* McDonald's Email Blast Includes Password to Monopoly Game Database
* Financial Cybercrime: Why Cryptocurrency is the Perfect 'Getaway Car'
* 'Azurescape' Kubernetes Attack Allows Cross-Container Cloud Compromise

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

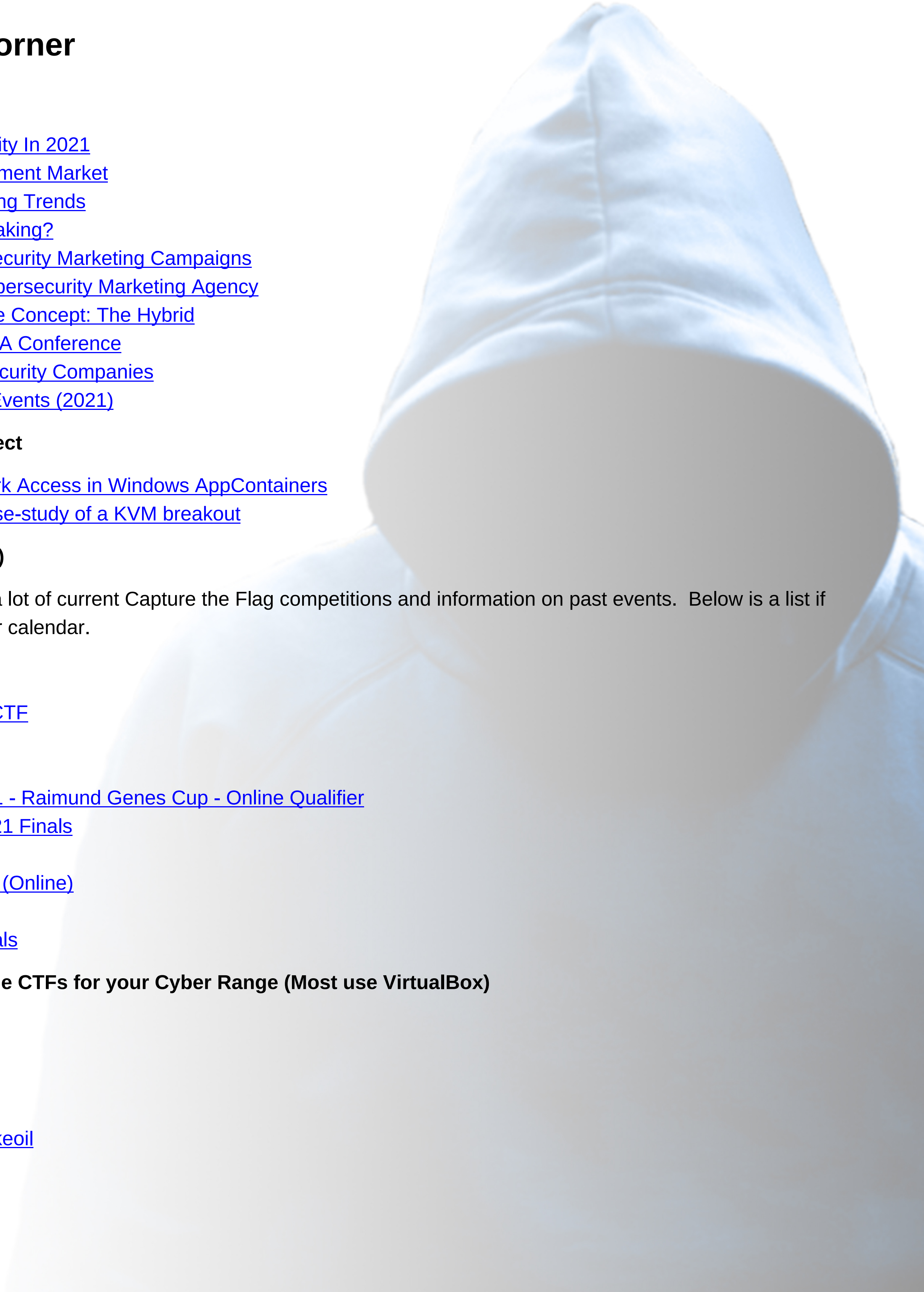
* Private 5G Security: Consider Security Risks Before Investing
* How Companies Can Prepare for Botnet Attacks on APIs
* 5 Ways to Use Microlearning to Educate Your Employees About Cybersecurity
* LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment
* Where Digital Meets Human: Letting HR Lead Cybersecurity Training
* The Post-Quantum Cryptography World Is Coming: Here's How to Prepare
* Building Blocks: How to Create a Privileged Access Management (PAM) Strategy
* Fighting Cyber Threats With Open-Source Tools and Open Standards
* Dissecting Sodinokibi Ransomware Attacks: Bringing Incident Response and Intelligence Together in the
* What Biden's Cybersecurity Executive Order Means for Supply Chain Attacks

InfoWorld

* Google Flutter 2.5 UI kit is now stable
* How to get a maxed-out cloud budget
* Java internet address resolution plan proposed
* Why devops teams should eliminate SLAs
* JetBrains previews data science IDE
* The lines between private data centers and public clouds are blurring
* Understanding Azure Virtual Networks
* How Docker broke in half
* Open source is selfish
* Microsoft open-sources Java garbage collection analyzer

C4ISRNET - Media for the Intelligence Age Military

* Pentagon taps industry for nuclear-powered propulsion for its satellites
* Israeli, British firms to deliver unmanned vehicles for UK experimental program
* Old systems and talent shortages pose new barriers to DOD data sharing
* To win battles of information, the US Army will need deep sensing and data handling
* How the Pentagon's joint IT provider will contribute to JADC2
* US Army to kick off mobile communications pilot for armored brigades
* US Army works through what 'information advantage' is and how to achieve it
* Lack of access to data during Afghanistan exit shines light on tech gap
* US Navy launches Mideast drone task force amid Iran tensions
* Space Force expects $1 billion in contracts in first year of Space Enterprise Consortium Reloaded



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

* Understanding Network Access in Windows AppContainers
* An EPYC escape: Case-study of a KVM breakout

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.

* VolgaCTF 2021 Final
* H@cktivityCon 2021 CTF
* PBjar CTF '21
* Overflow To Fall
* Trend Micro CTF 2021 - Raimund Genes Cup - Online Qualifier
* Midnight Sun CTF 2021 Finals
* Sunshine CTF 2021
* DownUnderCTF 2021 (Online)
* ChaffCTF 2021
* 0CTF/TCTF 2021 Finals

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

* Beelzebub: 1
* Vikings: 1
* DarkHole: 2
* Deathnote: 1
* digitalworld.local: snakeoil

Tools & Techniques

Packet Storm Security Tools Links

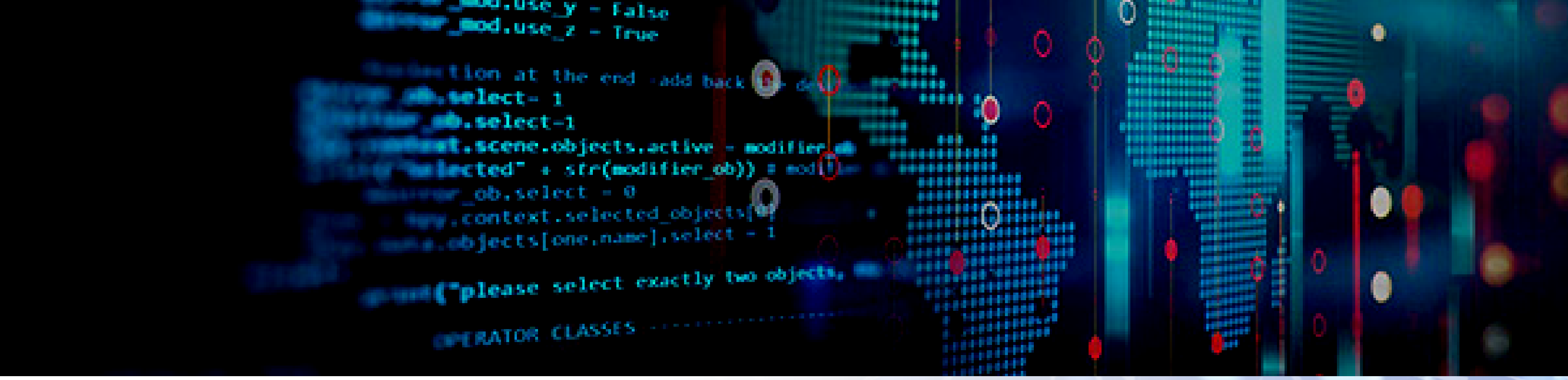
* Packet Fence 11.0.0
* Samhain File Integrity Checker 4.4.6
* Clam AntiVirus Toolkit 0.104.0
* SQLMAP - Automatic SQL Injection Tool 1.5.9
* nfstream 6.3.4
* Hashcat Advanced Password Recovery 6.2.4 Source Code
* Hashcat Advanced Password Recovery 6.2.4 Binary Release
* Dr Checker 4 Linux
* GNU Privacy Guard 2.2.30
* Flawfinder 2.0.19

Kali Linux Tutorials

* SLSA : Supply-chain Levels For Software Artifacts
* A Career as an Ethical Hacker
* PSPKIAudit : PowerShell toolkit for auditing Active Directory Certificate Services (AD CS)
* EDD : Enumerate Domain Data
* Git-Secret : Go Scripts For Finding An API Key / Some Keywords In Repository
* LazySign - Create Fake Certs For Binaries Using Windows Binaries And The Power Of Bat Files
* Brutus : An Educational Exploitation Framework Shipped On A Modular And Highly Extensible Multi-Taski
* PickleC2 : A Post-Exploitation And Lateral Movements Framework
* TsharkVM : Tshark + ELK Analytics Virtual Machine
* Process-Dump : Windows Tool For Dumping Malware PE Files From Memory Back To Disk For Analysis

GBHackers Analysis

* U.S. Cyber Command Warns of Active Mass Exploitation Attempts Targeting Confluence Flaws
* Conti Ransomware Gang Hacking Microsoft Exchange Servers Using ProxyShell Exploits
* WhatsApp Image Filter Bug Let Hackers Steal Sensitive Data
* F5 BIG-IP Flaw Let Hackers Execute Arbitrary System Commands
* The Truth About Russian Hackers



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Panel: Validating Evidence for Courtroom Testimony
* The Future of Work: Finding Evil Without Losing Your Mind
* Crossing the Threshold: Analysis of the Facebook Portal Mini
* Reporting for Digital Forensics | Jason Wilkins

Defcon Conference

* DEF CON 29 Cloud Village - Yuval Avrahami - WhoC   Peeking under the hood of CaaS offerings
* DEF CON 29 Cloud Village - Magno Logan - Workshop Kubernetes Security 101 Best Practices
* DEF CON 29 Cloud Village - Karl Fosaaen -   Extracting all the Azure Passwords
* DEF CON 29 Cloud Village - Wes Lambert - Onions In the Cloud Make the CISO Proud

Hak5

* HakByte: Learn Web Hosting on Your Raspberry Pi with Dataplicity
* Reliable Power and Protecting Octoprint Hardware w/Glytch
* Visualize Wardriving Data in a Python Notebook with Pandas & Folium

The PC Security Channel [TPSC]

* Norton buys Avast
* Lockbit Ransomware and the Accenture Hack

Eli the Computer Guy

* Office Hours with GUEST HOST Liam Allan (PLACEHOLDER)
* Operational and Physical Security (Cyber Security Part 3)
* Office Hours
* Employee Security Policy (Cyber Security Part 2)

Security Now

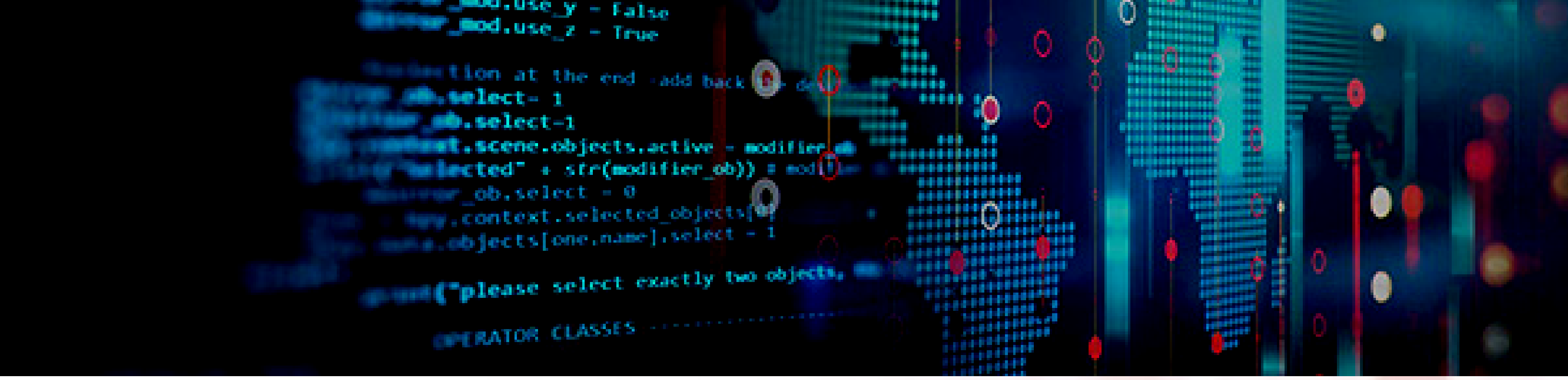
* TPM v1.2 vs 2.0 - BlueTooth Troubles, Internet Anonymity, Apple CSAM, Light Chaser
* Life: Hanging by a PIN - Credit Freeze vs. Credit Lock, SSD Bait & Switch, ProxyToken, Windows 11

Troy Hunt

* Weekly Update 260

Intel Techniques: The Privacy, Security, & OSINT Show

* 233-Anonymous Phone Update Parts II & III
* 232-Anonymous Phone Update Part I



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

* Flowspec Bulletproof Services Enable Cybercrime Worldwide
* RiskIQ Analysis Links ElTest and Gootloader Campaigns, Once Thought to Be Disparate
* Introducing Next-Gen Vulnerability Intelligence to Identify and Prioritize CVEs in Real-time
* Magecart Group 8: Patterns in Hosting Reveal Sustained Attacks on E-Commerce
* Your Growing Digital Attack Surface And How To Protect It
* 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

FireEye

* Metasploit Wrap-Up
* The Rise of Disruptive Ransomware Attacks: A Call To Action
* Cloud Challenges in the Age of Remote Work: Rapid7's 2021 Cloud Misconfigurations Report
* Security at Scale in the Open-Source Supply Chain
* CVE-2021-3546[78]: Akkadian Console Server Vulnerabilities (FIXED)
* Metasploit Wrap-Up
* Cybersecurity as Digital Detective Work: DFIR and Its 3 Key Components
* Active Exploitation of Confluence Server & Confluence Data Center: CVE-2021-26084
* SANS Experts: 4 Emerging Enterprise Attack Techniques
* [Security Nation] Jill Fraser and Deborah Blyth on Securing Colorado

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Atlassian Confluence WebWork OGNL Injection
* Internet Explorer JIT Optimization Memory Corruption
* ECOA Building Automation System Arbitrary File Deletion
* Backdoor.Win32.WinterLove.i Hardcoded Credential
* ECOA Building Automation System Local File Disclosure
* ECOA Building Automation System Authorization Bypass / Insecure Direct Object Reference
* ECOA Building Automation System Remote Privilege Escalation
* ECOA Building Automation System Missing Encryption
* ECOA Building Automation System Hardcoded SSH Credentials
* Backdoor.Win32.Wollf.h Code Execution
* ECOA Building Automation System Configuration Download Information Disclosure
* ECOA Building Automation System Cookie Poisoning / Authentication Bypass
* ECOA Building Automation System Cross Site Request Forgery
* Backdoor.Win32.VB.awm Authentication Bypass / Information Disclosure
* ECOA Building Automation System Directory Traversal
* ECOA Building Automation System Path Traversal / Arbitrary File Upload
* ECOA Building Automation System Weak Default Credentials
* HEUR.Trojan.Win32.Generic Insecure Permissions
* ECOA Building Automation System Hidden Backdoor Accounts
* POMS-PHP 1.0 SQL Injection
* Ionic Identity Vault 4.7 Android Biometric Authentication Bypass
* Rencode Denial Of Service
* WordPress TablePress 1.14 CSV Injection
* Bus Pass Management System 1.0 Cross Site Scripting
* WordPress Survey And Poll 1.5.7.3 SQL Injection

CXSecurity

* Atlassian Confluence WebWork OGNL Injection
* Patient Appointment Scheduler System 1.0 Shell Upload
* Usermin 1.820 Remote Code Execution (RCE) (Authenticated)
* Geutebruck Remote Command Execution
* Linux eBPF ALU32 32-bit Invalid Bounds Tracking Local Privilege Escalation
* Confluence Server 7.12.4 OGNL Injection Remote Code Execution
* Strapi 3.0.0-beta.17.7 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

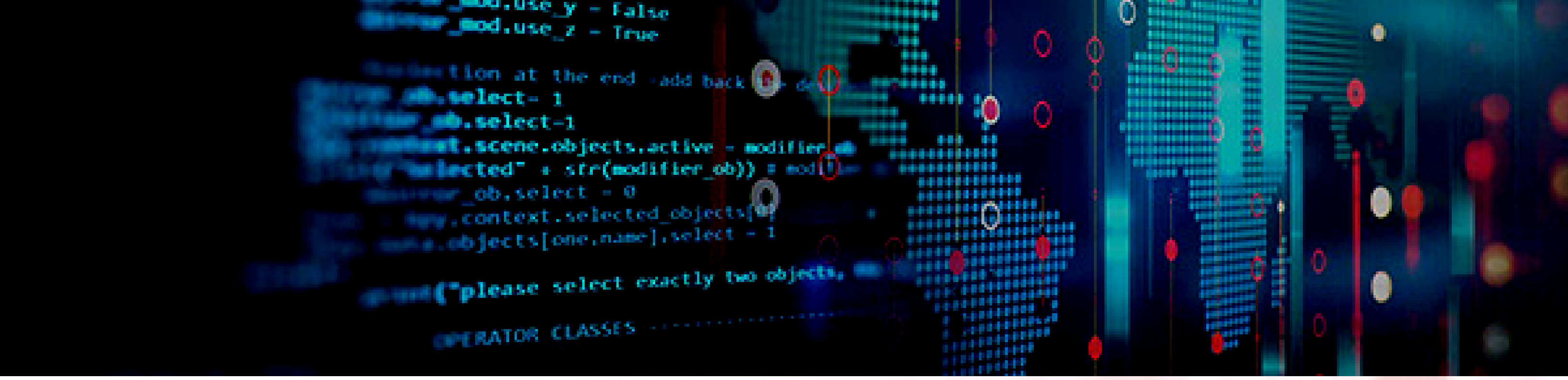
* [webapps] Apartment Visitor Management System (AVMS) 1.0 - SQLi to RCE
* [webapps] Wordpress Plugin Download From Files 1.48 - Arbitrary File Upload
* [webapps] ECOA Building Automation System - Arbitrary File Deletion
* [webapps] ECOA Building Automation System - Local File Disclosure
* [webapps] ECOA Building Automation System - Remote Privilege Escalation
* [local] ECOA Building Automation System - Missing Encryption Of Sensitive Information
* [remote] ECOA Building Automation System - Hard-coded Credentials SSH Access
* [webapps] ECOA Building Automation System - Hidden Backdoor Accounts and backdoor() Function
* [webapps] ECOA Building Automation System - Configuration Download Information Disclosure
* [webapps] ECOA Building Automation System - Cookie Poisoning Authentication Bypass
* [webapps] ECOA Building Automation System - 'multiple' Cross-Site Request Forgery (CSRF)
* [webapps] ECOA Building Automation System - Directory Traversal Content Disclosure
* [webapps] ECOA Building Automation System - Path Traversal Arbitrary File Upload
* [webapps] ECOA Building Automation System - Weak Default Credentials
* [webapps] Men Salon Management System 1.0 - Multiple Vulnerabilities
* [local] Active WebCam 11.5 - Unquoted Service Path
* [webapps] Bus Pass Management System 1.0 - 'adminname' Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin TablePress 1.14 - CSV Injection
* [webapps] WordPress Plugin Survey & Poll 1.5.7.3 - 'sss_params' SQL Injection (2)
* [webapps] WordPress Plugin WP Sitemap Page 1.6.4 - Stored Cross-Site Scripting (XSS)
* [webapps] Antminer Monitor 0.5.0 - Authentication Bypass
* [dos] SmartFTP Client 10.0.2909.0 - 'Multiple' Denial of Service
* [webapps] Patient Appointment Scheduler System 1.0 - Persistent/Stored XSS
* [webapps] Patient Appointment Scheduler System 1.0 - Unauthenticated File Upload & Remote Code Execut

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
```

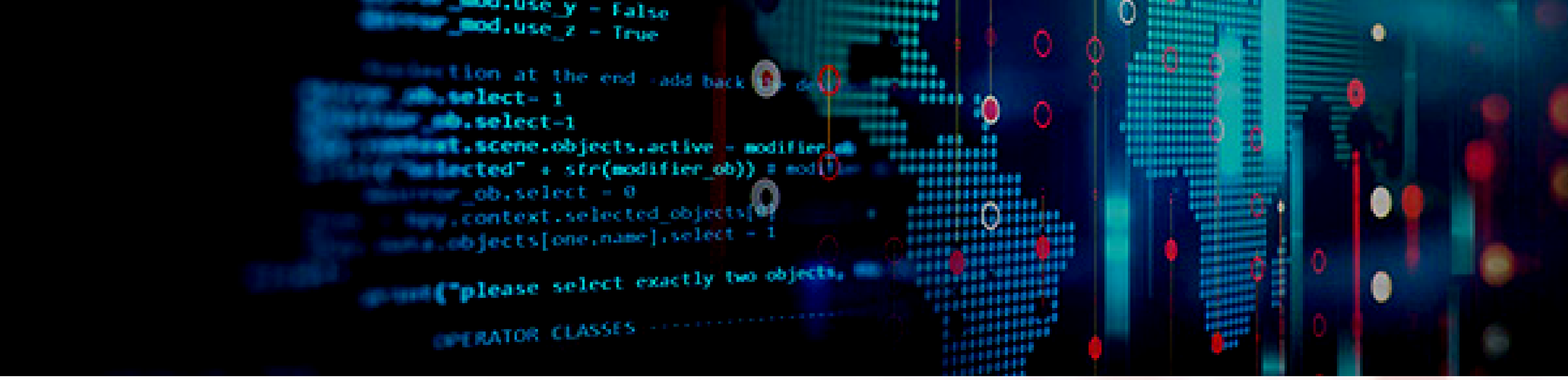
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



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.



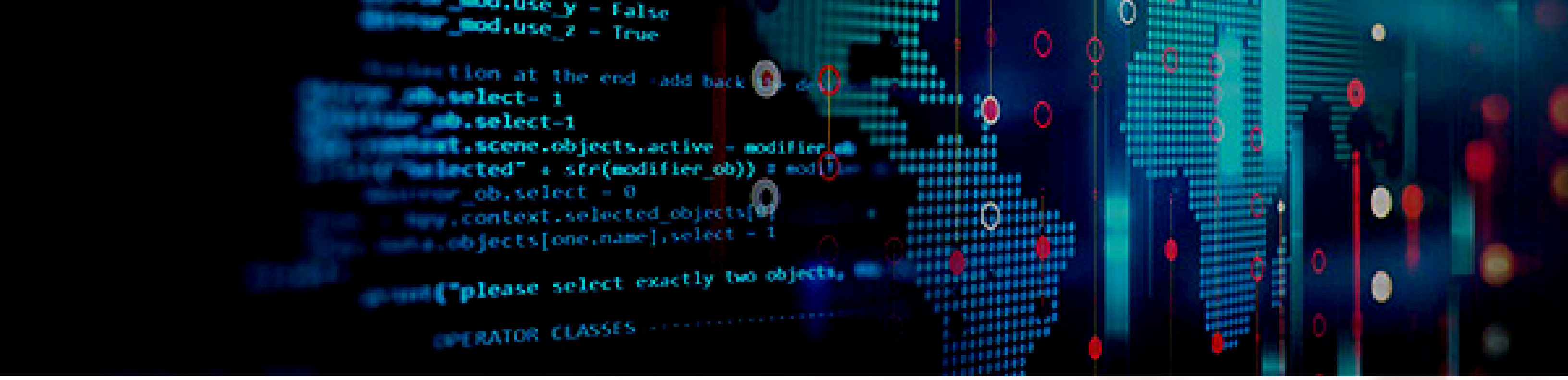
Dark Web News

Darknet Live

Empire Vendor "TheQueensHive" Pleads Guilty to Drug Charges
A man from New Mexico admitted selling methamphetamine, LSD, and MDMA through the "TheQueensHive&rdquo; vendor account on the darkweb. (via darknetlive.com)
Australian Drug Trafficker Sentenced to 16 Years in Prison
An Australian man was sentenced to more than ten years in prison for selling drugs purchased on the darkweb. (via darknetlive.com)
ProtonMail Is in the News for Complying With Law Enforcement
ProtonMail's cooperation with law enforcement resulted in the arrest of an activist in France. (via darknetlive.com)
Two Bavarians Arrested for Buying Counterfeit Xanax
Two Bavarian have been buying counterfeit Xanax on the darkweb for the purpose of resale. (via darknetlive.com)

Dark Web Link

NBI: Fighting Online Crime In Finland At Forefront Of Dark Web Drug Trade
According to the head of a crime prevention unit, the NBI(National Bureau of Investigation) and additional authorities have increased surveillance of the trading of illegal items on the dark web this year, but without adequate funds, the job will become increasingly difficult. The term &#8220;dark web&#8221; refers to internet sites that require specific software or [...] The post NBI: Fighting Online Crime In Finland At Forefront Of Dark Web Drug Trade appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Dark Web Scanner - Find Out If Your Email And Passwords Have Been Hacked
Panda, with the support of WatchGuard, has created a tool that use to scan the Dark Web and happens to check if the information related with your accounts has been co-operated: Dark Web Scanner Panda Security&#160;offers Dark Web Scanner free of charge to protect the online security of the user, who often finds himself without [...] The post Dark Web Scanner &#8211; Find Out If Your Email And Passwords Have Been Hacked appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Lynnmall Attack: Why Isis Is Tougher To Setback Online Than On The Battlefield
As the attack on Friday on a supermarket on New Zealand by an Isis sympathiser established, Isis's radical ideology continues to have strong allure for some disaffected Muslims in the west. Isis ideology didn't die with the demise of Isil and its intentions to build a caliphate in Syria and Iraq. Isis continues to radicalise [...] The post Lynnmall Attack: Why Isis Is Tougher To Setback Online Than On The Battlefield appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* WordPress Releases Security Update
* Citrix Releases Security Updates for Hypervisor
* Cisco Releases Security Updates for Multiple Products
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* Zoho Releases Security Update for ADSelfService Plus
* Microsoft Releases Mitigations and Workarounds for CVE-2021-40444
* CISA Insights on Risk Considerations for Managed Service Provider Customers
* Atlassian Releases Security Updates for Confluence Server and Data Center
* AA21-243A: Ransomware Awareness for Holidays and Weekends
* AA21-229A: BadAlloc Vulnerability Affecting BlackBerry QNX RTOS
* Vulnerability Summary for the Week of August 30, 2021
* Vulnerability Summary for the Week of August 23, 2021

Zero Day Initiative Advisories

ZDI-CAN-15192: Cisco
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kpc' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14805: Cisco
A CVSS score 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) from Agile Information Security' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14969: Parallels
A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Ben McBride' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15146: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14979: OpenText
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 'rac' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15148: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15144: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15147: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15149: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15152: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15229: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15151: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15150: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-10, 3 days ago. The vendor is given until 2022-01-08 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14952: X.Org

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 'Jan-Niklas Sohn' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15197: Bitdefender

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15199: 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: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-14950: X.Org

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 'Jan-Niklas Sohn' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-14951: X.Org

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 'Jan-Niklas Sohn' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15059: 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: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15206: Bitdefender

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15060: 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: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15123: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15124: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-15126: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-09-08, 5 days ago. The vendor is given until 2022-01-06 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-5069-2

Ubuntu Security Notice 5069-2 - USN-5069-1 fixed a vulnerability in mod-auth-mellon. This update provides the corresponding updates for Ubuntu 21.04. It was discovered that mod-auth-mellon incorrectly filtered certain URLs. A remote attacker could possibly use this issue to perform an open redirect attack. Various other issues were also addressed.

Ubuntu Security Notice USN-5070-1

Ubuntu Security Notice 5070-1 - Maxim Levitsky and Paolo Bonzini discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel allowed a guest VM to disable restrictions on VMLOAD/VMSAVE in a nested guest. An attacker in a guest VM could use this to read or write portions of the host's physical memory. Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. Various other issues were also addressed.

Red Hat Security Advisory 2021-3425-01

Red Hat Security Advisory 2021-3425-01 - Red Hat support for Spring Boot provides an application platform that reduces the complexity of developing and operating applications for OpenShift as a containerized platform. This release of Red Hat support for Spring Boot 2.3.10 serves as a replacement for Red Hat support for Spring Boot 2.3.6, and includes security and bug fixes and enhancements. For more information, see the release notes listed in the References section. Issues addressed include denial of service and information leakage vulnerabilities.

Ubuntu Security Notice USN-5072-1

Ubuntu Security Notice 5072-1 - Maxim Levitsky and Paolo Bonzini discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel allowed a guest VM to disable restrictions on VMLOAD/VMSAVE in a nested guest. An attacker in a guest VM could use this to read or write portions of the host's physical memory. Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. Various other issues were also addressed.

Red Hat Security Advisory 2021-3477-01

Red Hat Security Advisory 2021-3477-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include code execution, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-3466-01

Red Hat Security Advisory 2021-3466-01 - This release of Red Hat JBoss Enterprise Application Platform 7.3.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include denial of service and traversal vulnerabilities.

Ubuntu Security Notice USN-5071-1

Ubuntu Security Notice 5071-1 - Maxim Levitsky and Paolo Bonzini discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel allowed a guest VM to disable restrictions on VMLOAD/VMSAVE in a nested guest. An attacker in a guest VM could use this to read or write portions of the host's physical memory. Maxim Levitsky discovered that the KVM hypervisor implementation for AMD processors in the Linux kernel did not properly prevent a guest VM from enabling AVIC in nested guest VMs. An attacker in a guest VM could use this to write to portions of the host's physical memory. Various other issues were also addressed.

Red Hat Security Advisory 2021-3459-01

Red Hat Security Advisory 2021-3459-01 - The VDSM service is required by a Virtualization Manager to manage the Linux hosts. VDSM manages and monitors the host's storage, memory and networks as well as virtual machine creation, other host administration tasks, statistics gathering, and log collection. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-3467-01

Red Hat Security Advisory 2021-3467-01 - This release of Red Hat JBoss Enterprise Application Platform 7.3.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include denial of service and traversal vulnerabilities.

Ubuntu Security Notice USN-5066-2

Ubuntu Security Notice 5066-2 - USN-5066-1 fixed a vulnerability in PySAML2. This update provides the corresponding update for Ubuntu 16.04 ESM. Brian Wolff discovered that PySAML2 incorrectly validated cryptographic signatures. A remote attacker could possibly use this issue to alter SAML documents. Various other issues were also addressed.

Ubuntu Security Notice USN-5069-1

Ubuntu Security Notice 5069-1 - It was discovered that mod-auth-mellon incorrectly filtered certain URLs. A remote attacker could possibly use this issue to perform an open redirect attack.

Red Hat Security Advisory 2021-3481-01

Red Hat Security Advisory 2021-3481-01 - Neutron is a virtual network service for Openstack, and a part of Netstack. Just like OpenStack Nova provides an API to dynamically request and configure virtual servers, Neutron provides an API to dynamically request and configure virtual networks. These networks connect "interfaces" from other OpenStack services. The Neutron API supports extensions to provide advanced network capabilities.

Red Hat Security Advisory 2021-3303-04

Red Hat Security Advisory 2021-3303-04 - 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 container images for Red Hat OpenShift Container Platform 4.7.29.

Red Hat Security Advisory 2021-3468-01

Red Hat Security Advisory 2021-3468-01 - This release of Red Hat JBoss Enterprise Application Platform 7.3.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include denial of service and traversal vulnerabilities.

Red Hat Security Advisory 2021-3473-01

Red Hat Security Advisory 2021-3473-01 - Red Hat Ansible Automation Platform integrates Red Hat's automation suite consisting of Red Hat Ansible Tower, Red Hat Ansible Engine, and use-case specific capabilities for Microsoft Windows,network, security, and more, along with Software-as-a-Service -based capabilities and features for organization-wide effectiveness. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5068-1

Ubuntu Security Notice 5068-1 - It was discovered that GD Graphics Library incorrectly handled certain GD and GD2 files. An attacker could possibly use this issue to cause a crash or expose sensitive information. This issue only affected Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, Ubuntu 16.04 ESM, and Ubuntu 14.04 ESM. It was discovered that GD Graphics Library incorrectly handled certain TGA files. An attacker could possibly use this issue to cause a denial of service or expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5067-1

Ubuntu Security Notice 5067-1 - Jakub Hrozek discovered that SSSD incorrectly handled file permissions. A local attacker could possibly use this issue to read the sudo rules available for any user. This issue only affected Ubuntu 18.04 LTS. It was discovered that SSSD incorrectly handled Group Policy Objects. When SSSD is configured with too strict permissions causing the GPO to not be readable, SSSD will allow all authenticated users to login instead of being denied, contrary to expectations. This issue only affected Ubuntu 18.04 LTS. Various other issues were also addressed.

Ubuntu Security Notice USN-5066-1

Ubuntu Security Notice 5066-1 - Brian Wolff discovered that PySAML2 incorrectly validated cryptographic signatures. A remote attacker could possibly use this issue to alter SAML documents.

Ubuntu Security Notice USN-5065-1

Ubuntu Security Notice 5065-1 - It was discovered that Open vSwitch incorrectly handled decoding RAW_ENCAP actions. A remote attacker could use this issue to cause Open vSwitch to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5063-1

Ubuntu Security Notice 5063-1 - Ori Hollander discovered that HAProxy incorrectly handled HTTP header name length encoding. A remote attacker could possibly use this issue to inject a duplicate content-length header and perform request smuggling attacks.

Ubuntu Security Notice USN-5064-1

Ubuntu Security Notice 5064-1 - Maverick Chung and Qiaoyi Fang discovered that cpio incorrectly handled certain pattern files. A remote attacker could use this issue to cause cpio to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2021-3471-01

Red Hat Security Advisory 2021-3471-01 - This release of Red Hat JBoss Enterprise Application Platform 7.3.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include denial of service and traversal vulnerabilities.

Red Hat Security Advisory 2021-3454-01

Red Hat Security Advisory 2021-3454-01 - Red Hat Advanced Cluster Management for Kubernetes 2.3.2 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console&mdash;with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs and security issues.

Red Hat Security Advisory 2021-3447-01

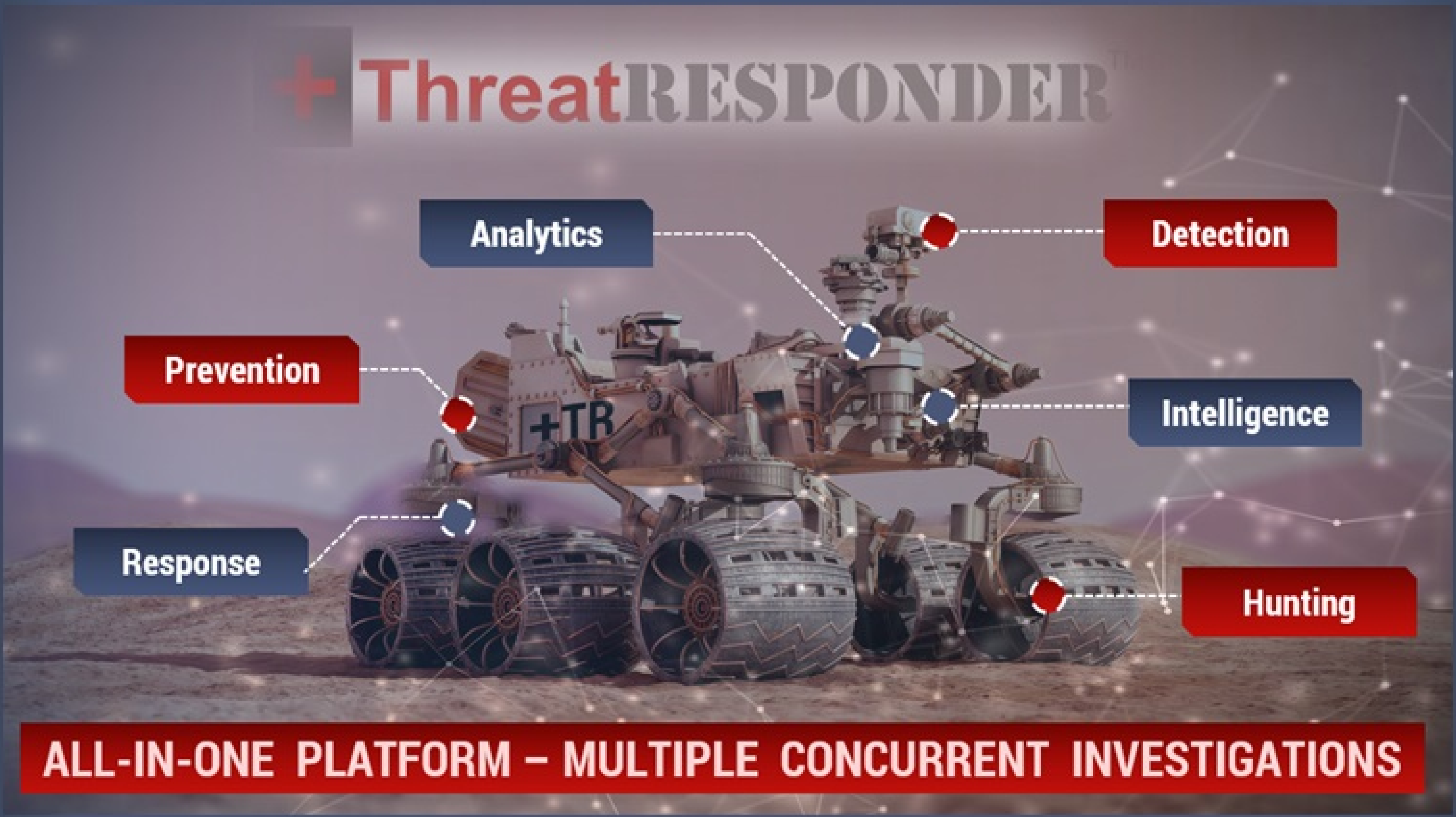
Red Hat Security Advisory 2021-3447-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include an out of bounds access vulnerability.

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

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

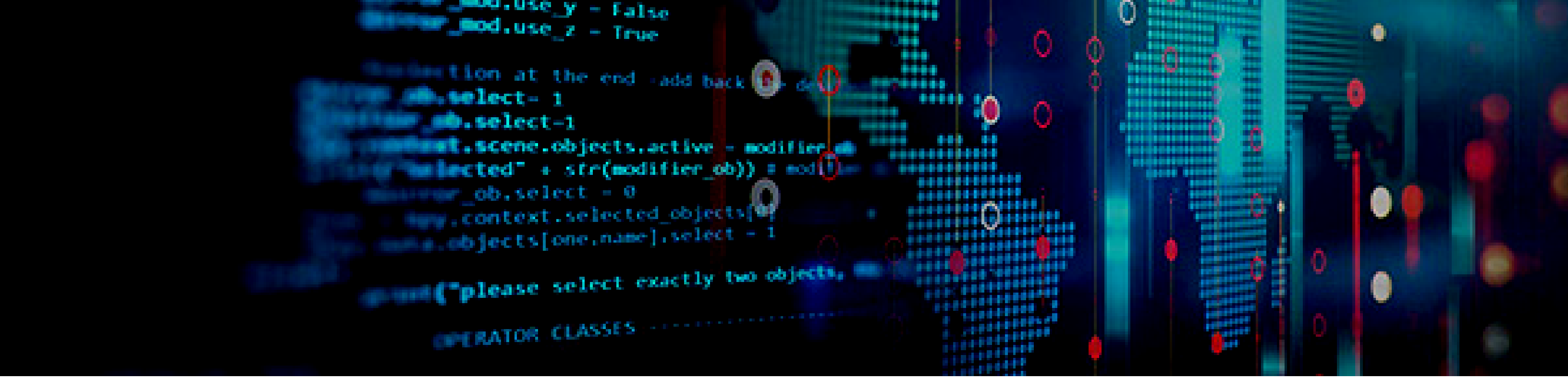
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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



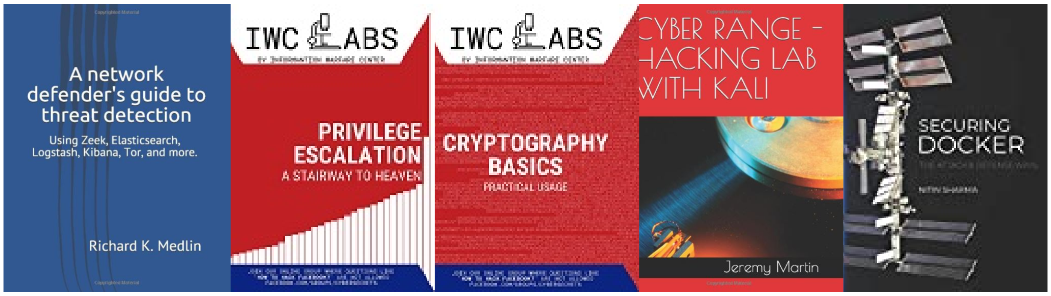
The Cyber Secrets publications on Amazon

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.

CYBER Secrets
What's Inside?
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
THE 8 LAYERS OF THE OSI CAKE
LAUNCHING EXPLOITS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION

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