Sep-27-21

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

September 27, 2021

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

Internet Storm Center Infocon Status

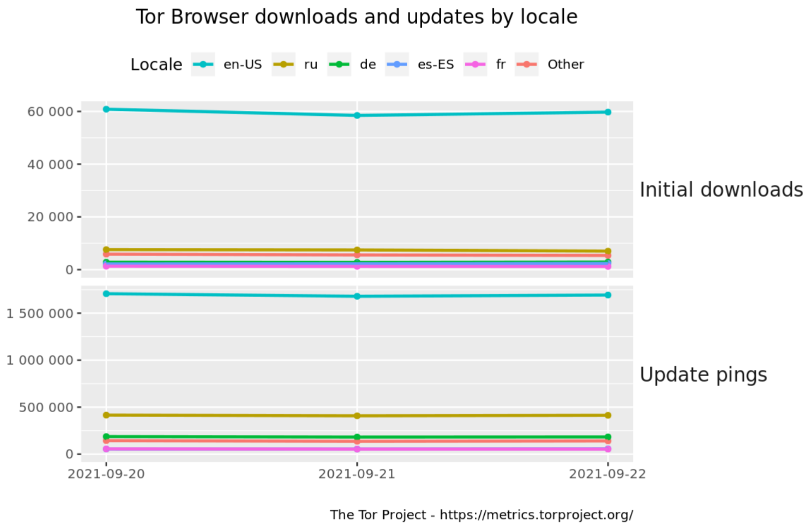
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. [amzn.to/2UuIG9B]()

Cyber Secrets was originally a video series and is on both [YouTube]().

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



Interesting News

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

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

*** CSI Linux 2021.2 has just been released! Download today! [csilinux.com]()

Index of Sections

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

* 100M IoT Devices Exposed By Zero-Day Bug
* Apple Patches 3 More Zero-Days Under Active Attack
* China Declares All Crypto-Currency Transactions Illegal
* FBI Withheld Ransomware Key From Businesses Over A Sting
* FamousSparrow APT Spies On Hotels, Governments
* Will Crypto Exchange Sanctions Slow Ransomware?
* ExpressVPN Employees Question Company About Exec Working For UAE Spy Unit
* VoIP Company Battles Massive Random DDoS Attack
* Facebook May Have Paid Off The FTC To Protect Zuckerberg From Cambridge Analytica Scandal
* How The Mafia Is Pivoting To Cybercrime
* TikTok, GitHub, Facebook Join Open Source Bug Bounty
* Confluence Code Exec Flaw Being Used By Crypto Miners
* $5.9 Million Ransomware Attack On Farming Cooperative May Cause Food Shortage
* Siemens Launches AI Solution To Fight Industrial Cybercrime
* HackerOne Expands To Tackle Open Source Projects
* Nation-State Group Breaches Alaska Department Of Health
* BSidesSF Call For Papers Announced
* FBI Says $133 Million Lost In Romance Scams In 2021
* Epik Data Breach Affects 15 Million Users, Including Non-Customers
* Google Announces Major Privacy Change Coming To Android
* Police Announce Huge Bust Of Mafia's Cyber Crime Operations
* Cryptocurrency Launchpad Hit By $3 Million Supply Chain Attack
* Telegram Emerges As New Dark Web For Cyber Criminals
* Tesla To Work With Global Regulators On Data Security
* Microsoft MSHTML Flaw Exploited By Ryuk Ransomware Gang

Krebs on Security

* Indictment, Lawsuits Revive Trump-Alfa Bank Story
* Does Your Organization Have a Security.txt File?
* Trial Ends in Guilty Verdict for DDoS-for-Hire Boss
* Customer Care Giant TTEC Hit By Ransomware
* Microsoft Patch Tuesday, September 2021 Edition
* 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

LATEST NEWS

Dark Reading

* What Is the Difference Between Security and Resilience?
* Consumers Share Security Fears as Risky Behaviors Persist
* TangleBot Campaign Underscores SMS Threat
* Contrast Application Security Platform Scales to Support OWASP Risks
* Our Eye Is on the SPARROW
* Endpoint Still a Prime Target for Attack
* Google Spots New Technique to Sneak Malware Past Detection Tools
* Primer: Microsoft Active Directory Security for AD Admins
* FamousSparrow APT Group Flocks to Hotels, Governments, Businesses
* SAIC Appoints Kevin Brown as Chief Information Security Officer
* Supply Chain and Ransomware Threats Drove 60% Increase in Global Cyber Intelligence Sharing Among Fin
* BlackFog ARM 64 Edition Provides Anti Data Exfiltration Across New Patforms
* Apple Patches Zero-Days in iOS, Known Vuln in macOS
* Microsoft Exchange Autodiscover Flaw Leaks Thousands of Credentials
* How to Implement a Security Champions Program
* Panorays Closes $42 Million Series B Funding Round
* NIST Brings Threat Modeling into the Spotlight
* Password Reuse Problems Persist Despite Known Risks
* What Are the Different Types of Cyber Insurance?
* 6 Lessons From Major Data Breaches This Year
* Who Is BlackMatter?
* UK MoD Data Breach Shows Cybersecurity Must Protect Both People and Data
* A Cyber-Resilience Model for the Next Era
* Strained Relationships Hinder DevSecOps Innovation
* CISA, FBI, NSA Warn of Increase in Conti Ransomware Attacks

The Hacker News

* A New Jupyter Malware Version is Being Distributed via MSI Installers
* Urgent Chrome Update Released to Patch Actively Exploited Zero-Day Vulnerability
* SonicWall Issues Patches for a New Critical Flaw in SMA 100 Series Devices
* A New APT Hacker Group Spying On Hotels and Governments Worldwide
* Apple's New iCloud Private Relay Service Leaks Users' Real IP Addresses
* Google Warns of a New Way Hackers Can Make Malware Undetectable on Windows
* Cisco Releases Patches 3 New Critical Flaws Affecting IOS XE Software
* Urgent Apple iOS and macOS Updates Released to Fix Actively Exploited Zero-Days
* Microsoft Exchange Bug Exposes ~100,000 Windows Domain Credentials
* A New Bug in Microsoft Windows Could Let Hackers Easily Install a Rootkit
* Why You Should Consider QEMU Live Patching

* New Android Malware Targeting US, Canadian Users with COVID-19 Lures
* Colombian Real Estate Agency Leak Exposes Records of Over 100,000 Buyers
* Microsoft Warns of a Wide-Scale Phishing-as-a-Service Operation
* New Nagios Software Bugs Could Let Hackers Take Over IT Infrastructures

LATEST NEWS

Security Week

* Threat Actor Targets Indian Government With Commercial RATs
* States at Disadvantage in Race to Recruit Cybersecurity Pros
* EU Denounces Alleged Russian Hacking Ahead of German Vote
* FamousSparrow Cyberspies Exploit ProxyLogon in Attacks on Governments, Hotels
* Google Says Threat Actors Using New Code Signing Tricks to Evade Detection
* SonicWall Patches Critical Vulnerability in SMA Appliances
* LG to Acquire Vehicle Cybersecurity Firm Cybellum
* CISA Opens IPv6 Guidance to Public Feedback
* Port of Houston Target of Suspected Nation-State Hack
* F5 to Acquire Threat Stack for $68 Million in Cash
* Working Securely From Anywhere With Zero Trust
* Apple Confirms New Zero-Day Attacks on Older iPhones
* Improving Security Posture to Lower Insurance Premiums
* Web Security Provider Jscrambler Raises $15 Million
* Report: Suspected Chinese Hack Targets Indian Media, Gov't
* Apple Deprecates Outdated TLS Protocols in iOS, macOS
* Third-Party Risk Management Firm Panorays Raises $42 Million
* Cisco Patches Critical Vulnerabilities in IOS XE Software
* VMware vCenter Servers in Hacker Crosshairs After Disclosure of New Flaw
* Attacks on Russian Government Orgs Exploit Recent Microsoft Office Zero-Day
* Facebook Ad Business Hit by New Apple Privacy Rules
* U.S. Issues Conti Alert as Second Farming Cooperative Hit by Ransomware
* Lithuanian Agency Warns Against Use of Chinese-made Phones
* Netgear Patches Remote Code Execution Flaw in SOHO Routers

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

* WHAT IS XDR (EXTENDED DETECTION AND RESPONSE)?
* Newest iPhone Launch is Now a Scammer's Advantage
* KnowBe4 Named a Leader in the Fall 2021 G2 Grid Report for Security Awareness Training
* [HEADS UP] Millions of malicious emails will slip past security filters in Q4
* Executives: Ransomware is the Greatest Threat Concern, But Few are Actually Prepared
* Travel-Related Phishing Scams and Websites Surge More Than 400%
* $1 Trillion Infrastructure Bill is the Catalyst for DOT-Impersonated Phishing Attacks Targeting Contr
* Social Media Quizzes May Be Data Scrapers Building Victim Profiles
* Kaspersky: Use of New QakBot Banking Trojan that Steals Emails Up 65%
* FBI Warns of Continued Ransomware Attacks Targeting the Food and Agriculture Sectors

ISC2.org Blog

* CISSPs from Around the Globe: An Interview with AJ Yawn
* Exclusive Resources and Discounts From Your (ISC)&sup2; Membership
* Ensuring Disaster Recovery and Business Continuity in the Cloud
* The Importance of Adopting a Risk Management Approach to Security and Privacy
* CCSP vs. Professional Cloud Security Manager: How Do They Compare?

HackRead

* Top 3 Ways to Find a Hidden File on a Mac
* Lithuania wants users to dump Chinese phones citing data collection
* Hackers hit Russian ministry, rocket center using MSHTML vulnerability
* Millions impacted as payment API vulnerabilities exposing transaction keys
* Google, Microsoft and Oracle generated most vulnerabilities in 2021
* New version of Jupyter infostealer delivered through MSI installer
* Netflix errors - How to fix them

Koddos

* Top 3 Ways to Find a Hidden File on a Mac
* Lithuania wants users to dump Chinese phones citing data collection
* Hackers hit Russian ministry, rocket center using MSHTML vulnerability
* Millions impacted as payment API vulnerabilities exposing transaction keys
* Google, Microsoft and Oracle generated most vulnerabilities in 2021
* New version of Jupyter infostealer delivered through MSI installer
* Netflix errors - How to fix them

LATEST NEWS

Naked Security

* S3 Ep51: OMIGOD a gaping hole, waybill scams, and Face ID hacked [Podcast]
* STILL ALIVE! iOS 12 gets 3 zero-day security patches - update now
* How Outlook "autodiscover" could leak your passwords - and how to stop it
* VMware patch bulletin warns: "This needs your immediate attention."
* iOS 15 launches with 22 documented security patches - including a Face ID bypass using a "3D model"
* "Back to basics" as courier scammers skip fake fees and missed deliveries
* OMIGOD, an exploitable hole in Microsoft open source code!
* S3 Ep50: Two 0-days plus another 0-day plus a fast food bug [Podcast]
* Apple products vulnerable to FORCEDENTRY zero-day attack - patch now!
* Serious Security: How to make sure you don't miss bug reports!

Threat Post

* Exchange/Outlook Autodiscover Bug Spills $100K+ Email Passwords
* TangleBot Malware Reaches Deep into Android Device Functions
* Critical Cisco Bugs Allow Code Execution on Wireless, SD-WAN
* Apple Patches 3 More Zero-Days Under Active Attack
* REvil Affiliates Confirm: Leadership Were Cheating Dirtbags
* 5 Tips for Achieving Better Cybersecurity Risk Management
* 100M IoT Devices Exposed By Zero-Day Bug
* FamousSparrow APT Wings in to Spy on Hotels, Governments
* Google Report Spotlights Uptick in Controversial 'Geofence Warrants' by Police
* Acronis Offers up to $5,000 to Users Who Spot Bugs in Its Cyber Protection Products

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

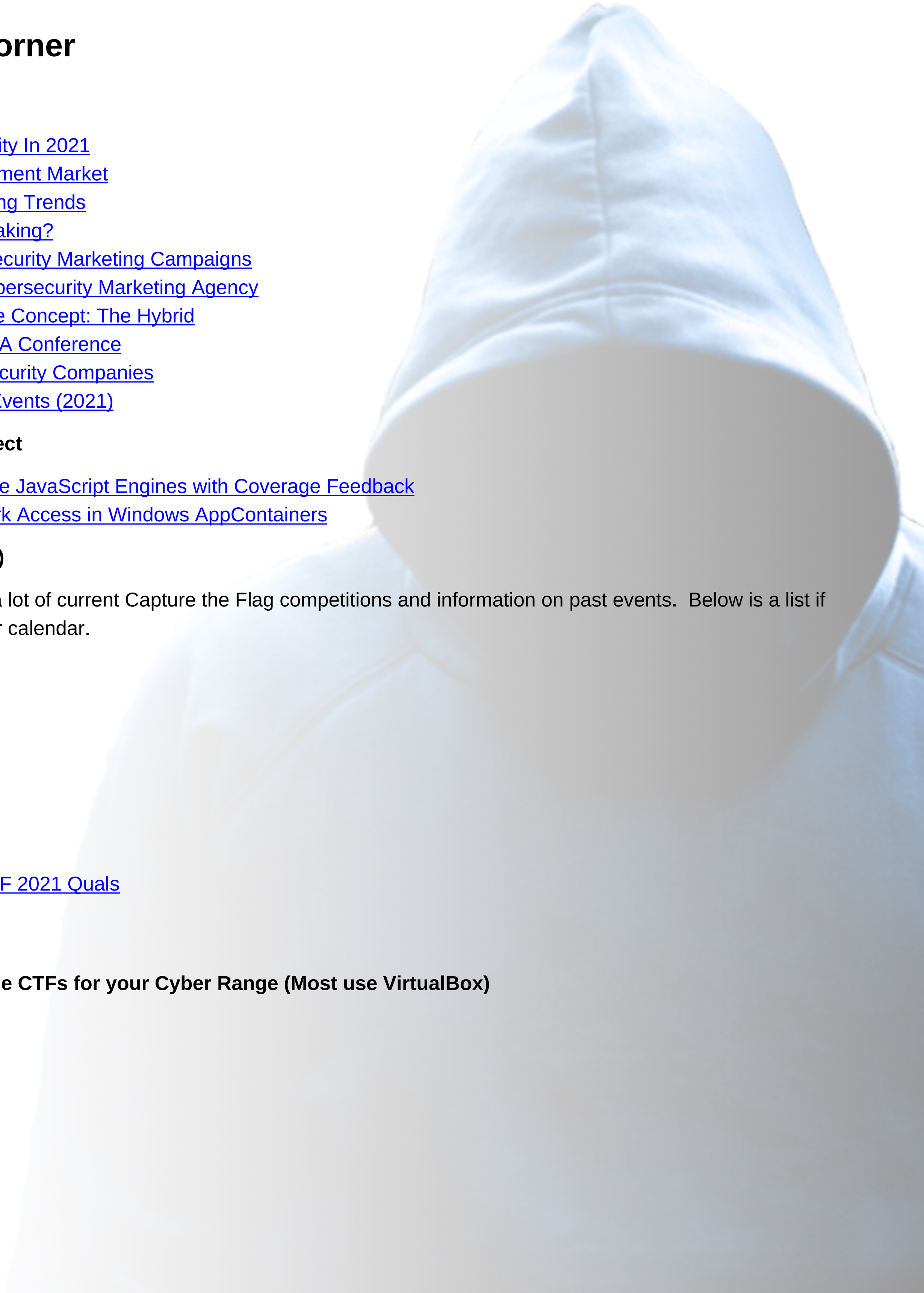
* Zero Trust: Remote Security For Now and the Future
* How Privileged Access Management Fits Into a Layered Security Strategy
* What is Web Application Security? A Protective Primer for Security Professionals
* New ZE Loader Targets Online Banking Users
* How to Build a Winning Cybersecurity Resume
* The CISO and the C-Suite: How to Achieve Better Working Relations
* 12 Benefits of Hiring a Certified Ethical Hacker
* Cybersecurity Solutions to Know in 2021: Open Source and Scaling Up
* Identity Management Beyond the Acronyms: Which Is Best for You?
* Zero Trust: Follow a Model, Not a Tool

InfoWorld

* What's new in Angular 13
* Move faster with continuous security scanning in the cloud
* Deis Labs unveils Hippo PaaS for WebAssembly
* 6 great new Java features you don't want to miss
* Easy racing bar charts in R with ddplot
* Swift 5.5 introduces async/await, structured concurrency, and actors
* Open source skills only got hotter during the pandemic
* Get started with Go testing
* Working with Azure Managed Instance for Cassandra
* How to choose the right data visualization tools for your apps

C4ISRNET - Media for the Intelligence Age Military

* Could solar panels in space power Army operations on Earth?
* Here are the cheap counter-drone solutions DoD tested in the Arizona desert
* US Army moves to full-rate production on tactical radios essential for multidomain operations
* Space Force to share internal digital models with industry
* Soldiers with this Stryker unit test tool to 'see' the electronic battlefield
* Air Force software tool helped coordinate Afghanistan evacuation of civilians
* Watchdog expects delays to Space Force's next missile warning satellites
* Army bomb techs field test new aerial drone
* Northrop tests interoperability between advanced airborne radar and electronic warfare system
* UAE, Britain ink defense research and AI tech deals. Here's what comes next.



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

* Fuzzing Closed-Source JavaScript Engines with Coverage Feedback
* Understanding Network Access in Windows AppContainers

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.

* DeconstruCT.F 2021
* TastelessCTF 2021
* TSG CTF 2021
* Sacramentum
* RuCTF 2021
* pbctf 2021
* DamCTF 2021
* SPbCTF's Student CTF 2021 Quals
* DEADFACE CTF
* iCTF

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

* doubletrouble: 1
* Beelzebub: 1
* Vikings: 1
* DarkHole: 2
* Deathnote: 1

Tools & Techniques

Packet Storm Security Tools Links

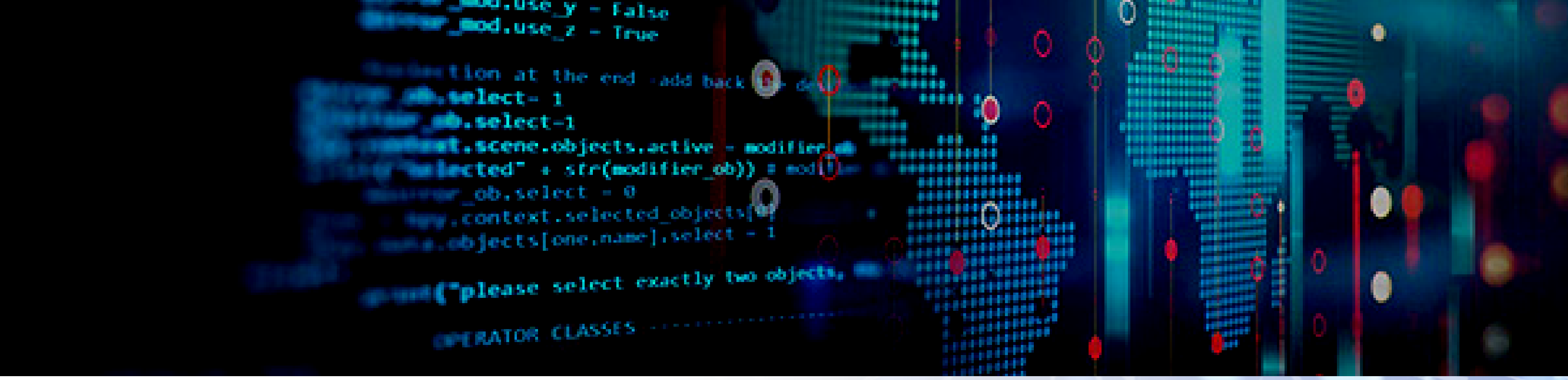
* Zeek 4.0.4
* Proxmark 4.14434
* litefuzz 1.0
* GNU Privacy Guard 2.2.31
* OpenDNSSEC 2.1.10
* Packet Fence 11.0.0
* Samhain File Integrity Checker 4.4.6
* Clam AntiVirus Toolkit 0.104.0
* SQLMAP - Automatic SQL Injection Tool 1.5.9
* nfstream 6.3.4

Kali Linux Tutorials

* Plution : Prototype Pollution Scanner Using Headless Chrome
* Ntlm_Theft : A Tool For Generating Multiple Types Of NTLMv2 Hash Theft Files
* DNSTake : A Fast Tool To Check Missing Hosted DNS Zones That Can Lead To Subdomain Takeover
* CVE-2021-40444 PoC : Malicious docx generator to exploit CVE-2021-40444 (Microsoft Office Word Remote
* Kali Linux 2021.3 : Penetration Testing and Ethical Hacking Linux Distribution
* Gokart : A Static Analysis Tool For Securing Go Code
* Vailyn : A Phased, Evasive Path Traversal + LFI Scanning & Exploitation Tool In Python
* Rootend : A *Nix Enumerator And Auto Privilege Escalation Tool
* BoobSnail : Allows Generating Excel 4.0 XLM Macro
* Peirates : Kubernetes Penetration Testing Tool

GBHackers Analysis

* Critical RCE Flaw in the core Netgear Firmware Let Remote Attackers to Take Control of an Affected Sy
* Apple Fixes iMessage Zero-Click Bug That Used to Deploy NSO Pegasus Spyware
* 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



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown | September 2021
* 2021 SANS DFIR Summit Day 2 Wrap Up
* SANS Law Enforcement Appreciation Programs
* 2021 SANS DFIR Summit Day 1 Wrap Up Panel

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelg&auml;nger Your H&auml;x Dollars at Work
* DEF CON 29 Red Team Village - CTF Day 2
* DEF CON 29 Recon Village - Ben S - Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

Hak5

* HakByte: Set Up a Headless Raspberry Pi Wardriving Rig
* What Does ExpressVPN Have To Do With The UAE's Project Raven? - ThreatWire
* HakByte: Create a $15 WarDriving Rig to Log WiFi Data w/ the ESP8266

The PC Security Channel [TPSC]

* Linux Ransomware
* Top 5 most dangerous Ransomware

Eli the Computer Guy

* Layered Network Introduction (Cyber Security Part 5)
* Office Hours - Tech Question and Answers
* Office Hours with Guest Host Martin Lehner (MSP Owner in the Yukon)
* Honeypot Introduction (Cyber Security Series)

Security Now

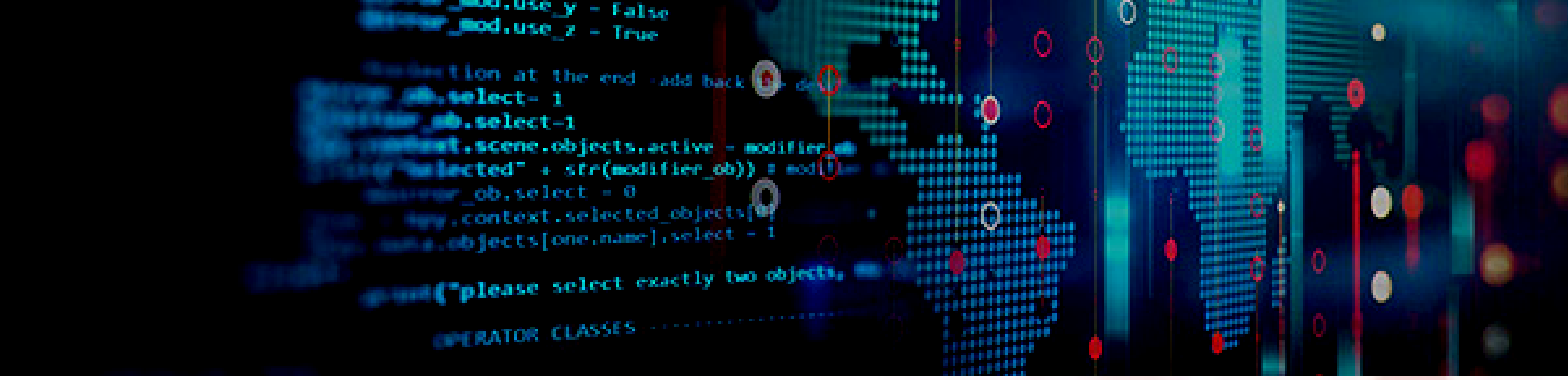
* Cobalt Strike - Android Auto-Revokes Permissions, DDoS on VoIP.ms, Patch Tuesday, Was GRC Pwned?
* The M&#275;ris Botnet - 0-Day Attack on Office Docs, WFH and Security, Return of REvil

Troy Hunt

* Weekly Update 262

Intel Techniques: The Privacy, Security, & OSINT Show

* 235-iOS 15 Privacy Guide
* 234-Privacy, Security, & OSINT Updates



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

* "Bom" Skimmer is Magecart Group 7's Latest Model
* Untangling the Spider Web
* Flowspec Bulletproof Services Enable Cybercrime Worldwide
* RiskIQ Analysis Links EITest 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

FireEye

* Metasploit Wrap-Up
* Ransomware: Is Critical Infrastructure in the Clear?
* Easier URI Targeting With Metasploit Framework
* Rapid7 Technical Support: Building a Career Path With Endless Possibilities
* Critical vCenter Server File Upload Vulnerability (CVE-2021-22005)
* Rapid7 Statement on the New Standard Contractual Clauses for International Transfers of Personal Data
* Login Authentication Goes Automated With New InsightAppSec Improvements
* Metasploit Wrap-Up
* SANS 2021 Threat Hunting Survey: How Organizations' Security Postures Have Evolved in the New Normal
* The Ransomware Killchain: How It Works, and How to Protect Your Systems

Proof of Concept (PoC) & Exploits

Packet Storm Security

* OpenVPN Monitor 1.1.3 Cross Site Request Forgery
* OpenVPN Monitor 1.1.3 Command Injection
* OpenVPN Monitor 1.1.3 Authorization Bypass / Denial Of Service
* SmarterTools SmarterTrack 7922 Information Disclosure
* WordPress 3DPrint Lite 1.9.1.4 Shell Upload
* Pharmacy Point Of Sale System 1.0 SQL Injection
* Police Crime Record Management Project 1.0 SQL Injection
* Redragon Gaming Mouse Denial Of Service
* WordPress Advanced Order Export For WooCommerce 3.1.7 Cross Site Scripting
* WordPress Fitness Calculators 1.9.5 Cross Site Request Forgery
* Backdrop CMS 1.20.0 Cross Site Request Forgery / Command Execution
* Gurock Testrail 7.2.0.3014 Improper Access Control
* Chrome HRTFDatabaseLoader::WaitForLoaderThreadCompletion Data Race
* OpenCats 0.9.4-2 XML Injection
* E-Negosyo System 1.0 Shell Upload
* E-Negosyo System 1.0 SQL Injection
* e107 CMS 2.3.0 Shell Upload
* Online Reviewer System 1.0 Shell Upload
* South Gate Inn Online Reservation System 1.0 Shell Upload / SQL Injection
* Sentry 8.2.0 Remote Code Execution
* Filerun 2021.03.26 Remote Code Execution
* TotalAV 5.15.69 Unquoted Service Path
* Simple Attendance System 1.0 SQL Injection
* Cloudron 6.2 Cross Site Scripting
* ManageEngine OpManager SumPDU Java Deserialization

CXSecurity

* Apartment Visitor Management System (AVMS) 1.0 SQLi to RCE
* Ulfius Web Framework Remote Memory Corruption
* AHSS-PHP 1.0 Cross Site Scripting / SQL Injection
* 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

Proof of Concept (PoC) & Exploits

Exploit Database

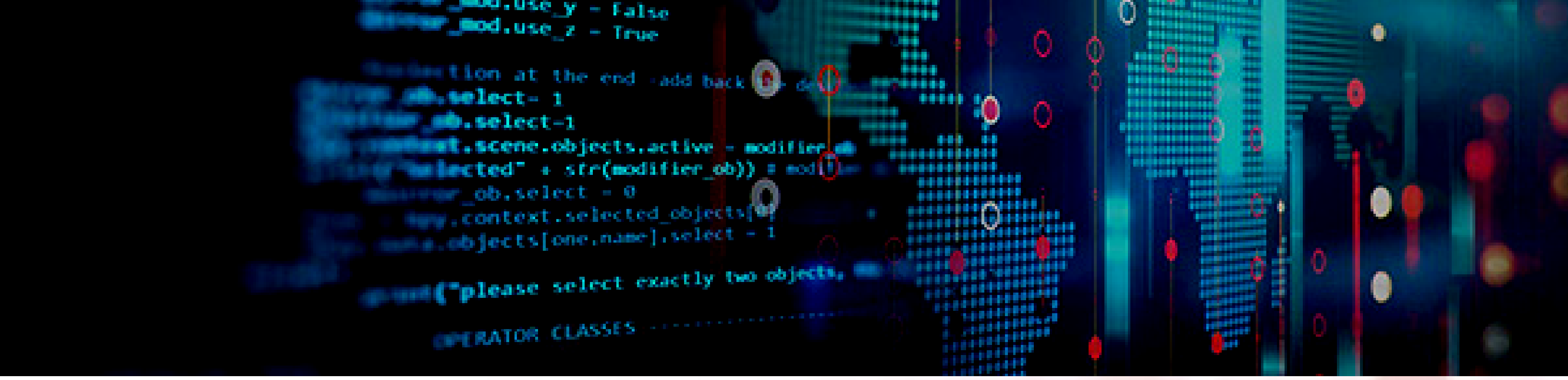
* [local] Cyberfox Web Browser 52.9.1 - Denial-of-Service (PoC)
* [remote] Cisco small business RV130W 1.0.3.44 - Inject Counterfeit Routers
* [webapps] Library System 1.0 - 'student_id' SQL injection (Authenticated)
* [webapps] WordPress Plugin Wappointment 2.2.4 - Stored Cross-Site Scripting (XSS)
* [local] Ether_MP3_CD_Burner 1.3.8 - Buffer Overflow (SEH)
* [local] Microsoft Windows cmd.exe - Stack Buffer Overflow
* [webapps] Pharmacy Point of Sale System 1.0 - SQLi Authentication BYpass
* [webapps] SmarterTools SmarterTrack 7922 - 'Multiple' Information Disclosure
* [webapps] Police Crime Record Management Project 1.0 - Time Based SQLi
* [webapps] Budget and Expense Tracker System 1.0 - Arbitrary File Upload
* [webapps] WordPress Plugin Fitness Calculators 1.9.5 - Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin Advanced Order Export For WooCommerce 3.1.7 - Reflected Cross-Site Scripti
* [webapps] Backdrop CMS 1.20.0 - 'Multiple' Cross-Site Request Forgery (CSRF)
* [dos] Redragon Gaming Mouse - 'REDRAGON_MOUSE.sys' Denial-Of-Service (PoC)
* [webapps] Wordpress Plugin 3DPrint Lite 1.9.1.4 - Arbitrary File Upload
* [webapps] Gurock Testrail 7.2.0.3014 - 'files.md5' Improper Access Control
* [webapps] Online Reviewer System 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Sentry 8.2.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Cloudron 6.2 - 'returnTo ' Cross Site Scripting (Reflected)
* [webapps] OpenCats 0.9.4-2 - 'docx ' XML External Entity Injection (XXE)
* [webapps] e107 CMS 2.3.0 - Remote Code Execution (RCE) (Authenticated)
* [local] TotalAV 5.15.69 - Unquoted Service Path
* [webapps] Filerun 2021.03.26 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Simple Attendance System 1.0 - Unauthenticated Blind SQLi

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
```

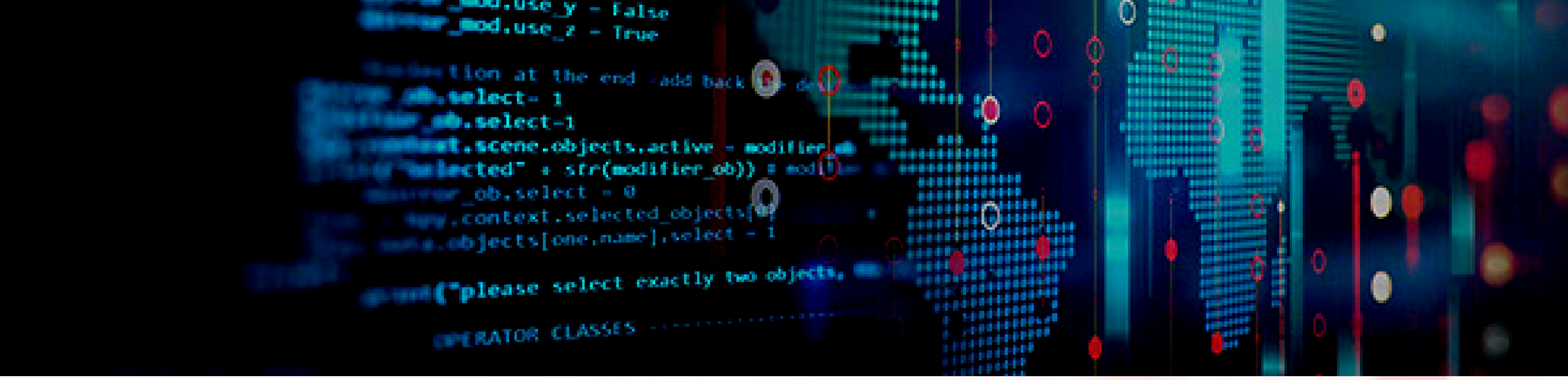
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



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.


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

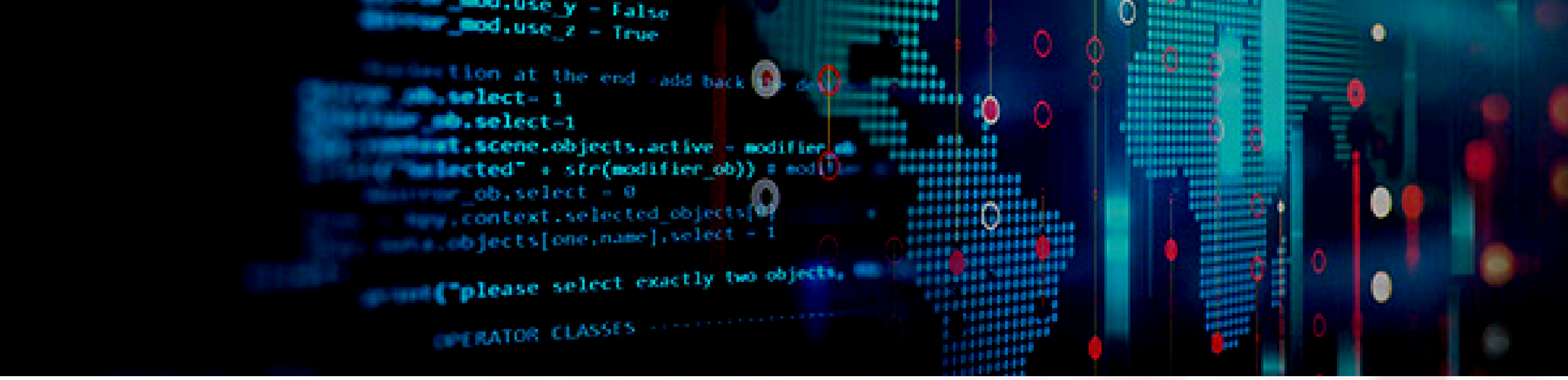
Dark Web News

Darknet Live

[Three Charged in $2 Million Unemployment Fraud Scheme]
Three California residents allegedly conspired to file fraudulent COVID-19 unemployment benefit claims with stolen information from the darkweb. (via darknetlive.com)
13 Arrested in Darkweb Child Abuse Case in Italy
Police in Italy arrested 13 suspects as a result of an investigation into a darkweb child abuse forum. (via darknetlive.com)
Two Arrested in German Darkweb Drug Trafficking Case
German police arrested two suspects for allegedly manufacturing and distributing drugs through the darkweb. (via darknetlive.com)
NL: EncroChat Hack Led to a Spike in Drug Lab Busts
The EncroChat hack resulted in a significant increase in the number of drug labs detected by police in the Netherlands in 2020. (via darknetlive.com)

Dark Web Link

Eastern Europe Sends Additional Crypto To The Dark Web Than Wherever Else
According to research, Eastern Europe contributes the most crypto to the dark web and also provides the most online traffic to fraudulent sites. According to a report by crypto analytics firm Chainalysis, dark net marketplaces established a new sales record in 2020, with $1.7 billion worth of cryptocurrencies. According to Chainalysis, Eastern Europe accounted for [...] The post Eastern Europe Sends Additional Crypto To The Dark Web Than Wherever Else appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
AFP To Mark Child Sex Slayers Sharing Abuse Material
As new rules strengthen investigators' ability to identify criminals, child sex slayerswho coach paedophiles over the dark web on how to harm kids will be targeted by the Australian civic Police. The AFP is issuing a new and unequivocal warning to offenders today: the AFP will seek to deploy new powers under the Surveillance Legislation [...] The post AFP To Mark Child Sex Slayers Sharing Abuse Material appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Us Detains Dark Web Moderator
A person from Southern Illinois was sentenced to 12 years and 7 months in federal prison for moderating a website dedicated to CSAM (child sexual abuse material). In October 2020, a federal grand jury indicted Sparta resident Kory R. Schulein, 37, on a single count of knowingly obtaining CSAM via the internet. Prosecutors said that [...] The post Us Detains Dark Web Moderator appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


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

Advisories

US-Cert Alerts & bulletins

* VMware vCenter Server Vulnerability CVE-2021-22005 Under Active Exploit
* Google Releases Security Updates for Chrome
* Apple Releases Security Updates
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Guidance: IPv6 Considerations for TIC 3.0
* CISA, FBI, and NSA&#8239;Release Joint Cybersecurity Advisory&#8239;on Conti Ransomware&#8239;
* Google Releases Security Updates for Chrome
* NETGEAR Releases Security Updates for RCE Vulnerability
* AA21-265A: Conti Ransomware
* AA21-259A: APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus
* Vulnerability Summary for the Week of September 13, 2021
* Vulnerability Summary for the Week of September 6, 2021

Zero Day Initiative Advisories

ZDI-CAN-15320: Apple
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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15322: 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: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15072: NIKON
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: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15166: NIKON
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: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15321: 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: 2021-09-24, 3 days ago. The vendor is given until

2022-01-22 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-15071: NIKON

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: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15214: NIKON

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: 2021-09-24, 3 days ago. The vendor is given until 2022-01-22 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-15137: Ivanti

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 'chudy' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-15168: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-15169: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-15188: Microsoft

A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'namnp' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-15217: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-15130: Ivanti

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chudy' was reported to the affected vendor on: 2021-09-22, 5 days ago. The vendor is given until 2022-01-20 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-14159: Microsoft

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-09-17, 10 days ago. The vendor is given until 2022-01-15 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-15161: Sante

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: 2021-09-17, 10 days ago. The vendor is given until 2022-01-15 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-14160: Microsoft

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-09-17, 10 days ago. The vendor is given until 2022-01-15 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-14189: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-09-16, 11 days ago. The vendor is given until 2022-01-14 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-14656: TP-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Team FLASHBACK: Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) + Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2021-09-16, 11 days ago. The vendor is given until 2022-01-14 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-14655: TP-Link

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Team FLASHBACK: Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) + Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2021-09-16, 11 days ago. The vendor is given until 2022-01-14 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-15237: Microsoft

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-16, 11 days ago. The vendor is given until 2022-01-14 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-15238: Microsoft

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-09-16, 11 days ago. The vendor is given until 2022-01-14 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-15281: 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: 2021-09-15, 12 days ago. The vendor is given until 2022-01-13 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-15279: 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: 2021-09-15, 12 days ago. The vendor is given until 2022-01-13 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-15254: 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: 2021-09-15, 12 days ago. The vendor is given until 2022-01-13 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

Apple Security Advisory 2021-09-23-2

Apple Security Advisory 2021-09-23-2 - Security Update 2021-006 Catalina addresses a code execution vulnerability.

Red Hat Security Advisory 2021-3660-01

Red Hat Security Advisory 2021-3660-01 - 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 7.4.1 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.0 and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.1 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, and traversal vulnerabilities.

Apple Security Advisory 2021-09-23-1

Apple Security Advisory 2021-09-23-1 - iOS 12.5.5 addresses code execution, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-3658-01

Red Hat Security Advisory 2021-3658-01 - 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 7.4.1 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.0 and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.1 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, and traversal vulnerabilities.

Red Hat Security Advisory 2021-3656-01

Red Hat Security Advisory 2021-3656-01 - 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 7.4.1 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.0 and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.1 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, and traversal vulnerabilities.

Ubuntu Security Notice USN-5089-2

Ubuntu Security Notice 5089-2 - USN-5089-1 updated ca-certificates. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. The ca-certificates package contained a CA certificate that will expire on 2021-09-30 and will cause connectivity issues. This update removes the "DST Root CA X3&rdquo; CA. Various other issues were also addressed.

Ubuntu Security Notice USN-5089-1

Ubuntu Security Notice 5089-1 - The ca-certificates package contained a CA certificate that will expire on 2021-09-30 and will cause connectivity issues. This update removes the "DST Root CA X3&rdquo; CA.

Ubuntu Security Notice USN-5088-1

Ubuntu Security Notice 5088-1 - It was discovered that EDK II incorrectly handled input validation in MdeModulePkg. A local user could possibly use this issue to cause EDK II to crash, resulting in a denial of service, obtain sensitive information or execute arbitrary code. Paul Kehrer discovered that OpenSSL used in EDK II incorrectly handled certain input lengths in EVP functions. An attacker could possibly use this issue to cause EDK II to crash, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-5087-1

Ubuntu Security Notice 5087-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Ubuntu Security Notice USN-5085-1

Ubuntu Security Notice 5085-1 - It was discovered that SQL parse incorrectly handled certain regular expression. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2021-3638-01

Red Hat Security Advisory 2021-3638-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, out of bounds read, path sanitization, and use-after-free vulnerabilities.

Apple Security Advisory 2021-09-20-10

Apple Security Advisory 2021-09-20-10 - iTunes 12.12 for Windows addresses code execution vulnerabilities.

Ubuntu Security Notice USN-5086-1

Ubuntu Security Notice 5086-1 - Johan Almbladh discovered that the eBPF JIT implementation for IBM s390x systems in the Linux kernel miscompiled operations in some situations, allowing circumvention of the BPF verifier. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Apple Security Advisory 2021-09-20-9

Apple Security Advisory 2021-09-20-9 - iTunes U 3.8.3 addresses a code execution vulnerability.

Apple Security Advisory 2021-09-20-8

Apple Security Advisory 2021-09-20-8 - Security Update 2021-005 Catalina addresses buffer overflow, bypass, code execution, denial of service, integer overflow, and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-5073-3

Ubuntu Security Notice 5073-3 - Norbert Slusarek discovered that the CAN broadcast manger protocol implementation in the Linux kernel did not properly initialize memory in some situations. A local attacker could use this to expose sensitive information. Murray McAllister discovered that the joystick device interface in the Linux kernel did not properly validate data passed via an ioctl. A local attacker could use this to cause a denial of service or possibly execute arbitrary code on systems with a joystick device registered. Various other issues were also addressed.

Apple Security Advisory 2021-09-20-7

Apple Security Advisory 2021-09-20-7 - macOS Big Sur 11.6 addresses buffer overflow, bypass, code execution, denial of service, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-3639-01

Red Hat Security Advisory 2021-3639-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, out of bounds read, path sanitization, and use-after-free vulnerabilities.

Apple Security Advisory 2021-09-20-6

Apple Security Advisory 2021-09-20-6 - iOS 14.8 and iPadOS 14.8 addresses code execution, denial of service, integer overflow, and use-after-free vulnerabilities.

Apple Security Advisory 2021-09-20-5

Apple Security Advisory 2021-09-20-5 - Safari 15 addresses code execution vulnerabilities.

Apple Security Advisory 2021-09-20-4

Apple Security Advisory 2021-09-20-4 - Xcode 13 addresses multiple issues in nginx.

Ubuntu Security Notice USN-5071-3

Ubuntu Security Notice 5071-3 - It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. An attacker who could start and control a VM could possibly use this to expose sensitive information or execute arbitrary code. Murray McAllister discovered that the joystick device interface in the Linux kernel did not properly validate data passed via an ioctl. A local attacker could use this to cause a denial of service or possibly execute arbitrary code on systems with a joystick device registered. Various other issues were also addressed.

Apple Security Advisory 2021-09-20-3

Apple Security Advisory 2021-09-20-3 - tvOS 15 addresses code execution and denial of service vulnerabilities.

Apple Security Advisory 2021-09-20-2

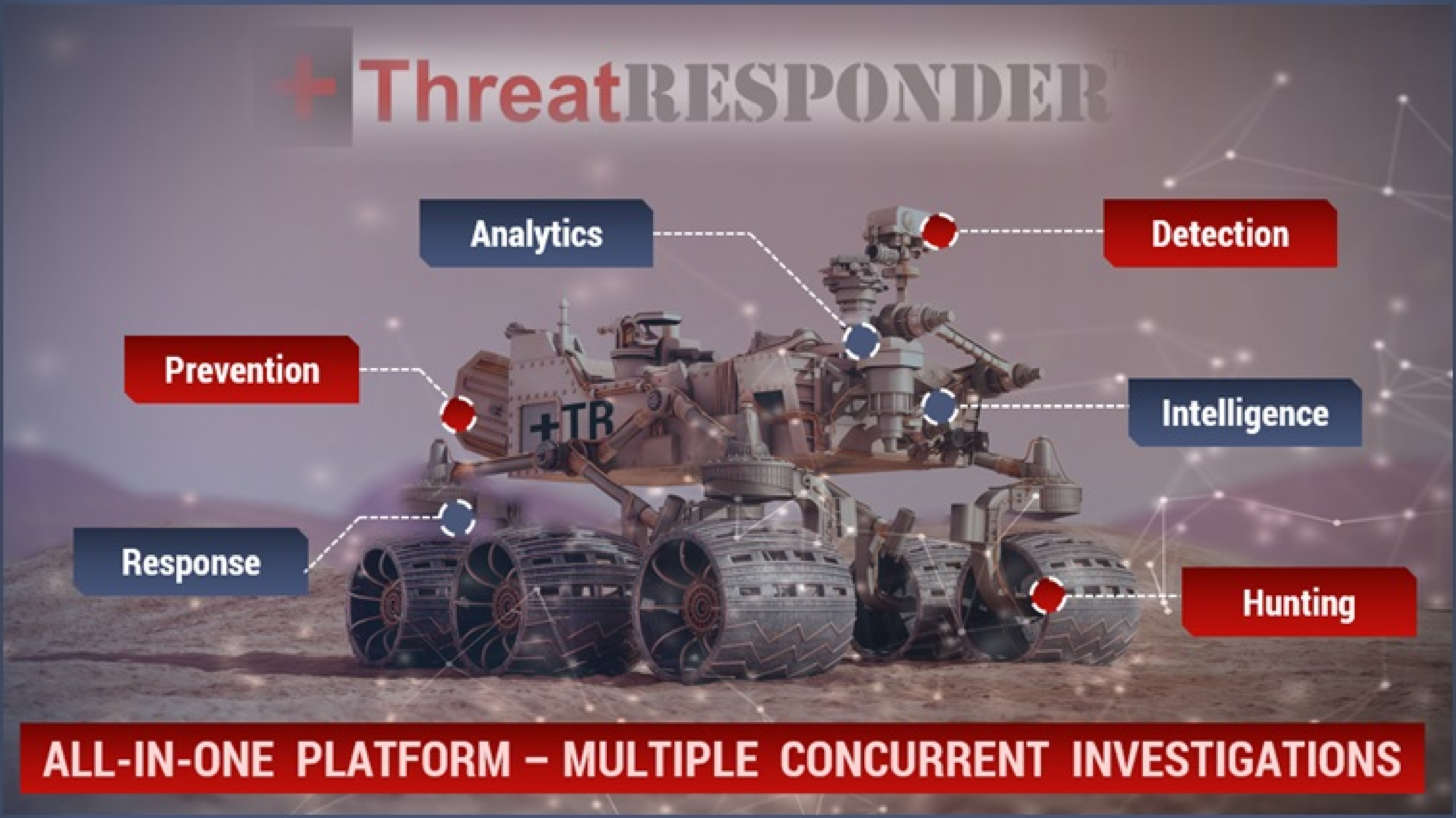
Apple Security Advisory 2021-09-20-2 - watchOS 8 addresses code execution and denial of service vulnerabilities.

Are You…

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

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

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

CSI Linux Tutorials:

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

Cyber Secrets

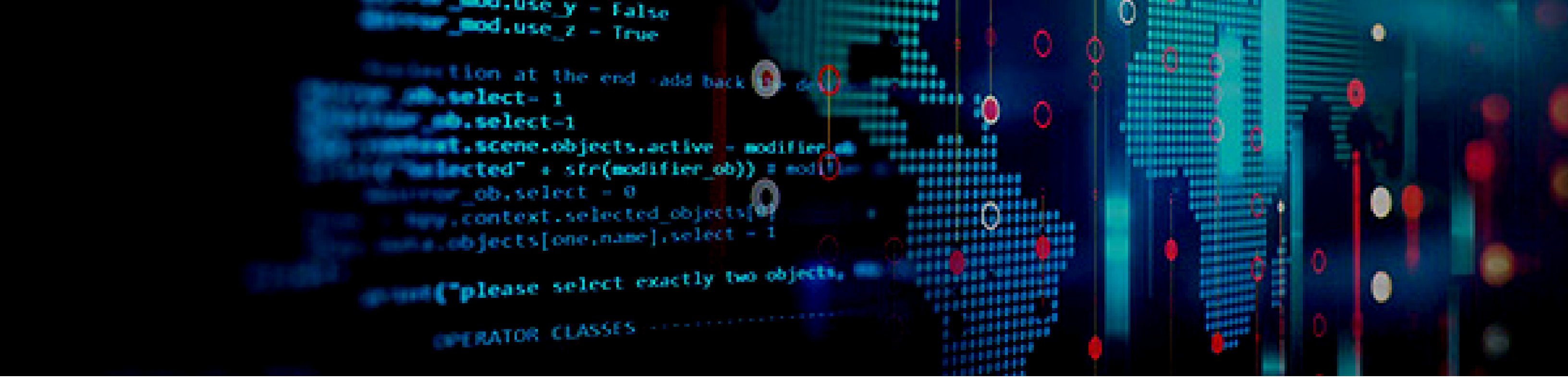
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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

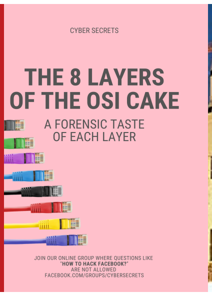


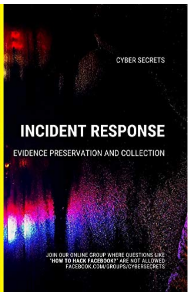
The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

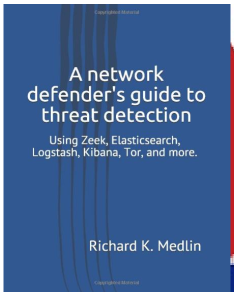
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

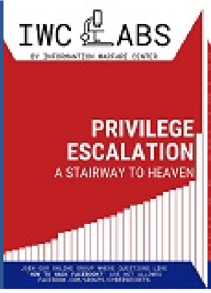
CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube channel

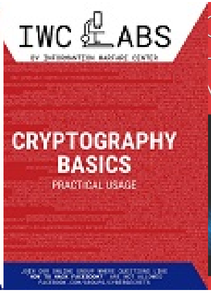


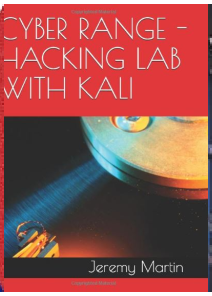


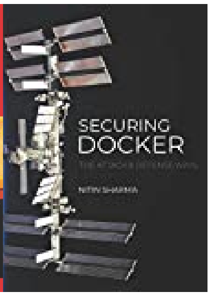
Other Publications from Information Warfare Center











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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP