Aug-30-21

CYBER WEEKLY AWARENESS REPORT

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

netSecurity®

INFORMATION WARFARE CENTER

Si LINUX

ARGOS APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

August 30, 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

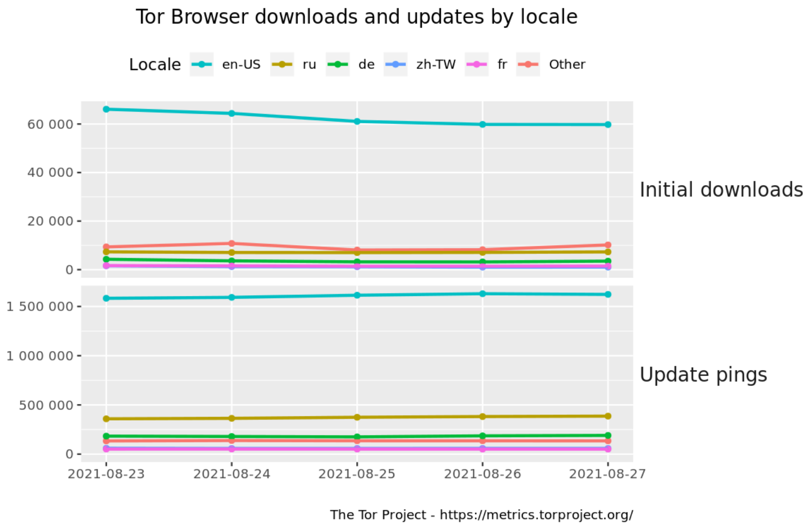
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

LATEST NEWS

Packet Storm Security

* How Data Brokers Sell Access To The Backbone Of The Internet
* Google, Amazon, Microsoft Unveil Massive Cybersecurity Initiatives After White House Meeting
* Realtek Flaw Exposes Dozens Of Brands To Supply Chain Attacks
* Warzone Bans 100,000 Cheaters In Largest Ban Wave Yet
* The Real Victims Of Mass-Crypto Hacks That Keep Happening
* Microsoft Breaks Silence On Barrage Of ProxyShell Attacks
* Proofpoint Wins $14 Million In IP Theft Court Battle
* These Four Rising Gangs Could Be Your Next Major Security Threat
* Custom WhatsApp Build Delivers Triada Malware
* Pegasus Spyware Uses iPhone Zero-Click iMessage Zero-Day
* Windows 10 Admin Rights Gobbled By Razer Devices
* Video Shows Moment Iranian Prison Realizes It Was Hacked
* Microsoft Spills 38 Million Sensitive Data Records
* Tech CEOs To Meet With Biden Over Infrastructure Security
* The State Department Has Reportedly Been Hacked
* Crypto Platform Poly Network Says Hacked Funds Returned
* The US Military May Soon Declassify A Secret Space Weapon
* Attackers Actively Exploiting Realtek SDK Flaws
* China Passes New Personal Data Privacy Law, To Take Effect Nov. 1
* Afghanistan: Will Fingerprint Data Point Taliban To Targets?
* T-Mobile Data Breach Now Affects More Than 50 Million
* Hackers Steal Nearly $100m In Japan Crypto Heist
* Friendly Hackers Save Ford From Potential Data Leak
* Postmortem On U.S. Census Hack Exposes Cybersecurity Failures
* Fortinet Slams Rapid7 For Disclosing Vulnerability

Krebs on Security

* Man Robbed of 16 Bitcoin Sues Young Thieves' Parents
* Wanted: Disgruntled Employees to Deploy Ransomware
* T-Mobile: Breach Exposed SSN/DOB of 40M+ People
* T-Mobile Investigating Claims of Massive Data Breach
* New Anti Anti-Money Laundering Services for Crooks
* Microsoft Patch Tuesday, August 2021 Edition
* Phishing Sites Targeting Scammers and Thieves
* Ransomware Gangs and the Name Game Distraction
* The Life Cycle of a Breached Database
* PlugwalkJoe Does the Perp Walk

LATEST NEWS

Dark Reading

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

The Hacker News

* How Does MTA-STS Improve Your Email Security?
* Get Lifetime Access to 24 Professional Cybersecurity Certification Prep Courses
* LockFile Ransomware Bypasses Protection Using Intermittent File Encryption
* Microsoft Warns of Widespread Phishing Attacks Using Open Redirects
* Microsoft, Google to Invest $30 Billion in Cybersecurity Over Next 5 Years
* Kaseya Issues Patches for Two New 0-Day Flaws Affecting Unitrends Servers
* Critical Cosmos Database Flaw Affected Thousands of Microsoft Azure Customers
* The Increased Liability of Local In-home Propagation
* F5 Releases Critical Security Patch for BIG-IP and BIG-IQ Devices
* New Passwordless Verification API Uses SIM Security for Zero Trust Remote Access
* VMware Issues Patches to Fix New Flaws Affecting Multiple Products
* Critical Flaw Discovered in Cisco APIC for Switches - Patch Released
* Preventing your Cloud 'Secrets' from Public Exposure: An IDE plugin solution
* Researchers Uncover FIN8's New Backdoor Targeting Financial Institutions
* B. Braun Infusomat Pumps Could Let Attackers Remotely Alter Medication Dosages

LATEST NEWS

Security Week

* U.S. Justice Department Introduces Cyber Fellowship Program
* Exploitation of Flaws in Delta Energy Management System Could Have 'Dire Consequences'
* T-Mobile Hack Involved Exposed Router, Specialized Tools and Brute Force Attacks
* CISA, Microsoft Issue Guidance on Recent Azure Cosmos DB Vulnerability
* Experts Warn of Dangers From Breach of Voter System Software
* Boston Public Library Hit With Cyberattack
* FBI Shares IOCs for 'Hive' Ransomware Attacks
* Vulnerability Allows Remote Hacking of Annke Video Surveillance Product
* Enterprise Technology Management Provider Oomnitza Raises $20 Million
* Amazon to Offer Free Cybersecurity Training Materials, MFA Devices
* In a Hybrid Workplace, Men Are More Likely to Engage in Risky Behavior Than Women: Study
* Critical Vulnerability Exposed Azure Cosmos DBs for Months
* FIN8 Hackers Add 'Sardonic' Backdoor to Malware Arsenal
* Engineering Workstations Are Concerning Initial Access Vector in OT Attacks
* Cisco Patches Serious Vulnerabilities in Data Center Products
* Atlassian Patches Critical Code Execution Vulnerability in Confluence
* How Threat Detection is Evolving
* Microsoft Issues Guidance on ProxyShell Vulnerabilities
* Vulnerabilities Allow Hackers to Tamper With Doses Delivered by Medical Infusion Pumps
* CISA Details Additional Malware Targeting Pulse Secure Appliances
* Hack Exposes Personal Data of Entire Swiss Town: Report
* Tech Companies Pledge Billions in Cybersecurity Investments
* Vade Secure Ordered to Pay $14 Million to Proofpoint in IP Theft Lawsuit
* VMware Patches High-Severity Vulnerabilities in vRealize Operations

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

* [FREE Resource Kit] Cybersecurity Awareness Month 2021 Now Available
* U.K. Organizations See Double the Number of Ransomware Attacks in the First Half of 2021
* Cryptominers are Tricked out of Cryptocurrency Using Phishing Scams Involving the Purchase of Mining
* Cybercriminals Can Post Jobs on LinkedIn Posing as Any Employer They Want
* A COVID-19 Phishing Caper
* A Look at a Ransomware Affiliate
* Nigerian Threat Actors Solicit Victim Organization Employees to Deploy Demon Ransomware
* Arrests in International Fraud Scheme Due to Social Engineering
* Hospitals Continue to be Ransomware Targets as Half Experience Shutdowns in the Last 6 Months
* Microsoft Warns of New Phishing-Turned-Vishing-Turned-Phishing Attack Aimed at Installing Ransomware

ISC2.org Blog

* CCSP vs. Cloud+: How Do They Stack Up?
* (ISC)&sup2; Security Congress 2021 is Now Fully Virtual
* Thinking about CAP or CISSP? Here's How They Compare.
* Five Steps to Get a Cybersecurity Job
* 2021 Q3 Updates from Our Chairperson and CEO: Membership Milestones and More

HackRead

* Why torrenting on Elon Musk's Starlink is not a good idea?
* T-Mobile hacker used brute force attack to steal customers' data
* Whitehat hackers accessed primary keys of Azure's Cosmos DB customers
* FIN8 Resurfaces with New Sardonic Backdoor
* Top 6 SEO Conferences in the USA
* New variant of PRISM Backdoor 'WaterDrop' targets Linux systems
* Unpatched Microsoft Exchange servers hit with ProxyShell attack

Koddos

* Why torrenting on Elon Musk's Starlink is not a good idea?
* T-Mobile hacker used brute force attack to steal customers' data
* Whitehat hackers accessed primary keys of Azure's Cosmos DB customers
* FIN8 Resurfaces with New Sardonic Backdoor
* Top 6 SEO Conferences in the USA
* New variant of PRISM Backdoor 'WaterDrop' targets Linux systems
* Unpatched Microsoft Exchange servers hit with ProxyShell attack

LATEST NEWS

Naked Security

* Big bad decryption bug in OpenSSL - but no cause for alarm
* S3 Ep47: Daylight robbery, spaghetti trouble, and mousetastic superpowers [Podcast]
* How a gaming mouse can get you Windows superpowers!
* What's *THAT* on my 3D printer? Cloud bug lets anyone print to everyone
* Japanese cryptocoin exchange robbed of $100,000,000
* S3 Ep46: Copyright scams, video snooping and Grand Theft Crypto [Podcast]
* Video surveillance network hacked by researchers to hijack footage
* Copyright scammers turn to phone numbers instead of web links
* S3 Ep45: Routers attacked, hacking tool hacked, and betrayers betrayed [Podcast]
* Hacker grabs $600m in cryptocash from blockchain company Poly Networks

Threat Post

* LockBit Gang to Publish 103GB of Bangkok Air Customer Data
* T-Mobile's Security Is 'Awful,' Says Purported Thief
* Parallels Offers 'Inconvenient' Fix for High-Severity Bug
* Experts: WH Cybersecurity Summit Should Be Followed by Regulation, Enforcement
* Winning the Cyber-Defense Race: Understand the Finish Line
* FIN8 Targets US Bank With New 'Sardonic' Backdoor
* Critical Azure Cosmos DB Bug Allows Full Cloud Account Takeover
* Ragnarok Ransomware Gang Bites the Dust, Releases Decryptor
* Top Strategies That Define the Success of a Modern Vulnerability Management Program
* 'Pay Ransom' Screen? Too Late, Humpty Dumpty - Podcast

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

* Young People Are the Key to Decreasing the Skills Gap
* Why Privileged Access Management Is So Hard in the Cloud
* Data Is Quicksand: Does Your Current Data Security Solution Pull You Out or Sink You Deeper?
* Data Poisoning: The Next Big Threat
* Red & Blue: United We Stand
* How to Quantify the Actual Cost of a Data Breach for Your Own Organization
* Three Key Benefits of Adopting SASE With a Services Partner
* Accelerate Your Journey to AWS with IBM Security
* New CISA Blacklist: What It Means For You
* How to Protect Yourself From a Server-Side Template Injection Attack

InfoWorld

* What you don't know about working with AWS
* Don't stop your migration!
* When a cloud provider retires a service you're using
* Kotlin update previews experimental features
* How to nail the Kubernetes certification exams
* An early look at SvelteKit
* 12 hot language projects riding WebAssembly
* What to expect in Java 18
* GitHub CLI 2.0 introduces extensions
* Security blind spots persist as companies cross-breed security with devops

C4ISRNET - Media for the Intelligence Age Military

* COVID-19 showed why the military must do more to accelerate machine learning for its toughest challen
* 2 companies win contracts to research cyber protections for military aircraft
* Space Force leaders say they're on their way to delivering the first digital military branch
* Military cyber operators will soon have a new tool to deliver virtual fires
* Space Systems Command is more than a name change, says new commander
* IT leader: New DoD enterprise cloud contract remains on schedule
* New Army cyber school leader wants to fix a problem for graduates
* Space Force, Lockheed are ready to start making the nation's new satellites to watch for missiles
* SPACECOM declares initial operational capability two years after launch
* Air Force secretary outlines short-term plan to shake up space acquisition

The Hacker Corner

Conferences

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

Google Zero Day Project

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

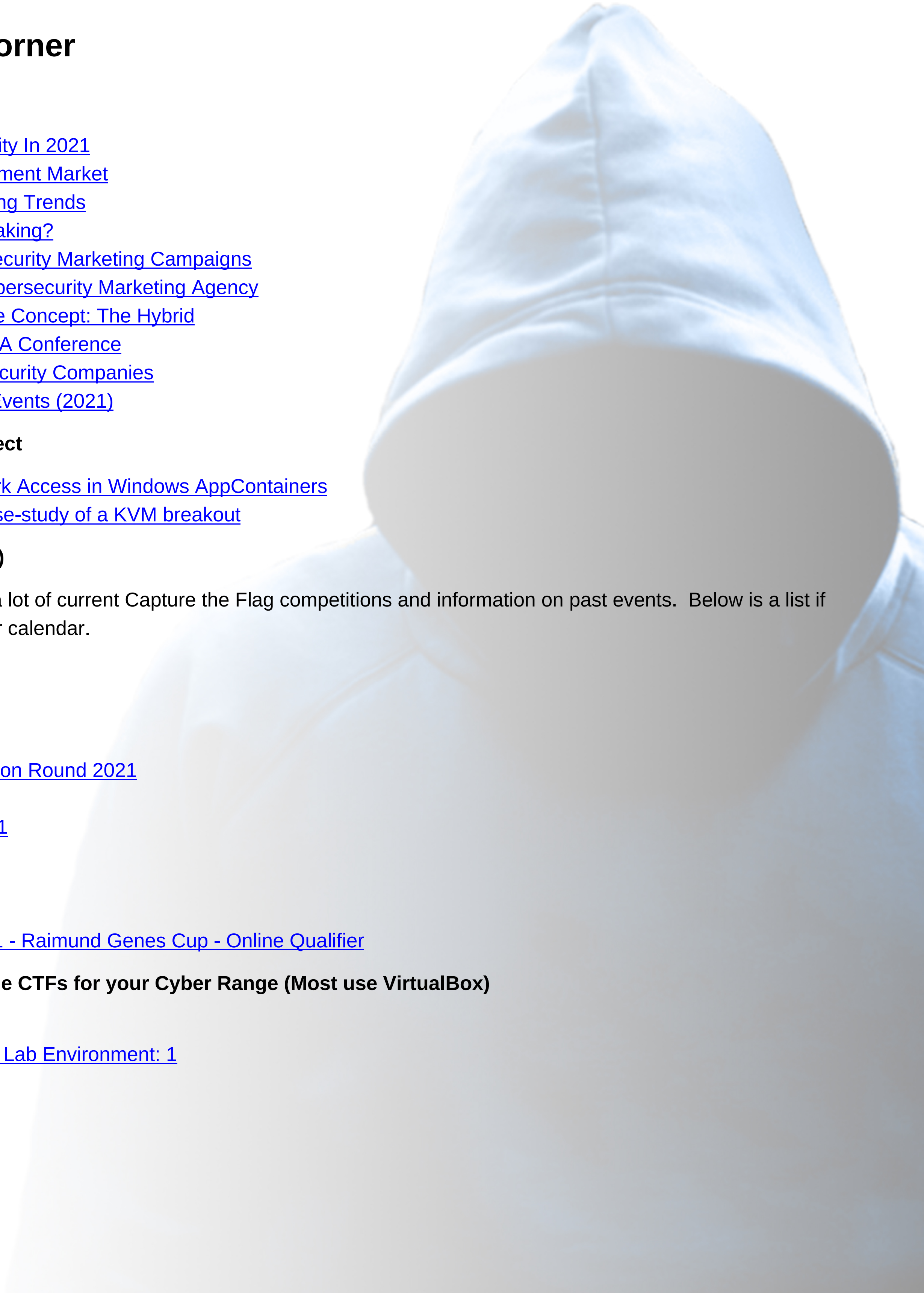
Capture the Flag (CTF)

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

* ALLES! CTF 2021
* GrabCON CTF 2021
* TMUCTF 2021
* CSAW CTF Qualification Round 2021
* RCTF 2021
* COMPFEST CTF 2021
* VolgaCTF 2021 Final
* PBjar CTF '21
* Overflow To Fall
* Trend Micro CTF 2021 - Raimund Genes Cup - Online Qualifier

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

* Snakeoil: 1
* Vulnerable Pentesting Lab Environment: 1
* EvilBox: One
* Chronos: 1
* Thoth Tech: 1



Tools & Techniques

Packet Storm Security Tools Links

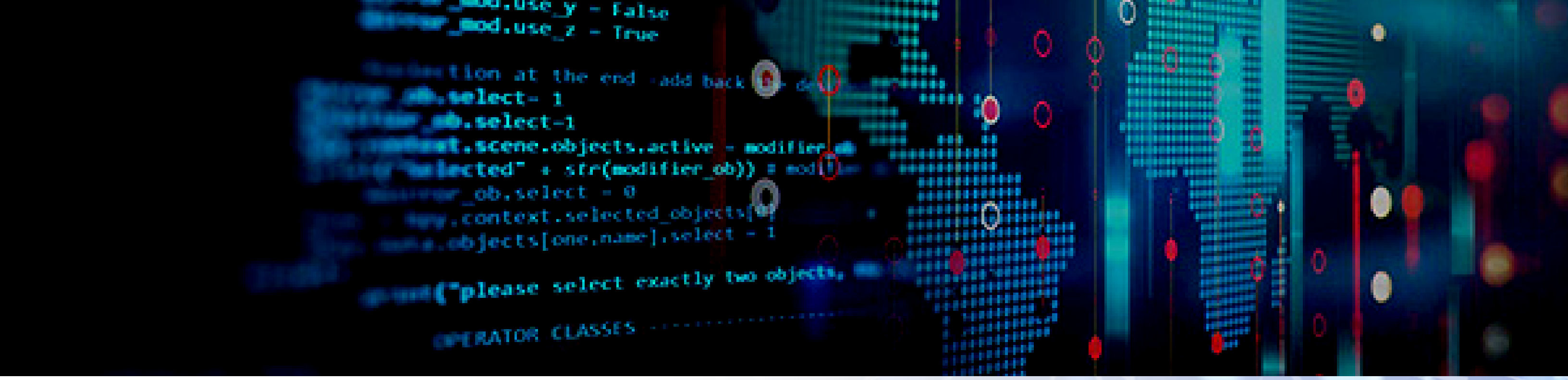
* Wireshark Analyzer 3.4.8
* I2P 1.5.0
* OpenSSL Toolkit 1.1.1l
* GRR 3.4.5.1
* Faraday 3.17.1
* OpenSSH 8.7p1
* TOR Virtual Network Tunneling Tool 0.4.6.7
* Faraday 3.17.0
* Nmap Port Scanner 7.92
* SQLMAP - Automatic SQL Injection Tool 1.5.8

Kali Linux Tutorials

* Rtl_433 : Program To Decode Radio Transmissions From Devices On The ISM Bands
* LightMe : HTTP Server Serving Obfuscated Power shell Scripts/Payloads
* PackageDNA : Tool To Analyze Software Packages Of Different Programming Languages That Are Being Or W
* FisherMan : CLI Program That Collects Information From Facebook User Profiles Via Selenium
* REW-sploit : Emulate And Dissect MSF And *Other* Attacks
* Allstar : GitHub App To Set And Enforce Security Policies
* AuraBorealisApp : A Tool For Visualizing Python Package Registry Security Audit Data
* PowerShell Armoury : A PowerShell Armoury For Security Guys And Girls
* Sniffle : A Sniffer For Bluetooth 5 And 4.X LE
* SGXRay : Automating Vulnerability Detection for SGX Apps

GBHackers Analysis

* F5 BIG-IP Flaw Let Hackers Execute Arbitrary System Commands
* The Truth About Russian Hackers
* Unpatched Fortinet Bug Would Allow Remote Attackers To Execute Arbitrary Commands
* Critical Vulnerability In Millions of IoT Devices Lets Hackers Spy on You Remotely
* Severe Vulnerabilities in Realtek SDK Affects Around Millions of IoT Devices



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Greppin' Logs | Jon Stewart & Noah Rubin
* To the Moon! The Cyber Kill Chain Meets Blockchain | Jackie Koven
* Breaches Be Crazy | Eric Capuano & Whitney Champion
* Scoring and Judging Artifacts in Autopsy | Brian Carrier

Defcon Conference

* DEF CON 29 Adversary Village - Carlos Polop - New Generation of PEAS
* DEF CON 29 Adversary Village - Mark Loveless - A Short History and An Example Attack
* DEF CON 29 Adversary Village - Mauro Eldritch, Luis Ramirez - Everything is a C2 if you're brave
* DEF CON 29 Adversary Village - Jose Garduno - C2Centipede APT level C2 communications for common rev

Hak5

* HakByte: Getting Started with Breadboards & Arduino (Hardware Prototyping 1/5)
* Architecting a Continuous Recon Platform | /dev/hack s01e02
* Razer Mice + Microsoft Windows = Privilege Escalation - ThreatWire

The PC Security Channel [TPSC]

* Lockbit Ransomware and the Accenture Hack
* BlackMatter Ransomware

Eli the Computer Guy

* eBeggar Wednesday (on Monday) - Airpods MAX edition
* Cyber Security Introduction (Cyber Security Part 1)
* Office Hours -Tech Questions and Answers (8/25/21)
* eBeggar Wednesday - FAUCI PROBLEMS edition

Security Now

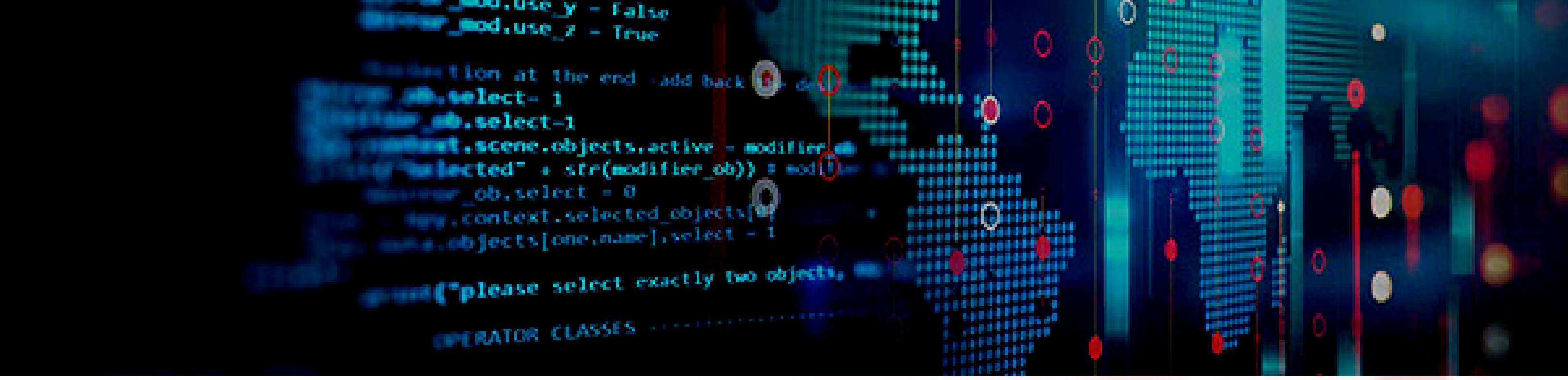
* Microsoft's Reasoned Neglect - T-Mobile's Major Data Leak, Razer Mouse Hack, Overlay Networks
* Microsoft's Culpable Negligence - Firefox Update, Magniber, Merger of Avast and NortonLifeLock

Troy Hunt

* Weekly Update 258

Intel Techniques: The Privacy, Security, & OSINT Show

* 232-Anonymous Phone Update Part I
* 231-This Week In Privacy, Security, & OSINT



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

* 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
* Bear Tracks: Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers
* New Analysis Shows XAMPP Serving Agent Tesla and Formbook Malware
* Taking a Closer Look at a Malicious Infrastructure Mogul
* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem

FireEye

* [The Lost Bots] Episode 4: Deception Technology
* Metasploit Wrap-Up
* The Cybersecurity Skills Gap Is Widening: New Study
* [R]Evolution of the Cyber Threat Intelligence Practice
* Cybercriminals Selling Access to Compromised Networks: 3 Surprising Research Findings
* [The Lost Bots] Bonus Episode: Velociraptor Contributor Competition
* Rapid7 MDR Named a Market Leader, Again!
* Metasploit Wrap-Up
* Why Joining Rapid7 Was the Best Decision for These Sales Professionals, Even During a Pandemic
* Rapid7 Announces Partner of the Year Awards 2021 Winners

Proof of Concept (PoC) & Exploits

Packet Storm Security

* ProcessMaker 3.5.4 Local File Inclusion
* Online Leave Management System 1.0 Shell Upload
* HP OfficeJet 4630/7110 MYM1FN2025AR 2117A Cross Site Scripting
* WordPress Mail Masta 1.0 Local File Inclusion
* Online Traffic Offense Management System 1.0 Remote Code Execution
* Shoutcast Server 2.6.0.753 Crash
* RaspAP 2.6.6 Remote Code Execution
* Simple Phone Book/Directory 1.0 SQL Injection
* Microsoft Exchange ProxyShell Remote Code Execution
* Online Traffic Offense Management System 1.0 SQL Injection
* NetModule Router Software Password Handling / Session Fixation
* Laundry Booking Management System 1.0 SQL Injection
* Laundry Booking Management System 1.0 Cross Site Scripting
* Altus Sistemas de Automacao Products CSRF / Command Injection / Hardcoded Credentials
* WebKit Element::dispatchMouseEvent Heap Use-After-Free
* JavaScriptCore Crash Proof Of Concept
* WebKit WebCore::FrameLoader::PolicyChecker::checkNavigationPolicy Heap Use-After-Free
* Charity Management System CMS 1.0 Code Execution / XSS / SQL Injection
* Simple Image Gallery 1.0 Shell Upload
* Crossfire Server 1.0 Buffer Overflow
* Crime Records Management System 1.0 SQL Injection
* Hospital Management System Cross Site Scripting
* COVID-19 Testing Management System 1.0 SQL Injection
* Lucee Administrator imgProcess.cfm Arbitrary File Write
* GeoVision Geowebserver 5.3.3 LFI / XSS / CSRF / Code Execution

CXSecurity

* CyberPanel 2.1 Remote Code Execution (RCE) (Authenticated)
* WordPress Mail Masta 1.0 Local File Inclusion
* NetModule Router Software Password Handling / Session Fixation
* Simple Water Refilling Station Management System 1.0 Remote Code Execution (RCE) through File Upload
* Crossfire Server 1.0 Buffer Overflow
* Hospital Management System Cross Site Scripting
* Atlassian Crowd pdkinstall Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

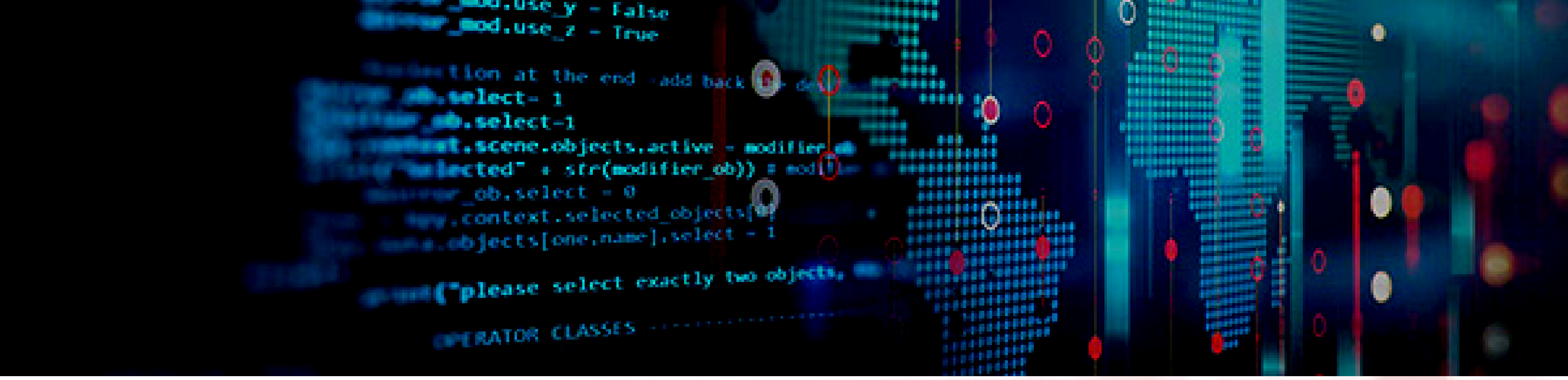
* [webapps] Bus Pass Management System 1.0 - 'viewid' SQL Injection
* [webapps] Usermin 1.820 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ZesleCP 3.1.9 - Remote Code Execution (RCE) (Authenticated)
* [webapps] COMMAX UMS Client ActiveX Control 1.7.0.2 - 'CNC_Ctrl.dll' Heap Buffer Overflow
* [webapps] COMMAX WebViewer ActiveX Control 2.1.4.5 - 'Commax_WebViewer.ocx' Buffer Overflow
* [webapps] CyberPanel 2.1 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ProcessMaker 3.5.4 - Local File inclusion
* [webapps] Online Leave Management System 1.0 - Arbitrary File Upload to Shell (Unauthenticated)
* [webapps] HP OfficeJet 4630/7110 MYM1FN2025AR/2117A - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Mail Masta 1.0 - Local File Inclusion (2)
* [webapps] RaspAP 2.6.6 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Simple Phone book/directory 1.0 - 'Username' SQL Injection (Unauthenticated)
* [webapps] Online Traffic Offense Management System 1.0 - Remote Code Execution (RCE) (Unauthenticated
* [webapps] Laundry Booking Management System 1.0 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Laundry Booking Management System 1.0 - 'Multiple' SQL Injection
* [webapps] Online Traffic Offense Management System 1.0 - 'id' SQL Injection (Authenticated)
* [webapps] Charity Management System CMS 1.0 - Multiple Vulnerabilities
* [remote] crossfire-server 1.9.0 - 'SetUp()' Remote Buffer Overflow
* [webapps] COVID19 Testing Management System 1.0 - 'Multiple' SQL Injections
* [webapps] Simple Image Gallery 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Crime records Management System 1.0 - 'Multiple' SQL Injection (Authenticated)
* [local] SonicWall NetExtender 10.2.0.300 - Unquoted Service Path
* [webapps] GeoVision Geowebserver 5.3.3 - LFI / XSS / HHI / RCE
* [webapps] COMMAX CVD-Axx DVR 5.1.4 - Weak Default Credentials Stream Disclosure

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
```

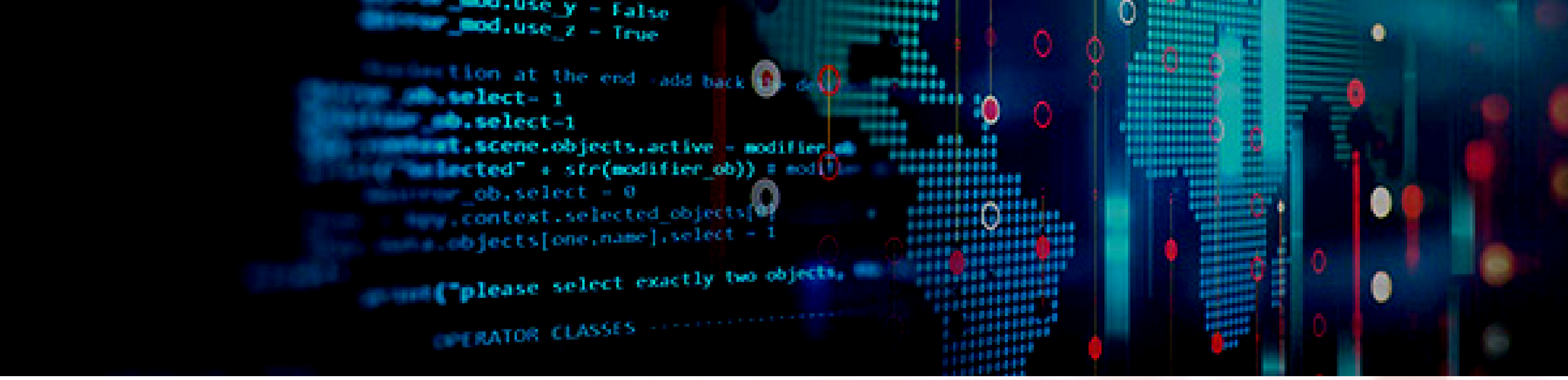
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


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

Latest Hacked Websites

Published on Zone-h.org

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


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

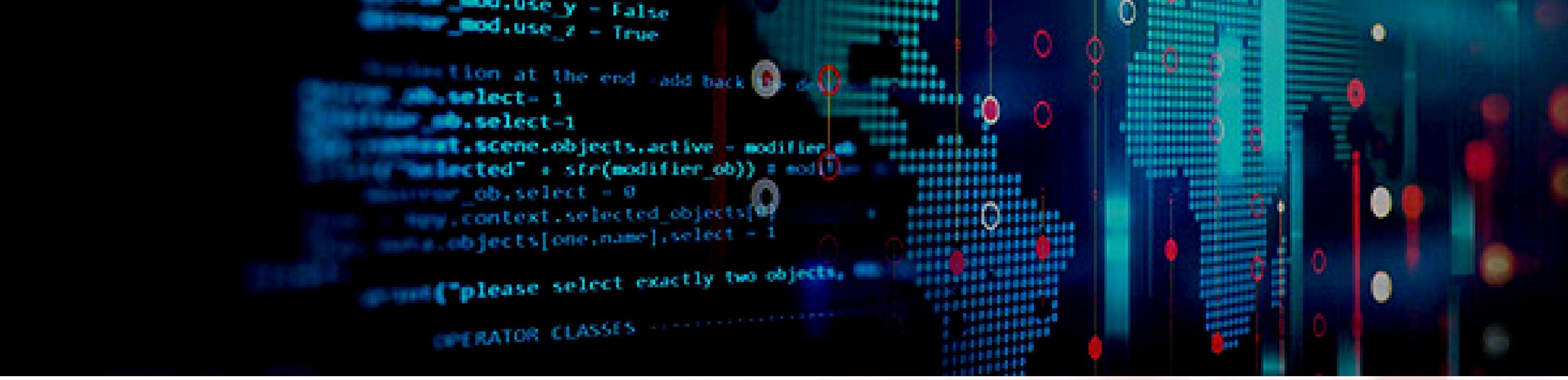
Dark Web News

Darknet Live

Australian Man Arrested for Importing 406 Grams of Meth
Australian authorities arrested and charged a man for allegedly importing methamphetamine. (via darknetlive.com)
Malta: Man Tried to Purchase a Gun on the Darkweb
A businessman in Malta is expected to be charged for allegedly purchasing firearms and explosives on the darkweb. (via darknetlive.com)
Counterfeit Xanax Vendor "Rangoon" Sentenced to Prison
A Florida man is set to spend the next 36 months in prison for manufacturing and distributing counterfeit Xanax pills through the darkweb. (via darknetlive.com)
Australian Police Seized $8.5 Million in Cryptocurrency
Police in Victoria, Australia, seized cryptocurrency worth more than $6 million during a darkweb drug trafficking investigation. (via darknetlive.com)

Dark Web Link

When Ransomware Strikes, Can You Recuperate Fast Enough?
Ransomware assaults are becoming more prevalent, and they may even be purchased as a service on the dark Web. There have been several cases in the press when big corporations have been left with little choice but to pay a ransom to regain access to their data, which may cost hundreds of thousands of dollars. [...] The post When Ransomware Strikes, Can You Recuperate Fast Enough? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
New Surveillance Law To Battle Crime On The 'Dark Web' Has Civil Rights Groups Worried
Australian law enforcement agencies will be given new 'exceptional' powers to combat serious cybercrime, raising concerns among legal bodies and civil rights organisations. The federal government has enacted legislation giving top law enforcement agencies unprecedented and intrusive tools to battle cybercrime on the dark web, but some organisations are concerned about the scope of the [...] The post New Surveillance Law To Battle Crime On The 'Dark Web' Has Civil Rights Groups Worried appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Italian Mafia Organizations Use Cryptocurrencies More And More, According To The Dia
In Italy, the mafia and other organised criminal groups are increasingly utilising cryptocurrency. In an interview with Zeit Online, the Italian Anti-Mafia Directorate (DIA), our country's police body dedicated to combating this sort of crime, claimed this. Dia's representative stated that virtually all criminal groups, especially mafia-type organisations, are very interested in leveraging digital assets [...] The post Italian Mafia Organizations Use Cryptocurrencies More And More, According To The Dia appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


.use_y = False
mod.use_z = True
tion at the end -add back
.select= 1
.select=1
.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

* CISA Adds Single-Factor Authentication to list of Bad Practices
* Microsoft Azure Cosmos DB Guidance
* FBI Releases Indicators of Compromise Associated with Hive Ransomware
* &#8239;ICSJWG 2021 Fall Virtual Meeting
* Cisco Releases Security Updates&#8239;for Multiple Products
* VMware Releases Security Updates for Multiple Products&#8239;
* OpenSSL Releases Security&#8239;Update&#8239;
* FBI Releases Indicators of Compromise Associated with OnePercent Group Ransomware
* AA21-229A: BadAlloc Vulnerability Affecting BlackBerry QNX RTOS
* AA21-209A: Top Routinely Exploited Vulnerabilities
* Vulnerability Summary for the Week of August 23, 2021
* Vulnerability Summary for the Week of August 16, 2021

Zero Day Initiative Advisories

ZDI-CAN-14607: 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 'Lays (@_L4ys) of TrapaSecurity' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15101: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15100: Sante
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: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15105: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15076: 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: 2021-08-27, 3 days ago. The vendor is given until

2021-12-25 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-15099: Sante

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: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15107: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15102: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15077: 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: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15106: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15103: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15104: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-14615: Epic Games

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15098: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15112: 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 'Mat Powell of Trend

Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15108: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15111: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15110: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15113: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-15109: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-27, 3 days ago. The vendor is given until 2021-12-25 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-14618: BMC

A CVSS score 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Markus Wulftange (@mwulftange)' was reported to the affected vendor on: 2021-08-25, 5 days ago. The vendor is given until 2021-12-23 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-14234: Kaspersky

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-08-25, 5 days ago. The vendor is given until 2021-12-23 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-14235: Kaspersky

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 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-08-25, 5 days ago. The vendor is given until 2021-12-23 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-14702: WECON

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-08-25, 5 days ago. The vendor is given until 2021-12-23 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5051-2

Ubuntu Security Notice 5051-2 - USN-5051-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Ingo Schwarze discovered that OpenSSL incorrectly handled certain ASN.1 strings. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly obtain sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5052-1

Ubuntu Security Notice 5052-1 - MongoDB would fail to properly invalidate existing sessions for deleted users. This could allow a remote authenticated attacker to gain elevated privileges if their user account was recreated with elevated privileges.

Ubuntu Security Notice USN-5037-2

Ubuntu Security Notice 5037-2 - USN-5037-1 fixed vulnerabilities in Firefox. The update introduced a regression that caused Firefox to repeatedly prompt for a password. This update fixes the problem. Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, trick a user into accepting unwanted permissions, or execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5051-1

Ubuntu Security Notice 5051-1 - John Ouyang discovered that OpenSSL incorrectly handled decrypting SM2 data. A remote attacker could use this issue to cause applications using OpenSSL to crash, resulting in a denial of service, or possibly change application behaviour. Ingo Schwarze discovered that OpenSSL incorrectly handled certain ASN.1 strings. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly obtain sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5050-1

Ubuntu Security Notice 5050-1 - It was discovered that the bluetooth subsystem in the Linux kernel did not properly perform access control. An authenticated attacker could possibly use this to expose sensitive information. Michael Brown discovered that the Xen netback driver in the Linux kernel did not properly handle malformed packets from a network PV frontend, leading to a use-after-free vulnerability. An attacker in a guest VM could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

PotPlayer 1.7.21523 Build 210729 Out-Of-Bounds Write

PotPlayer version 1.7.21523 build 210729 suffers from an out-of-bounds write vulnerability that cause an exploitable crash and may potentially lead to code execution and information disclosure.

Ubuntu Security Notice USN-5048-1

Ubuntu Security Notice 5048-1 - It was discovered that Inetutils telnet server allows remote attackers to execute arbitrary code via short writes or urgent data. An attacker could use this vulnerability to cause a DoS or possibly execute arbitrary code.

Red Hat Security Advisory 2021-3219-01

Red Hat Security Advisory 2021-3219-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4 for Red Hat Enterprise Linux 7 and 8. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-3217-01

Red Hat Security Advisory 2021-3217-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.3 for Red Hat Enterprise Linux 6, 7, and 8. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-3218-01

Red Hat Security Advisory 2021-3218-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-3216-01

Red Hat Security Advisory 2021-3216-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.3. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-3125-01

Red Hat Security Advisory 2021-3125-01 - This release of Red Hat build of Eclipse Vert.x 4.1.2 includes security updates, bug fixes, and enhancements.

Kernel Live Patch Security Notice LSN-0080-1

Andy Nguyen discovered that the netfilter subsystem in the Linux kernel contained an out-of-bounds write in its setsockopt() implementation. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

Ubuntu Security Notice USN-5046-1

Ubuntu Security Notice 5046-1 - It was discovered that the bluetooth subsystem in the Linux kernel did not properly perform access control. An authenticated attacker could possibly use this to expose sensitive information. Michael Brown discovered that the Xen netback driver in the Linux kernel did not properly handle malformed packets from a network PV frontend, leading to a use-after-free vulnerability. An attacker in a guest VM could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5045-1

Ubuntu Security Notice 5045-1 - 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. It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device initialization failure, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-3207-01

Red Hat Security Advisory 2021-3207-01 - This release of Red Hat Integration - Camel Quarkus - 1.8.1 tech-preview 2 serves as a replacement for tech-preview 1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, denial of service, information leakage, man-in-the-middle, and traversal vulnerabilities.

Red Hat Security Advisory 2021-3205-01

Red Hat Security Advisory 2021-3205-01 - A minor version update is now available for Red Hat Camel K that includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include bypass, code execution, denial of service, information leakage, man-in-the-middle, and traversal vulnerabilities.

Ubuntu Security Notice USN-5044-1

Ubuntu Security Notice 5044-1 - It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device initialization failure, leading to a double-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the bluetooth subsystem in the Linux kernel did not properly handle HCI device detach events, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5043-1

Ubuntu Security Notice 5043-1 - It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. It was discovered that Exiv2 incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service. These issues only affected Ubuntu 20.04 LTS and Ubuntu 21.04. Various other issues were also addressed.

Ubuntu Security Notice USN-5042-1

Ubuntu Security Notice 5042-1 - It was discovered that HAProxy incorrectly handled the HTTP/2 protocol. A remote attacker could possibly use this issue to bypass restrictions.

Red Hat Security Advisory 2021-3173-01

Red Hat Security Advisory 2021-3173-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include bypass and out of bounds write vulnerabilities.

Red Hat Security Advisory 2021-3176-01

Red Hat Security Advisory 2021-3176-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-3181-01

Red Hat Security Advisory 2021-3181-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include bypass and out of bounds write vulnerabilities.

Red Hat Security Advisory 2021-3172-01

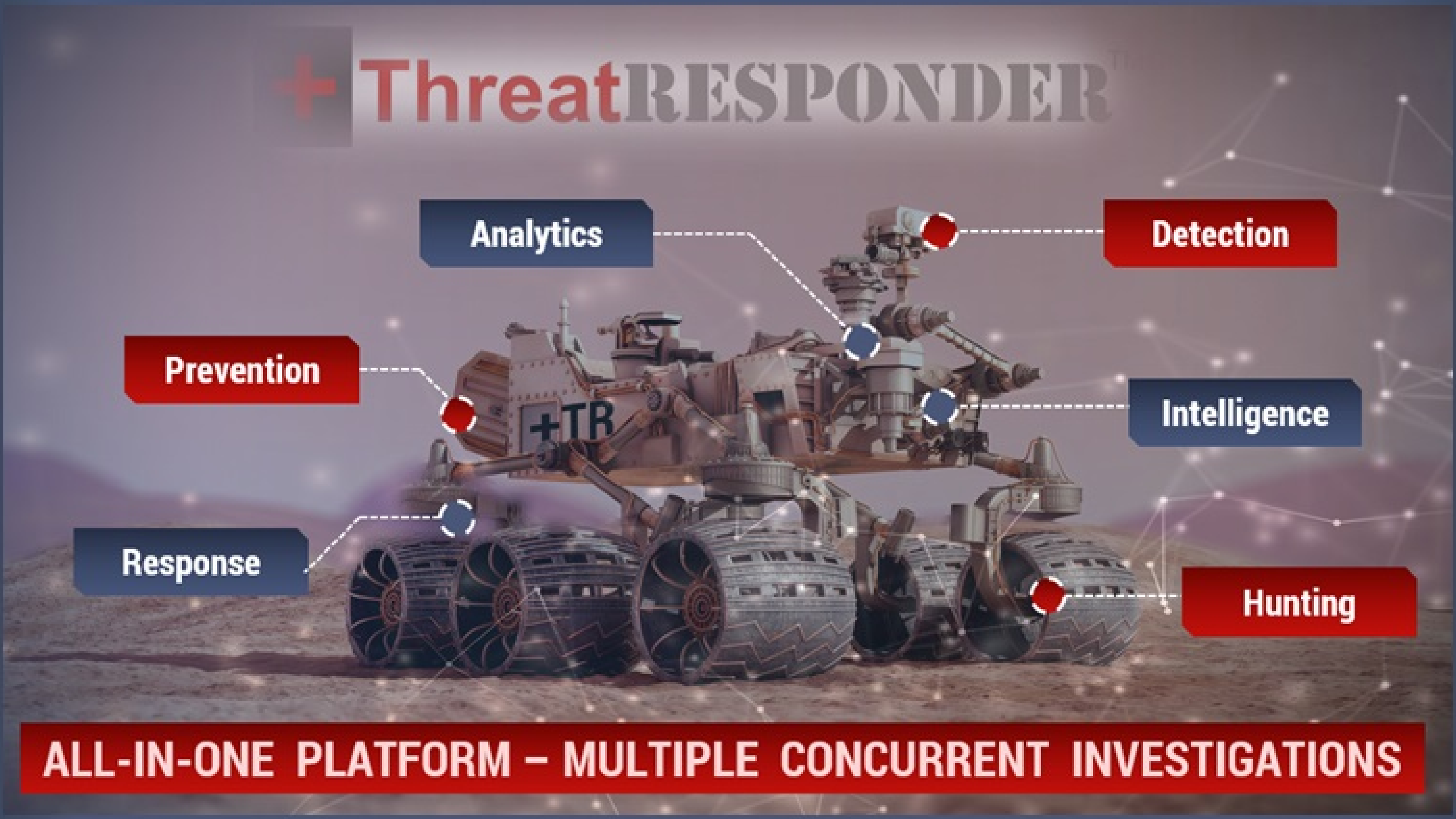
Red Hat Security Advisory 2021-3172-01 - EDK is a project to enable UEFI support for Virtual Machines. This package contains a sample 64-bit UEFI firmware for QEMU and KVM. Issues addressed include a buffer overflow vulnerability.

Are You…

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

Do DFIR Investigations Better

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



The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

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

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

CSI Linux Tutorials:

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

Cyber Secrets

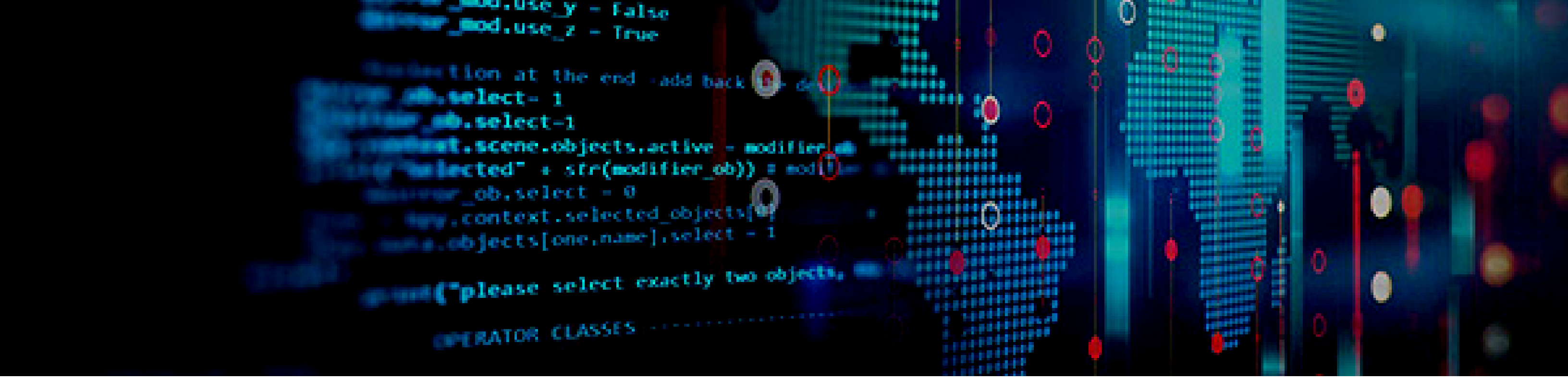
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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

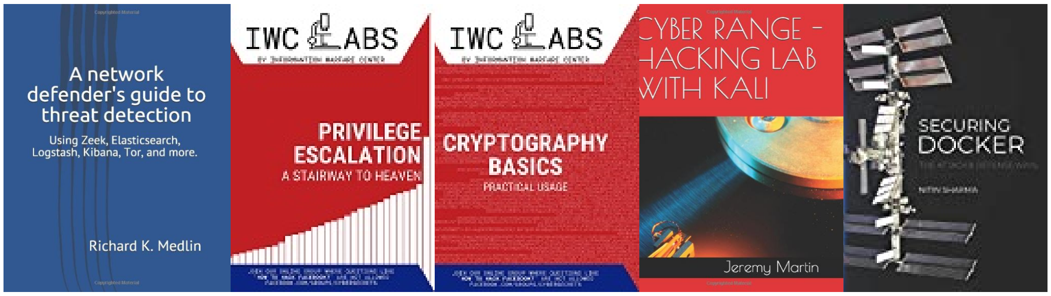


The Cyber Secrets publications on Amazon

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

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

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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP