May-24-21

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

May 24, 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

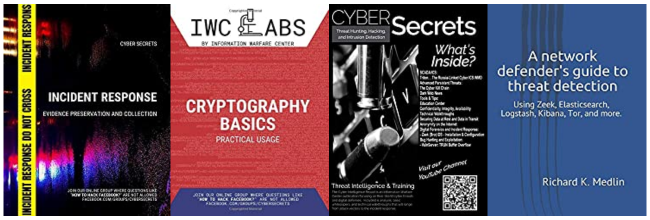
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

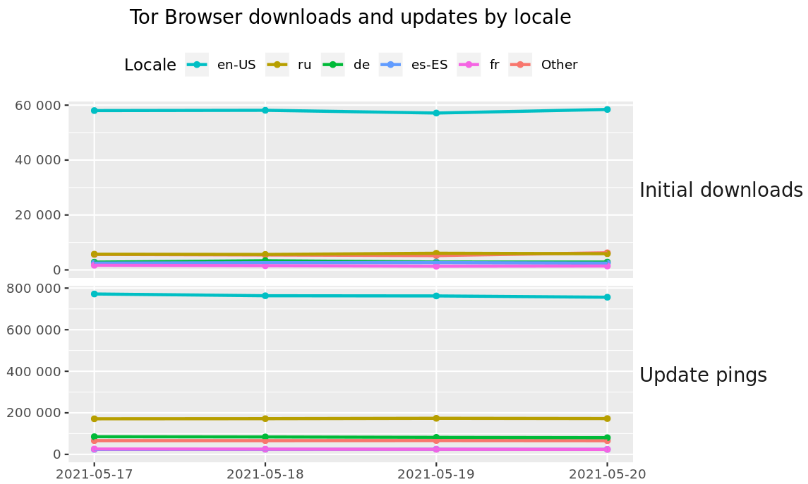
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.


INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
IWC LABS
CRYPTOGRAPHY BASICS
PRACTICAL USAGE
CYBER Secrets
What's Inside?
A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin



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.

* CSI Linux 2021.2 Beta is now availible for those that have 2021.1 already installed. To upgrade, open a command line and type: wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh

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

Index of Sections

Current News

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

The Hacker Corner:

* Security Conferences
* Google Zero Day Project

Cyber Range Content

* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques

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

InfoSec Media for the Week

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

Exploits and Proof of Concepts

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

Cyber Crime & Malware Files/Links Latest Identified

* CyberCrime-Tracker

Advisories

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

Information Warfare Center Products

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

LATEST NEWS

Packet Storm Security

* Hackers Take Note: The No Starch Press Foundation 2021 Grant Cycle Is Here
* What Makes North Korean Hacking Groups More Creative?
* 100M Android Users Hit By Rampant Cloud Leaks
* Vulns In Billions Of Wi-Fi Devices Let Hackers Bypass Firewalls
* CNA Financial Paid $40 Million Ransom To Regain Control Of Systems
* 4 Vulnerabilities Under Attack Give Hackers Full Control Of Android Devices
* Fraudsters Employ Amazon Vishing Attacks In Fake Order Scams
* Apple Isn't Happy About The Amount Of Mac Malware Out There
* Should Paying Hacker Ransoms Be Illegal?
* Amazon Extends Ban On Police Using Rekognition
* Florida Water Plant Compromise Came Hours After Worker Visited Malicious Site
* How Dow Jones Used The Pandemic To Undergo A Zero Trust Overhaul
* What Beijing's New Crackdown Means For Crypto In China
* Microsoft, Adobe Exploits Top List Of Crooks' Wish List
* Bizarro Banking Trojan Sports Sophisticated Backdoor
* SolarWinds Hack: Russian Denial Unconvincing
* City Pays $350k After Suing "Hackers" For Opening Dropbox Link It Sent To Them
* RevengeRAT And AysncRAT Target Aerospace And Travel Sectors
* Ireland Won't Pay Ransom For Attack On Health Service
* How Apple's AirTag Turns Us Into Unwitting Spies
* DarkSide Suffers Server Shutdowns
* Rapid7 Source Code, Alert Data Accessed In Codecov Supply Chain Attack
* DarkSide Explained: The Ransomware Group Behind The Attack
* US Fuel Pipeline Paid Hackers $5 Million In Ransom
* Toshiba Unit Hacked By DarkSide

Krebs on Security

* How to Tell a Job Offer from an ID Theft Trap
* Recycle Your Phone, Sure, But Maybe Not Your Number
* Try This One Weird Trick Russian Hackers Hate
* DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized
* Microsoft Patch Tuesday, May 2021 Edition
* A Closer Look at the DarkSide Ransomware Gang
* Fintech Startup Offers $500 for Payroll Passwords
* Investment Scammer John Davies Reinvents Himself?
* Malicious Office 365 Apps Are the Ultimate Insiders
* The Wages of Password Re-use: Your Money or Your Life

LATEST NEWS

Dark Reading

* Data in Danger Amid New IT Challenges
* FBI Issues Conti Ransomware Alert as Attacks Target Healthcare
* Cloud Security Blind Spots: Where They Are and How to Protect Them
* Latest Security News From RSAC 2021
* The Edge Poll: Moving On
* The Changing Face of Cybersecurity Awareness
* Dev-Sec Disconnect Undermines Secure Coding Efforts
* Lack of Skills, Maturity Hamper Threat Hunting at Many Organizations
* Don't Let Scary Headlines Shape Your Company's Cyber-Resilience Strategy
* Maricopa County CISO: Online Misinformation/Disinformation in 2020 Election a 'Gamechanger'
* 100M Users' Data Exposed via Third-Party Cloud Misconfigurations
* Security Providers Describe New Solutions (& Growing Threats) at RSAC
* Cost Savings, Better Security Drive Adoption of Emerging Technologies
* 3 Ways Anti-Vaxxers Will Undercut Security With Misinformation
* How 2 New Executive Orders May Reshape Cybersecurity & Supply Chains for a Post-Pandemic World
* Cobalt Strike Becomes a Preferred Hacking Tool by Cybercrime, APT Groups
* SolarWinds CEO: Attack Began Much Earlier Than Previously Thought
* Google Chrome Makes It Easier to Update Compromised Passwords
* Attackers Took 5 Minutes to Start Scanning for Exchange Server Flaws
* Automation & Pervasive, Connected Technology to Pose Cyber Threats in 2030

The Hacker News

* Details Disclosed On Critical Flaws Affecting Nagios IT Monitoring Software
* FBI Analyst Charged With Stealing Counterterrorism and Cyber Threat Info
* FBI Warns Conti Ransomware Hit 16 U.S. Health and Emergency Services
* Air India Hack Exposes Credit Card and Passport Info of 4.5 Million Passengers
* Insurance Firm CNA Financial Reportedly Paid Hackers $40 Million in Ransom
* Microsoft Warns of Data Stealing Malware That Pretends to Be Ransomware
* 23 Android Apps Expose Over 100,000,000 Users' Personal Data
* Is Single Sign-On Enough to Secure Your SaaS Applications?
* Watering Hole Attack Was Used to Target Florida Water Utilities
* Android Issues Patches for 4 New Zero-Day Bugs Exploited in the Wild
* DarkSide Ransomware Gang Extorted $90 Million from Several Victims in 9 Months
* Mozilla Begins Rolling Out 'Site Isolation' Security Feature to Firefox Browser
* A Simple 1-Click Compromised Password Reset Feature Coming to Chrome Browser
* How Apple Gave Chinese Government Access to iCloud Data and Censored Apps
* Free "vCISO Clinic" offers Resource-Constrained InfoSec Leaders a Helping Hand

LATEST NEWS

Security Week

* Hacker Who Sold UPMC Employee Information Pleads Guilty
* Growing Mystery of Suspected Energy Attacks Draws US Concern
* India's National Carrier Says Hack Leaked Passengers' Data
* ICS Vendors Assessing Impact of New OPC UA Vulnerabilities
* Microsoft Unveils SimuLand: Open Source Attack Techniques Simulator
* Tulsa Cybersecurity Attack Similar to Pipeline Attack
* RSA Conference 2021 - Summary of Vendor Announcements
* UK-Based API Security Firm 42Crunch Raises $17 Million
* Data Access Control Firm Immuta Raises $90 Million in Series D Funding
* Healthcare IoT Cybersecurity Firm Cynerio Raises $30 Million
* Lessons Learned From High-Profile Exploits
* Alaska Health Department Website Targeted in Malware Attack
* Endpoint Security Provider ThreatLocker Raises $20 Million
* Member of Russian Gang That Hacked Tax Prep Firms Sentenced to Prison in U.S.
* Google: Four Recently Patched Android Vulnerabilities Exploited in Attacks
* Israel Says Its Fighter Jets Bombed Buildings Used by Hamas Cyber Unit
* Hackers Targeted SolarWinds Earlier Than Previously Known
* Scans for Vulnerable Exchange Servers Started 5 Minutes After Disclosure of Flaws
* Glass and Metal Packaging Giant Ardagh Group Discloses Cyberattack
* Colonial Pipeline CEO Explains $4.4M Ransomware Payment
* Probe Into Florida Water Plant Hack Led to Discovery of Watering Hole Attack
* DarkSide: Newly Found Variant and Implications for the Ransomware Gang's Future
* Google Workspace Gets New Security Features
* Emerson Patches Several Vulnerabilities in X-STREAM Gas Analyzers
* Lawmakers Reintroduce 'Pipeline Security Act' Following Colonial Hack

Infosecurity Magazine

* Amex Fined After Sending Over Four Million Spam Emails
* Air India: Supplier Breach Hit 4.5 Million Passengers
* Insurance Giant Reportedly Paid $40 Million Ransom
* iC3 Logs Six Millionth Complaint
* Telemarketing Fraudster Jailed for 10 Years
* Ransomware Gang Gifts Decryption Tool to HSE
* Report Shows Global CISOs Failing to Practice What They Preach
* Global Credential Stuffing Attempts Hit 193 Billion in 2020
* Cloud Misconfiguration Exposes 100M+ Android Users
* #RSAC: The Most Dangerous New Attack Techniques
* #RSAC: The Rise of the Chief Product Security Officer

* #RSAC: Cyber-threat Landscape "the Worst It's Ever Been" Due to Nation-State Behaviors

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Ransomware-as-a-Service is Organizing, Becoming More Devastating and Costly
* The FBI's Internet Crime Complaint Center Marks Its 6 Millionth Complaint as Pace Accelerates
* Credential Stuffing the Financial Services Sector
* When Cryptocurrency Investments Really Are Too Good To Be True
* Transparent Tribe Uses Spoofed Domains in Social Engineering Attacks
* CyberheistNews Vol 11 #19 [Heads Up] Phishing Scammers Can Now Remove the 'External Sender' Email War
* [NEW PhishER Feature] Flip the Script on Phishing Emails with PhishFlip
* Zix Phishing Campaign Tricks Users into a False Sense of Security
* Ransoms Increase 43% as More Ransomware Attacks Include the Threat to Leak Exfiltrated Data
* Healthcare Organizations Should Expect Cyber Insurance Premiums to Increase 25 to 50% This Year

ISC2.org Blog

* More Than Likely, Or Less Than Probable: Is a truly quantitative security analysis possible?
* Many Cybersecurity Jobseekers Lack a Full Understanding of the Role They Seek
* What's Next for Cybersecurity Workers? You Tell Us.
* Cloud (Mis)Configuration: What Do You Need to Consider?
* (ISC)&sup2; Supports NIST Encouragement of Inclusive Cybersecurity Terminology

HackRead

* Watch out as fake ransomware attack infects PCs with StrRAT
* 23 Android apps caught leaking sensitive data of 100 million users
* A UK recruitment firm exposed sensitive applicants data for months
* Fake ransom scams targeting families of missing persons
* Chrome on Android will alert, fix your compromised password
* Lighthouse, PageSpeed insights usage up 70% with core web vitals looming
* Why Web Application Security Is Important

Koddos

* Watch out as fake ransomware attack infects PCs with StrRAT
* 23 Android apps caught leaking sensitive data of 100 million users
* A UK recruitment firm exposed sensitive applicants data for months
* Fake ransom scams targeting families of missing persons
* Chrome on Android will alert, fix your compromised password
* Lighthouse, PageSpeed insights usage up 70% with core web vitals looming
* Why Web Application Security Is Important

LATEST NEWS

Naked Security

* S3 Ep33: Eufy camera leak, Afterburner crisis, and AirTags (again) [Podcast]
* Regulator fines COVID-19 tracker for turning contact data into sales leads
* "Those aren't my kids!" - Eufy camera owners report video mixups
* Apple AirTag hacked again - free internet with no mobile data plan!
* Gamers beware! Crooks take advantage of MSI download outage&hellip;
* S3 Ep32: AirTag jailbreak, Dell vulns, and a never-ending scam [Podcast]
* Beware fake online trading apps, on iOS as well as Android
* Apple AirTag jailbroken already - hacked in rickroll attack
* Never say never! Warren Buffett caught up in integer overflow error&hellip;
* S3 Ep31: Apple zero-days, Flubot scammers and PHP supply chain bug [Podcast]

Threat Post

* DarkSide Getting Taken to 'Hackers' Court' For Not Paying Affiliates
* Building SIEM for Today's Threat Landscape
* WP Statistics Bug Allows Attackers to Lift Data from WordPress Sites
* Email Campaign Spreads StrRAT Fake-Ransomware RAT
* 100M Android Users Hit By Rampant Cloud Leaks
* The Gig Economy Creates Novel Data-Security Risks
* Four Android Bugs Being Exploited in the Wild
* 2021 Attacker Dwell Time Trends and Best Defenses
* Apple Exec Calls Level of Mac Malware 'Unacceptable'
* Can Nanotech Secure IoT Devices From the Inside-Out?

Null-Byte

* 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
* Protect Your Browsing with This 10-Year VPN Subscription
* How to Write Your Own Subdomain Enumeration Script for Better Recon
* Learn to Code Today with This $20 Web Development Course
* How to Install Kali Linux as a Portable Live USB for Pen-Testing & Hacking on Any Computer

LATEST NEWS

IBM Security Intelligence

* What Every Incident Response Plan Needs
* 5 Unique Online Scams and How to Defend Against Them
* Taking Time Off? What Your Out of Office Message Tells Attackers
* Security by Design and NIST 800-160, Part 3: Technical Processes
* The State of Small Business Cybersecurity in 2021
* Accelerate Your Hybrid Cloud Journey With Security Confidence
* User Behavior Analytics: What It Is and How It Advances Digital Security
* Avoiding Video Background Snafus: How to Hold Safe Meetings Online
* How to Boost Your Health Care Data Cybersecurity Immune System
* Using FAIR and NIST CSF for Security Risk Management

InfoWorld

* You're thinking about Kubernetes all wrong
* ProxyJump is safer than SSH agent forwarding
* How AI can enhance customer experience
* Google preps new web platform APIs
* In search of good cybersecurity
* Google unveils DevTools extension for Angular
* JDK 17: The new features in Java 17
* Build a Java application in Visual Studio Code
* Striking a balance with 'open' at Snowflake
* Google Flutter gains sound null safety, payments plug-in

C4ISRNET - Media for the Intelligence Age Military

* Russia's real-world experience is driving counter-drone innovations
* Aevum announces all-in-one drone for satellite launches, cargo delivery and surveillance
* US Air Force's newest refueling tanker to get gear allowing F-35 and F-22 to share data
* SOCOM CIO to industry: 'Rethink your business models'
* The Pentagon needs a plan to get punched in the mouth
* US Army tackles enduring system to counter both drone and cruise missile threats
* Teledyne, FLIR merger brings deep space to deep-sea sensing tech under one roof
* Air Force held first information warfare test exercises
* Liftoff to orbit in under an hour: Space Force launches missile warning satellite
* SOCOM investing in new capabilities to address technology shortfalls

The Hacker Corner

Conferences

* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)
* How To Sponsor Cybersecurity Conferences
* How To Secure Earned Cybersecurity Speaking Engagements
* World RPA & AI Summit | Interview with Ashley Pena

Google Zero Day Project

* Fuzzing iOS code on macOS at native speed
* Designing sockfuzzer, a network syscall fuzzer for XNU

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.

* Pwn2Win CTF 2021
* ICHSA CTF 2021
* wtfctf
* Zh3r0 CTF V2
* S.H.E.L.L. CTF
* BCACTF 2.0
* Circle City Con CTF 2021
* FAUST CTF 2021
* HSCTF 8
* The Threat Interceptors Challenge

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

* hacksudo: L.P.E.
* hacksudo: FOG
* Prime (2021): 2
* DriftingBlues: 9 (final)
* AdmX: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

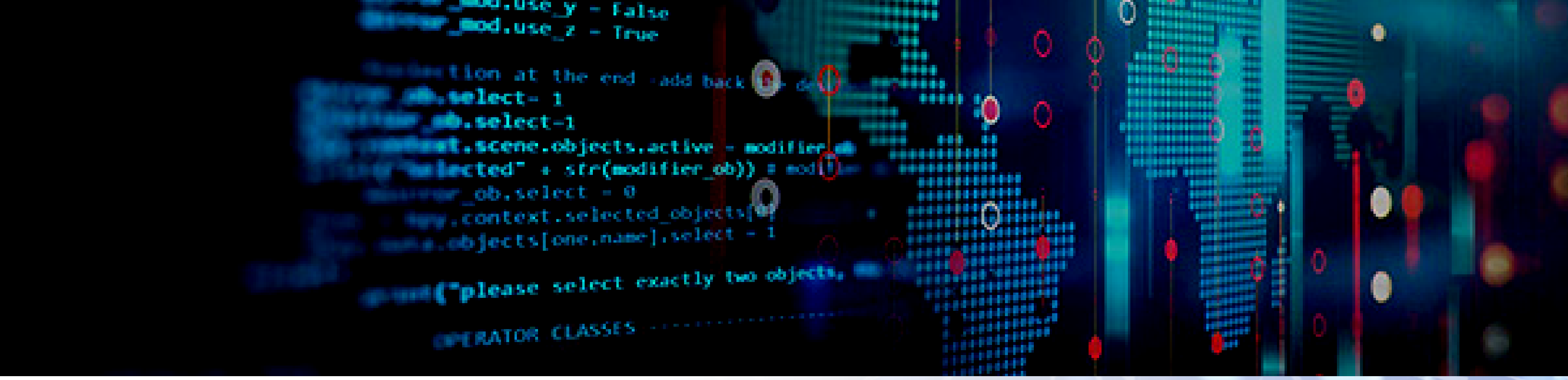
* Sifter 12
* GRR 3.4.3.1
* I2P 0.9.50
* Faraday 3.15.0
* Hashcat Advanced Password Recovery 6.2.1 Source Code
* Hashcat Advanced Password Recovery 6.2.1 Binary Release
* Wapiti Web Application Vulnerability Scanner 3.0.5
* Global Socket 1.4.30
* Packet Fence 10.3.0
* TOR Virtual Network Tunneling Tool 0.4.5.8

Kali Linux Tutorials

* Understanding the Principle of Least Privilege
* VAST : Visibility Across Space And Time
* Baserunner : A Tool For Exploring Firebase Datastores
* LibAFL : Advanced Fuzzing Library - Slot Your Fuzzer Together In Rust
* WordPress Brute Force : Super Fast Login WordPress Brute Force
* Priv2Admin : Exploitation Paths Allowing You To (Mis)Use The Windows Privileges
* Kiterunner : Contextual Content Discovery Tool
* Red-Detector : Scan Your EC2 Instance To Find Its Vulnerabilities Using Vuls.io
* Evasor : A Tool To Be Used In Post Exploitation Phase For Blue
* Pystinger : Bypass Firewall For Traffic Forwarding Using Webshell

GBHackers Analysis

* Scheme Flooding Let Hackers Identifying Users While Browsing Websites Including the Tor
* FragAttacks - New Security Vulnerabilities Affect Billions of Wi-Fi Devices
* Foxit Reader Vulnerability Let Hackers Run Malicious Code via PDFs
* New Spectre Vulnerability Let Hackers Attack Billions of Computers
* Hundreds of Millions of Dell Systems Vulnerable to Hack Due to Driver Bug



Weekly Cyber Security Video and Podcasts

SANS DFIR

* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course
* Why take FOR500: Windows Forensic Analysis course OnDemand
* iOS Third Party Apps Analysis how to use the new reference guide poster

Defcon Conference

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

Hak5

* Can a Spreadsheet Really Destroy Your Computer?
* Road Closed Ahead - Hack Across America 2021 - Hak5 2907
* Wi-Fi Can Be Hacked (Again); DarkSide Goes Offline After Pipeline Hack - ThreatWire

The PC Security Channel [TPSC]

* Darkside Ransomware: The threat behind the state of emergency in the US
* Apple Supplier Hacked by REVIL Ransomware: Live Demo & Analysis

Eli the Computer Guy

* Do you have PRIDE - Startup Life
* Employees OWNERSHIP - Startup Life
* Business Networking REALITY - Startup Life
* Dealing with WORLD CHANGE - Startup Life

Security Now

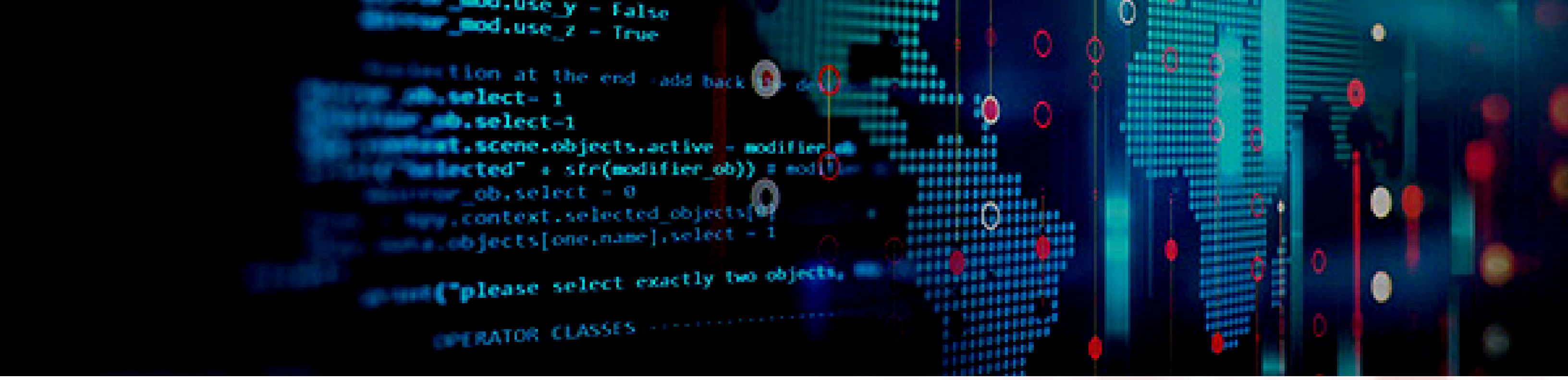
* The WiFi Frag Attacks - DarkSide Follow-Up, DarkTracer, Patch Tuesday, The Frontiers Saga
* News From the Darkside - Exim Email Server, Tor's Exit Nodes, TsuNAME, Project Hail Mary

Troy Hunt

* Weekly Update 244

Intel Techniques: The Privacy, Security, & OSINT Show

* 217-Extreme Privacy 3 & New VOIP Strategies
* 216-The Consequences of Extreme Privacy



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

* DarkSide is Standing Down, But Its Affiliates Live On
* Next-Gen Threat Intelligence: Adding Profound Value to Security and Risk Functions
* TrickBot: Get to Know the Malware That Refuses to Be Killed
* SolarWinds: Illuminating the Hidden Patterns That Advance the Story
* For Threat Actors, Shadow Z118 is the Kit That Keeps on Giving
* RiskIQ is Illuminating the Global Attack Surface With Next-Gen Security Intelligence
* Yanbian Gang Malware Continues with Wide-Scale Distribution and C2
* Agent Tesla: Malware-as-a-Service Enables Trend Analysis
* RiskIQ Named a Strong Performer in The Forrester Waveâ„¢: External Threat Intelligence Services, Q1 2
* A Vulnerable World: RiskIQ's Unique View of the Microsoft Exchange Landscape

FireEye

* Metasploit Wrap-Up
* Want to stay ahead of emerging threats? Here's how.
* Rapid7's 2021 ICER Takeaways: Vulnerability Disclosure Programs Among the Fortune 500
* Calling for cybersecurity in infrastructure modernization
* How to Implement Secure and Compliant IaC
* A Look Into Remote Onboarding at Rapid7
* How to Address the Current Complexity and Chaos of Cloud IAM
* Metasploit Wrap-Up
* Rapid7's 2021 ICER Takeaways: High-Risk Services Among the Fortune 500
* Top Challenges for Security Analytics and Operations, and How a Cloud-Based SIEM Can Help

Proof of Concept (PoC) & Exploits

Packet Storm Security

* DELL dbutil_2_3.sys 2.3 Arbitrary Write / Privilege Escalation
* WordPress WP Statistics 13.0.7 SQL Injection
* libX11 Insufficient Length Check / Injection
* Microsoft Exchange ProxyLogon Collector
* Mozilla Firefox 88.0.1 File Extension Execution
* Spotweb-Develop 1.4.9 Cross Site Scripting
* Acer Updater Service 1.2.3500.0 Unquoted Service Path
* Acer Backup Manager Module 3.0.0.99 Unquoted Service Path
* Microsoft HTTP Protocol Stack Remote Code Execution
* ASUS HID Access Service 1.0.94.0 Unquoted Service Path
* Backdoor.Win32.RMFdoor.c Authentication Bypass / Code Execution
* Backdoor.Win32.Psychward.ds Weak Hardcoded Password
* Backdoor.Win32.Psychward.c Code Execution
* ManageEngine ADSelfService Plus 6.1 CSV Injection
* In4Suit ERP 3.2.74.1370 SQL Injection
* Visual Studio Code 1.47.1 Denial Of Service
* WebSSH For iOS 14.16.10 Denial Of Service
* COVID19 Testing Management System 1.0 Cross Site Scripting
* COVID19 Testing Management System 1.0 SQL Injection
* WordPress Stop Spammers 2021.8 Cross Site Scripting
* rxvt 2.7.0 / rxvt-unicode 9.22 Code Execution
* Microsoft ACL Shortcomings
* NiceHash Miner Excavator 1.6.7c Cross Site Request Forgery
* NetMotion Mobility Server MvcUtil Java Deserialization
* Backdoor.Win32.Delf.aez Code Execution

CXSecurity

* libX11 Insufficient Length Check / Injection
* Microsoft Exchange 2019 Unauthenticated Email Download (Metasploit)
* Spotweb-Develop 1.4.9 Cross Site Scripting
* NetMotion Mobility Server MvcUtil Java Deserialization
* Subrion CMS 4.2.1 Shell Upload
* WebSSH for iOS 14.16.10 mashREPL Denial of Service (PoC)
* Microsoft Windows TokenMagic Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

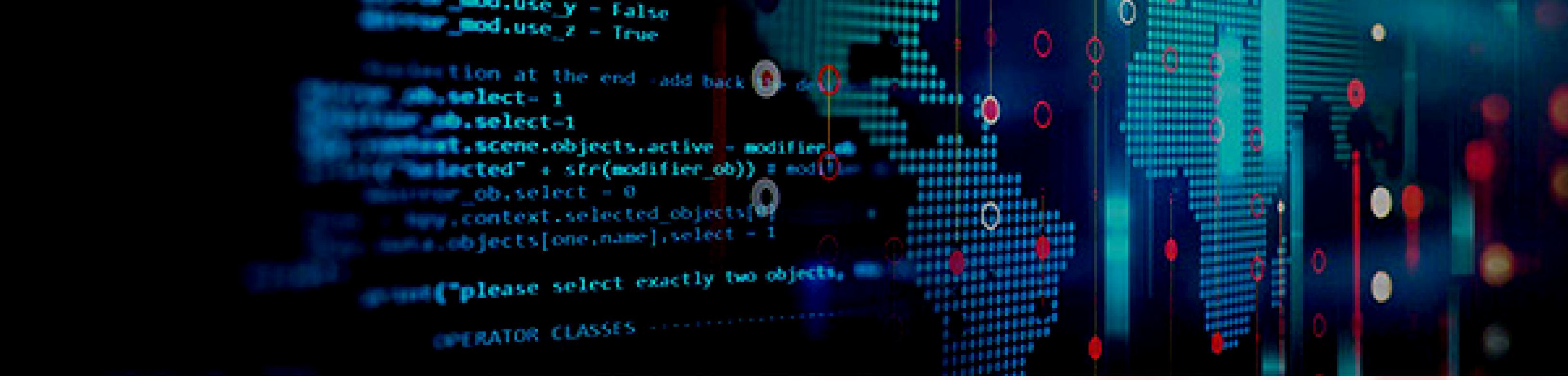
* [webapps] WordPress Plugin ReDi Restaurant Reservation 21.0307 - 'Comment' Stored Cross-Site Scriptin
* [webapps] Codiad 2.8.4 - Remote Code Execution (Authenticated) (2)
* [webapps] Shopizer 2.16.0 - 'Multiple' Cross-Site Scripting (XSS)
* [local] ePowerSvc 6.0.3008.0 - 'ePowerSvc.exe' Unquoted Service Path
* [local] DiskBoss Service 12.2.18 - 'diskbsa.exe' Unquoted Service Path
* [dos] iDailyDiary 4.30 - Denial of Service (PoC)
* [webapps] Schlix CMS 2.2.6-6 - Arbitary File Upload And Directory Traversal Leads To RCE (Authenticat
* [remote] Solaris SunSSH 11.0 x86 - libpam Remote Root (2)
* [webapps] Microsoft Exchange 2019 - Unauthenticated Email Download (Metasploit)
* [local] DELL dbutil_2_3.sys 2.3 - Arbitrary Write to Local Privilege Escalation (LPE)
* [local] Mozilla Firefox 88.0.1 - File Extension Execution of Arbitrary Code
* [webapps] Spotweb 1.4.9 - DOM Based Cross-Site Scripting (XSS)
* [local] Acer Updater Service 1.2.3500.0 - 'UpdaterService.exe' Unquoted Service Path
* [local] Backup Manager Module 3.0.0.99 - 'IScheduleSvc.exe' Unquoted Service Path
* [local] ASUS HID Access Service 1.0.94.0 - 'AsHidSrv.exe' Unquoted Service Path
* [webapps] COVID19 Testing Management System 1.0 - 'Admin name' Cross-Site Scripting (XSS)
* [webapps] COVID19 Testing Management System 1.0 - SQL Injection (Auth Bypass)
* [webapps] ManageEngine ADSelfService Plus 6.1 - CSV Injection
* [webapps] In4Suit ERP 3.2.74.1370 - 'txtLoginId' SQL injection
* [dos] WebSSH for iOS 14.16.10 - 'mashREPL' Denial of Service (PoC)
* [local] Visual Studio Code 1.47.1 - Denial of Service (PoC)
* [webapps] WordPress Plugin Stop Spammers 2021.8 - 'log' Reflected Cross-site Scripting (XSS)
* [webapps] Microsoft Exchange 2019 - Unauthenticated Email Download
* [webapps] EgavilanMedia PHPCRUD 1.0 - 'First Name' SQL 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
```

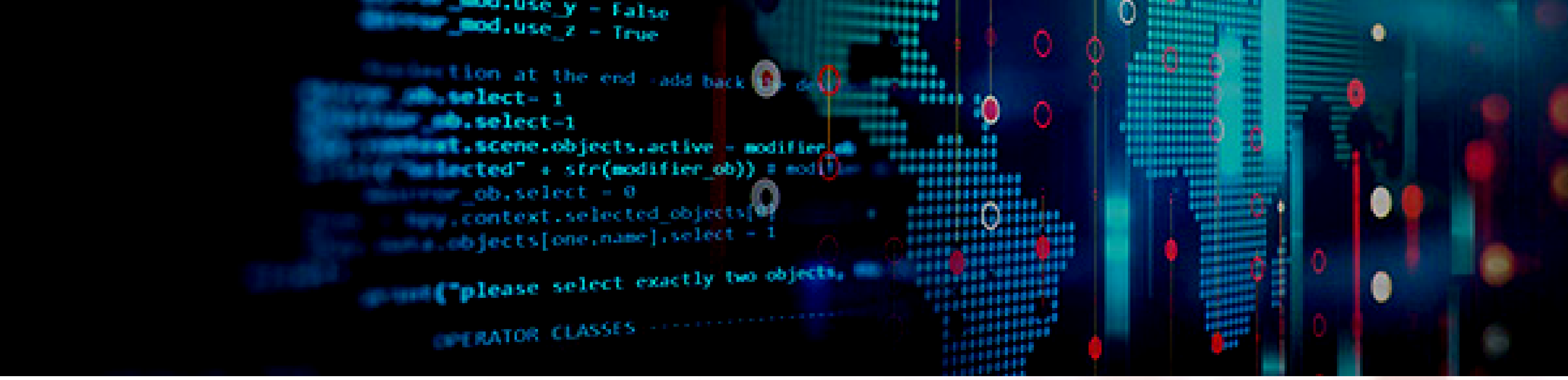
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://kshos.go.th/readme.html
http://kshos.go.th/readme.html notified by Unknown45
http://stevta.gos.pk/rn.html
http://stevta.gos.pk/rn.html notified by Ren4Sploit
http://kmc.gos.pk/rn.html
http://kmc.gos.pk/rn.html notified by Ren4Sploit
http://mis.stevta.gos.pk/rn.html
http://mis.stevta.gos.pk/rn.html notified by Ren4Sploit
http://kda.gos.pk/rn.html
http://kda.gos.pk/rn.html notified by Ren4Sploit
http://mne.stevta.gos.pk/rn.html
http://mne.stevta.gos.pk/rn.html notified by Ren4Sploit
https://smic.mi.th/ryukz.html
https://smic.mi.th/ryukz.html notified by xRyukZ
https://lampung.polri.go.id/ex.htm
https://lampung.polri.go.id/ex.htm notified by C@tCRUTz
http://tojounauna.go.id/read.htm
http://tojounauna.go.id/read.htm notified by Mr.L3RB1
https://sari.gov.et
https://sari.gov.et notified by Cyber_Horus Group
http://arrca.gov.et
http://arrca.gov.et notified by Cyber_Horus Group
http://www.earcs.gov.et
http://www.earcs.gov.et notified by Cyber_Horus Group
http://www.direagriwater.gov.et
http://www.direagriwater.gov.et notified by Cyber_Horus Group
https://mairie-villarsstgeorges.fr/license.html
https://mairie-villarsstgeorges.fr/license.html notified by L4663R666H05T
http://dprd.cilacapkab.go.id/read.txt
http://dprd.cilacapkab.go.id/read.txt notified by Mr.L3RB1
http://www.jdih.alorkab.go.id/read.txt
http://www.jdih.alorkab.go.id/read.txt notified by Mr.L3RB1
http://jdih-setwan.alorkab.go.id/read.txt
http://jdih-setwan.alorkab.go.id/read.txt notified by Mr.L3RB1



Dark Web News

Darknet Live

"NSWGreat" Sentenced to 14 Years in Prison

An Australian man was sentenced to prison for masterminding a multi-million dollar darkweb drug trafficking operation. (via darknetlive.com)

German Man Arrested for Reselling Amphetamine

Neubrandenburg authorities arrested a German man for allegedly reselling large quantities of drugs he had purchased on the darkweb. (via darknetlive.com)

Scotland: Two Sentenced for Selling Drugs on the Darkweb

In Scotland's first darkweb drug trafficking sentencing, two men were sentenced to prison for supplying large quantities of drugs through the darkweb (via darknetlive.com)

Opioid Vendor "H00k3d" Pleads Guilty to Drug Charges

A New York man admitted selling more than $1 million worth of opioids and counterfeit currency on darkweb markets. (via darknetlive.com)

Dark Web Link

Darknet Data Hack: Hacker Pleads Guilty On Stolen Database Sale

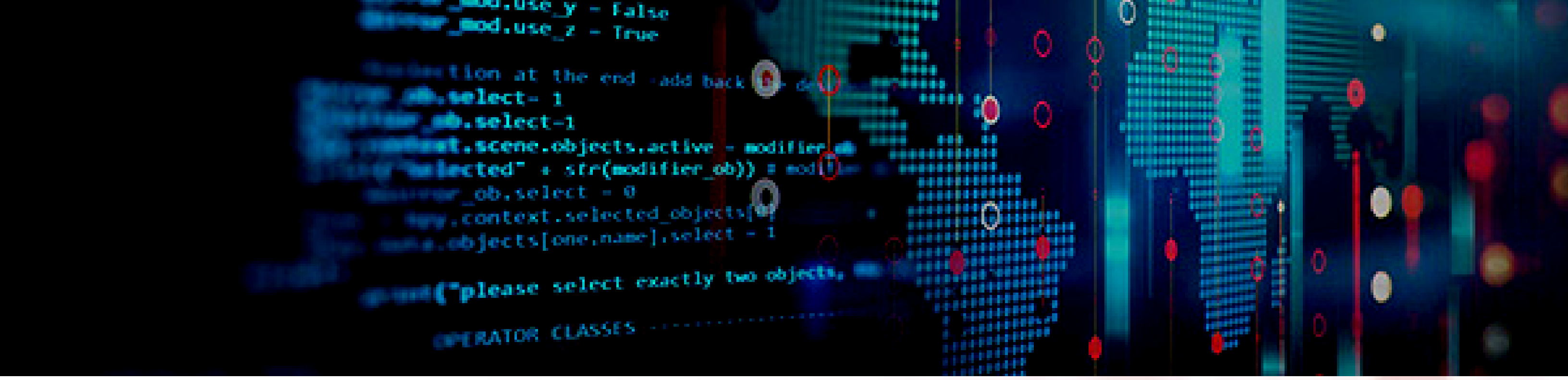
A Michigan man has pleaded guilty on Thursday morning for conducting a darknet data hack. He had hacked a database of UPMC employees in 2014 and stole the personal information of over 65,000 people. The accused had also sold the stolen data on the dark web. The accused, identified as Justin Sean Johnson, aged 30 [...] The post Darknet Data Hack: Hacker Pleads Guilty On Stolen Database Sale appeared first on Dark Web Link | Deep web Onion Links | Darknet News .

DarkSide Gang: The Ransomware Group Now Retires On $90 Million

The DarkSide Gang, one of the most prominent ransomware groups, has extorted over $90 million in Bitcoin (BTC). Following this, they had allegedly discontinued its illegal operations, as new research states. Analysts at Elliptic, a London-based blockchain analytics firm, had mentioned in a report published on Tuesday that they had unearthed a now-empty cryptocurrency wallet. The [...] The post DarkSide Gang: The Ransomware Group Now Retires On $90 Million appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

Dark Web Dealer For Carfentanil Now Received 11 Years Imprisonment

A Kelowna based dark web dealer for drugs who had operated a pretty sophisticated carfentanil and fentanyl trafficking has been imprisoned. His appeal by the B.C's highest court had been coherently denied. The imprisoned dark web dealer was a father aged 38 years bearing the name James Shawn Nelson. The imprisoned had no prior criminal [...] The post Dark Web Dealer For Carfentanil Now Received 11 Years Imprisonment appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Cisco&#8239;Releases Security Updates for Multiple&#8239;Products&#8239;&#8239;
* Update to CISA-FBI Joint Cybersecurity Advisory on DarkSide Ransomware
* CISA Publishes Eviction Guidance for Networks Affected by SolarWinds and AD/M365 Compromise
* WordPress Releases Security Update
* Adobe Releases Security Updates for Multiple&#8239;Products&#8239;
* Microsoft Releases May 2021 Security Updates
* Citrix Releases Security Updates for Workspace App for Windows
* Juniper Networks Releases Security Updates
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for
* Vulnerability Summary for the Week of May 10, 2021
* Vulnerability Summary for the Week of May 3, 2021

Zero Day Initiative Advisories

ZDI-CAN-13556: 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: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13887: 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: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13886: Trend Micro
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) and Simon Zuckerbraun of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13885: Trend Micro
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) and Simon Zuckerbraun of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13861: Trend Micro
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: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13874: Trend Micro

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) and Simon Zuckerbraun of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-05-21, 3 days ago. The vendor is given until 2021-09-18 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-13558: 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: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13875: 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: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13817: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13777: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13776: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13773: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13775: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13770: Siemens

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 'xina1i' was reported to the affected vendor on: 2021-05-19, 5 days ago. The vendor is given until 2021-09-16 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-13425: VMware

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L) severity vulnerability discovered by 'Sergey Gerasimov of Solidlab' was reported to the affected vendor on: 2021-05-18, 6 days ago. The vendor is given until 2021-09-15 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-13426: VMware

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 'Sergey Gerasimov of Solidlab' was reported to the affected vendor on: 2021-05-18, 6 days ago. The vendor is given until 2021-09-15 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-12789: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12870: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12787: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12784: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12866: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12786: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12871: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12785: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 11 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Red Hat Security Advisory 2021-2077-01

Red Hat Security Advisory 2021-2077-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include buffer overflow, denial of service, and memory leak vulnerabilities.

Red Hat Security Advisory 2021-2070-01

Red Hat Security Advisory 2021-2070-01 - 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 7.4.7 serves as a replacement for Red Hat Single Sign-On 7.4.6, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-2063-01

Red Hat Security Advisory 2021-2063-01 - 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 7.4.7 serves as a replacement for Red Hat Single Sign-On 7.4.6, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Red Hat Security Advisory 2021-2064-01

Red Hat Security Advisory 2021-2064-01 - 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 7.4.7 serves as a replacement for Red Hat Single Sign-On 7.4.6, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Red Hat Security Advisory 2021-2065-01

Red Hat Security Advisory 2021-2065-01 - 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 7.4.7 serves as a replacement for Red Hat Single Sign-On 7.4.6, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Red Hat Security Advisory 2021-2061-01

Red Hat Security Advisory 2021-2061-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-2053-01

Red Hat Security Advisory 2021-2053-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications.

Ubuntu Security Notice USN-4962-1

Ubuntu Security Notice 4962-1 - It was discovered that Babel incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.

Red Hat Security Advisory 2021-2046-01

Red Hat Security Advisory 2021-2046-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution and information leakage vulnerabilities.

Ubuntu Security Notice USN-4963-1

Ubuntu Security Notice 4963-1 - It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash or hand, resulting in a denial of service.

Red Hat Security Advisory 2021-2047-01

Red Hat Security Advisory 2021-2047-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution and information leakage vulnerabilities.

Red Hat Security Advisory 2021-2048-01

Red Hat Security Advisory 2021-2048-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution and information leakage vulnerabilities.

Red Hat Security Advisory 2021-1552-01

Red Hat Security Advisory 2021-1552-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.11.

Red Hat Security Advisory 2021-2051-01

Red Hat Security Advisory 2021-2051-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution and information leakage vulnerabilities.

Red Hat Security Advisory 2021-1551-01

Red Hat Security Advisory 2021-1551-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.11. Issues addressed include a resource exhaustion vulnerability.

Ubuntu Security Notice USN-4961-1

Ubuntu Security Notice 4961-1 - It was discovered that pip incorrectly handled unicode separators in git references. A remote attacker could possibly use this issue to install a different revision on a repository.

Ubuntu Security Notice USN-4960-1

Ubuntu Security Notice 4960-1 - Etienne Champetier discovered that runC incorrectly checked mount targets. An attacker with a malicious container image could possibly mount the host filesystem into the container and escalate privileges.

Red Hat Security Advisory 2021-2033-01

Red Hat Security Advisory 2021-2033-01 - X.Org is an open-source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2021-2032-01

Red Hat Security Advisory 2021-2032-01 - The slapi-nis packages contain the NIS server plug-in and the Schema Compatibility plug-in for use with the 389 Directory Server. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2042-01

Red Hat Security Advisory 2021-2042-01 - Red Hat OpenShift Container Storage is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Container Storage is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-2034-01

Red Hat Security Advisory 2021-2034-01 - Redis is an advanced key-value store. It is often referred to as a data-structure server since keys can contain strings, hashes, lists, sets, and sorted sets. For performance, Redis works with an in-memory data set. You can persist it either by dumping the data set to disk every once in a while, or by appending each command to a log. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2036-01

Red Hat Security Advisory 2021-2036-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.203 and .NET Runtime 5.0.6. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2021-2026-01

Red Hat Security Advisory 2021-2026-01 - Red Hat Identity Management is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2025-01

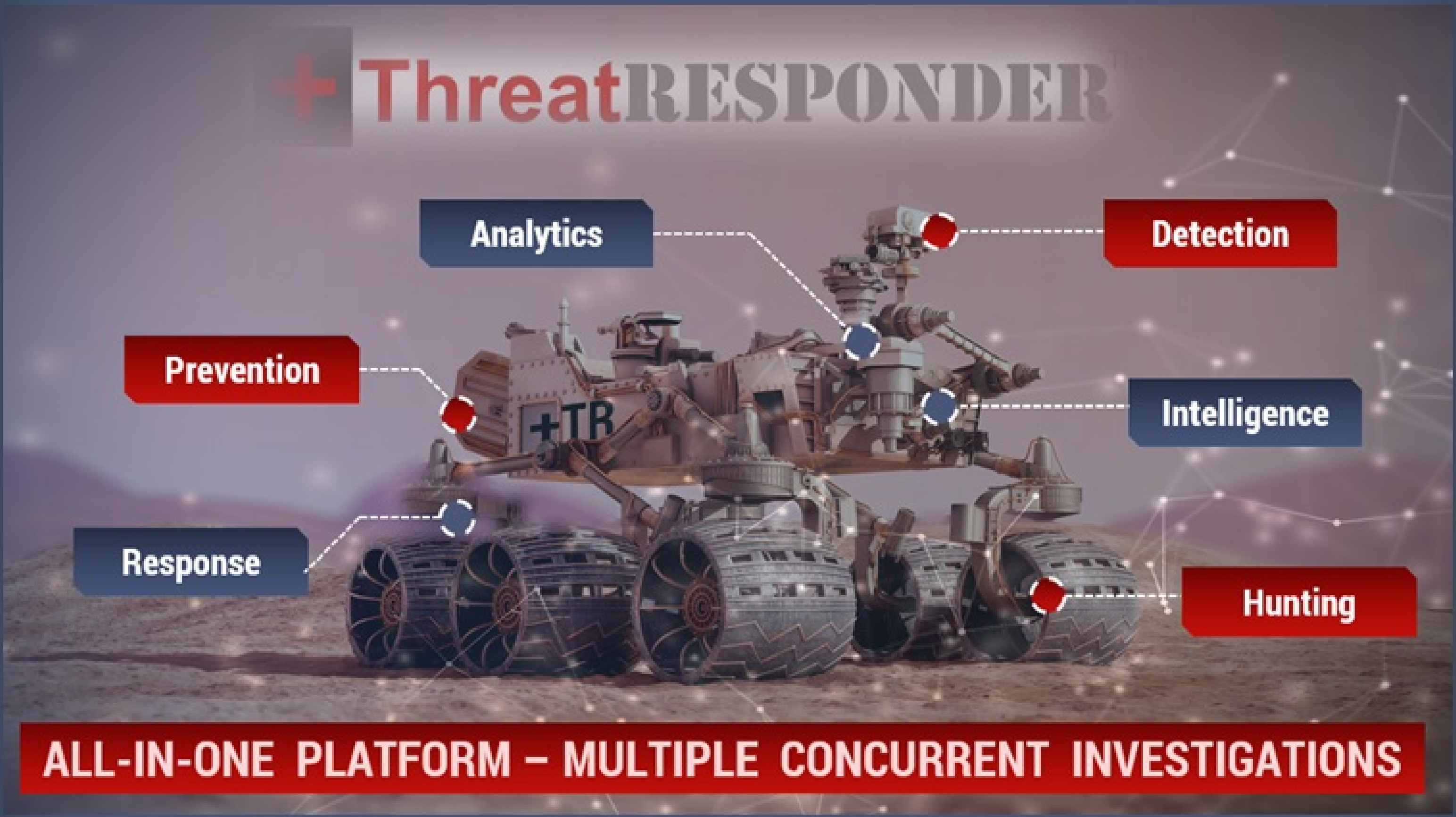
Red Hat Security Advisory 2021-2025-01 - Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects. Issues addressed include a HTTP request smuggling vulnerability.

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: 2021.1

Download here.

CSI Linux 2021.1 is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux 2021.1 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 2021.2 BETA Release:

CSI Linux 2021.2 Beta is now availible for those that have 2021.1 installed. To upgrade, open the CLI and type:

```
wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh
```

CSI Linux Tutorials for 2021.1:

PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

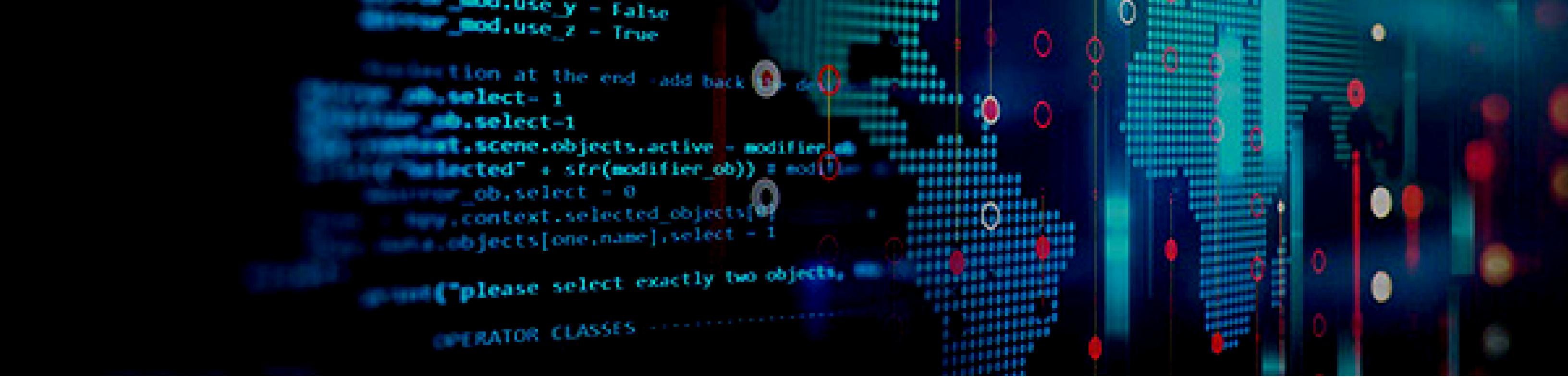
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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

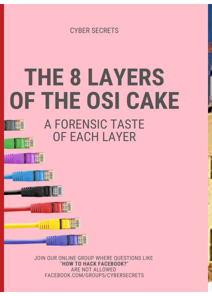


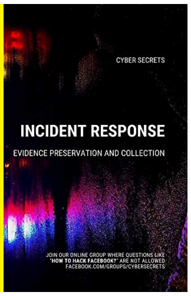
The Cyber Secrets publications on Amazon

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.

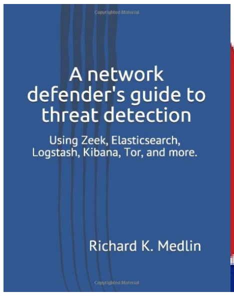
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

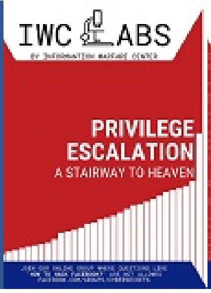
CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel

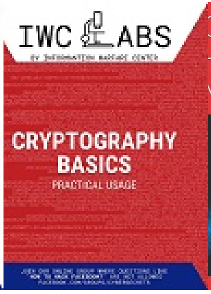


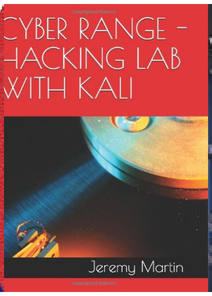


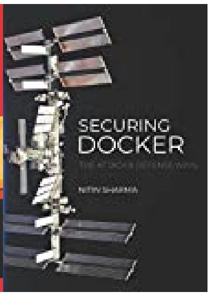
Other Publications from Information Warfare Center











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