Aug-23-21

CYBER WEEKLY AWARENESS REPORT

netSecurity®

INFORMATION WARFARE CENTER

LINUX

ARGOS
APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

August 23, 2021

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

Summary

Internet Storm Center Infocon Status

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

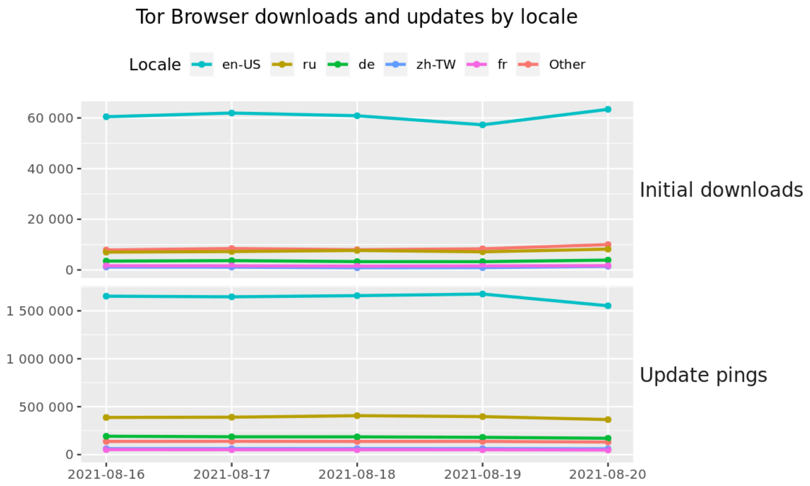
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

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

Cyber Secrets was originally a video series and is on both YouTube.

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



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

Interesting News

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

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

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* 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
* GitHub Pushes Users To Enable 2FA
* T-Mobile Says Data On 40 Million People Stolen By Hackers
* Unpatched Fortinet Bug Allows Firewall Takeovers
* 9to5Mac Writer Paid Source $500 In Bitcoin For Stolen Apple Data
* HolesWarm Malware Exploits Windows, Linux Servers
* Apple: CSAM Image-Detection Backdoor Narrow In Scope
* A Third Of Companies Have Experienced Ransomware
* Hospitals Hamstrung By Ransomware Are Turning Away Patients
* Desire To Connect IoT Devices Can Lead To Risky New Flaws
* Brazilian National Treasury Hit With Ransomware Attack
* SynAck Ransomware Group Releases Decryption Keys And Rebrands
* T-Mobile Investigating Claims Of Customer Data Breach
* The Taliban Have Taken Afghanistan
* AFP Seeks Upgrade To Telco Interception And Surveillance
* United Nations Calls For Moratorium On Sale Of Surveillance Tech Like NSO Group's Pegasus
* Phishing Campaign Leverages Legit DocuSign Email Notifications
* Poly Network Rewards Hacker With $500,000 Bug Bounty
* Hackers Uncover Weaknesses In Agriculture Giants' Systems

Krebs on Security

* 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
* Serial Swatter Who Caused Death Gets Five Years in Prison

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

* Navigating Vendor Risk Management as IT Professionals
* Researchers Detail Modus Operandi of ShinyHunters Cyber Crime Group
* Top 15 Vulnerabilities Attackers Exploited Millions of Times to Hack Linux Systems
* WARNING: Microsoft Exchange Under Attack With ProxyShell Flaws
* Cloudflare mitigated one of the largest DDoS attack involving 17.2 million rps
* ShadowPad Malware is Becoming a Favorite Choice of Chinese Espionage Groups
* Cybercrime Group Asking Insiders for Help in Planting Ransomware
* Mozi IoT Botnet Now Also Targets Netgear, Huawei, and ZTE Network Gateways
* Critical Flaw Found in Older Cisco Small Business Routers Won't Be Fixed
* Researchers Find New Evidence Linking Diavol Ransomware to TrickBot Gang
* Critical ThroughTek SDK Bug Could Let Attackers Spy On Millions of IoT Devices
* BadAlloc Flaw Affects BlackBerry QNX Used in Millions of Cars and Medical Devices
* Iranian Hackers Target Several Israeli Organizations With Supply-Chain Attacks
* Does a VPN Protect You from Hackers?
* NK Hackers Deploy Browser Exploits on South Korean Sites to Spread Malware

LATEST NEWS

Security Week

* Cloudflare Mitigated Record-Setting 17.2 Million RPS DDoS Attack
* Cyber Warfare May be Losing Its Advantage of Deniability
* Details Disclosed for Critical Vulnerability in Sophos Appliances
* PetitPotam Vulnerability Exploited in Ransomware Attacks
* CISA Warns Organizations of ProxyShell Attacks on Exchange Servers
* JPMorgan Chase Bank Notifies Customers of Data Exposure
* Number of T-Mobile Customers Confirmed to Be Affected by Hack Reaches 54 Million
* CISA Issues Guidance on Protecting Data From Ransomware
* Google Discloses Details of Unpatched Windows AppContainer Flaw
* Third-Party Patches Available for More PetitPotam Attack Vectors
* High-Severity DoS Vulnerability Patched in BIND DNS Software
* China Passes Tough New Online Privacy Law
* Hackers Steal $97 Million from Japanese Crypto-Exchange Liquid
* Cisco: Critical Flaw in Older SMB Routers Will Remain Unpatched
* Over 600 ICS Vulnerabilities Disclosed in First Half of 2021: Report
* Cyberattack Forces Memorial Health System to Cancel Surgeries, Divert Patients
* Detect: The Third Pillar of Industrial Cybersecurity
* GitHub Encourages Users to Adopt Two-Factor Authentication
* Belarus Brands Group Who Claimed to Hack Interior Ministry 'Extremist'
* Report: Census Hit by Cyberattack, US Count Unaffected
* Report: Iranian APT Hexane Targets Israeli Companies
* Threat Detection and Response Firm Blumira Raises $10.3 Million
* Blockchain Security Company CertiK Raises $24 Million
* T-Mobile Confirms Data Breach Impacts Millions of Customers

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

* "Compromise" is the "C" in "MICE"
* CISA shares guidance on how to prevent ransomware data breaches
* Phishing Attacks Have Increased by 22% This Year
* Defending Against Ransomware Attacks Should Start (and Can End) With Security Awareness Training
* Can the Microsoft 365 Platform Be Trusted to Stop Security Breaches?
* Deepfakes Continue to be a Concern as the Technology Improves and Becomes More Convincing
* Trend Micro: Most Organizations in the World Will Likely Be Compromised in the Next 12 Months
* Cyber Attacks Grow 125% as Ransomware Tops the List Plaguing Enterprise Organizations
* The Average Ransom Demand of $5.3M in 2021 is Up 518% From Last Year
* Copyright Scammers Now Making Phone Calls

ISC2.org Blog

* Asset Visibility - Breaking the Fourth Wall in Cybersecurity
* Containers in the Cloud: Key Benefits and Challenges
* Navigating the Troubled Waters of Risk Management
* Top Cybersecurity Podcasts
* How Has CAP Certification Evolved to Lead in Risk Management?

HackRead

* US military personnel defrauded into losing $822m through scams
* The Five Best Widgets To Have On Your Website
* Google shares details of unpatched Windows AppContainer vulnerability
* 5 WordPress Security Solutions with Free SSL Certificates
* HolesWarm crypto malware hits unpatched Linux, Windows servers
* AT&T breach? ShinyHunters selling AT&T database with 70 million SSN
* Human rights watchdog 'Karapatan' hit by weeks long DDOS attacks

Koddos

* US military personnel defrauded into losing $822m through scams
* The Five Best Widgets To Have On Your Website
* Google shares details of unpatched Windows AppContainer vulnerability
* 5 WordPress Security Solutions with Free SSL Certificates
* HolesWarm crypto malware hits unpatched Linux, Windows servers
* AT&T breach? ShinyHunters selling AT&T database with 70 million SSN
* Human rights watchdog 'Karapatan' hit by weeks long DDOS attacks

LATEST NEWS

Naked Security

* 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
* Home and small business routers under attack - how to see if you are at risk
* S3 Ep44: Unreported holes, retro computing, and tech support for malware [Podcast]
* Conti ransomware affiliate goes rogue, leaks "gang data"
* "Cobalt Strike" network attack tool patches crashtastic server bug

Threat Post

* Managing Privileged Access to Secure the Post-COVID Perimeter
* Attackers Actively Exploiting Realtek SDK Flaws
* Web Censorship Systems Can Facilitate Massive DDoS Attacks
* Nigerian Threat Actors Solicit Employees to Deploy Ransomware for Cut of Profits
* What's Next for T-Mobile and Its Customers? - Podcast
* How Ready Are You for a Ransomware Attack?
* Critical Cisco Bug in Small Business Routers to Remain Unpatched
* InkySquid State Actor Exploiting Known IE Bugs
* Windows EoP Bug Detailed by Google Project Zero
* COVID-19 Contact-Tracing Data Exposed, Fake Vax Cards Circulate

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

* Behavior Transparency: Where Application Security Meets Cyber Awareness
* New Collar: How Digital Badges and Skilling for Students Can Reduce the Skills Gap
* How Biden's Cloud Security Executive Order Stacks Up to Industry Expectations
* How Ransomware Trends Are Changing Cyber Insurance
* What Does The Great Resignation Mean for Data Security?
* Critical Infrastructure Attack Trends: What Business Leaders Should Know
* Hunting for Evidence of DLL Side-Loading With PowerShell and Sysmon
* How AI Prevents Fatigue After Data Breaches
* Highly Regulated or Not, These Data Security Use Cases Still Apply
* Analysis of Diavol Ransomware Reveals Possible Link to TrickBot Gang

InfoWorld

* 4 reasons to get Kubernetes-certified, and 4 reasons not to
* Tips for agile and devops teams in a hybrid work model
* JetBrains' Go language IDE prepares for generics
* What to expect in Java 18
* 'Why cloud computing?' is always a good question
* Microsoft details .NET 6 performance boosts
* How to use string interpolation in C# 9
* How to use Auth0 with Node.js and Express
* Get started with FastAPI
* Build mixed reality for Microsoft Edge with WebXR

C4ISRNET - Media for the Intelligence Age Military

* Space Force standing up STARCOM to train guardians
* Kratos, General Atomics get more money for Skyborg development
* Two Saudi firms to co-produce Sky Guard drone for operational use
* General Dynamics building lightweight vehicle electronic warfare system for US Army
* With Chinese and Russian knives at the throat of GPS, Senate calls for a study, waits for administrat
* The Space Force met its 18-month deadline to get up and running. Here's what's next.
* New US Air Force secretary to shake up Advanced Battle Management Program
* Army Special Forces want to integrate more with other military units on info warfare
* US and Canada want to collaborate on NORAD modernization
* US Army wants a high-altitude jammer

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

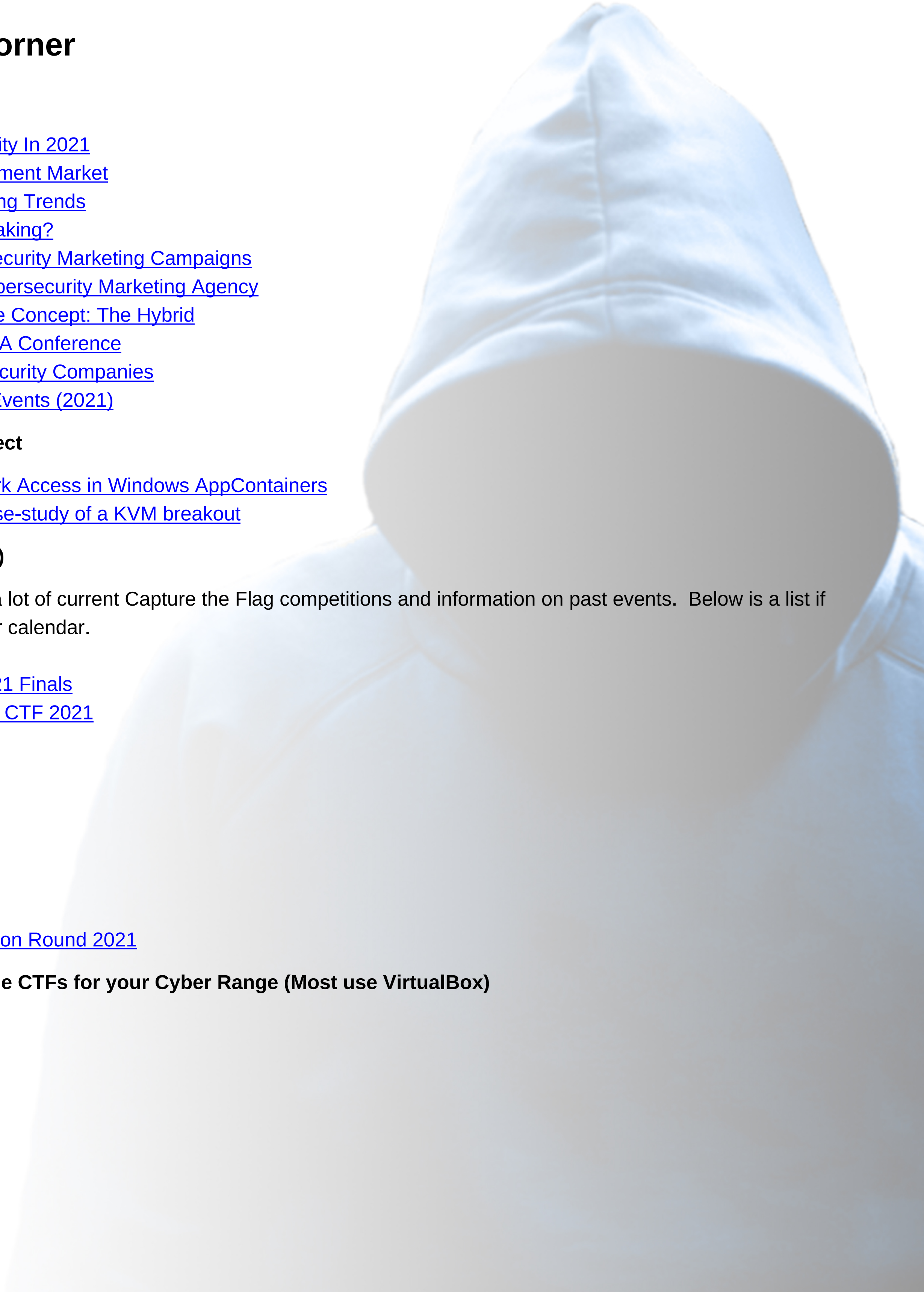
Capture the Flag (CTF)

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.

* Midnight Sun CTF 2021 Finals
* HITB SECCONF EDU CTF 2021
* YauzaCTF 2021
* FwordCTF 2021
* WMCTF 2021
* WORMCON 0x01
* ALLES! CTF 2021
* GrabCON CTF 2021
* TMUCTF 2021
* CSAW CTF Qualification Round 2021

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

* Chronos: 1
* Thoth Tech: 1
* hacksudo: Thor
* Looz: 1
* Hack Me Please: 1



Tools & Techniques

Packet Storm Security Tools Links

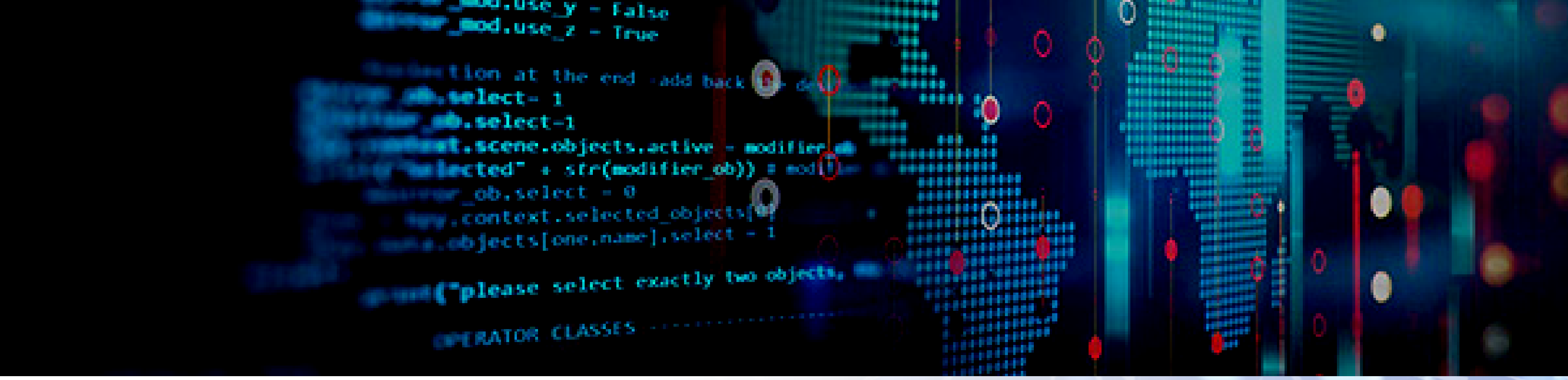
* OpenSSH 8.7p1
* TOR Virtual Network Tunneling Tool 0.4.6.7
* Faraday 3.17.0
* Nmap Port Scanner 7.92
* SQLMAP - Automatic SQL Injection Tool 1.5.8
* Logwatch 7.5.6
* Lynis Auditing Tool 3.0.6
* American Fuzzy Lop plus plus 3.14c
* Hashcat Advanced Password Recovery 6.2.3 Source Code
* Hashcat Advanced Password Recovery 6.2.3 Binary Release

Kali Linux Tutorials

* Tko-Subs : A Tool That Can Help Detect And Takeover Subdomains With Dead DNS Records
* Bantam : A PHP Backdoor Management And Generation tool/C2 Featuring End To End Encrypted Payload Stre
* NinjaDroid : Ninja Reverse Engineering On Android APK Packages
* Nimplant : A Cross-Platform Implant Written In Nim
* How Does Your Browser Spy on You?
* Http-Request-Smuggling : HTTP Request Smuggling Detection Tool
* AlanFramework : A Post-Exploitation Framework
* Karton : Distributed Malware Processing Framework Based On Python, Redis And MinIO
* Wsh : Web Shell Generator And Command Line Interface
* Jarm : Active Transport Layer Security (TLS) server fingerprinting tool

GBHackers Analysis

* 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
* Microsoft Reported Another Windows Print Spooler RCE Zero-day Bug
* SolarWinds Actors Hacked 27 State Attorneys' Offices in the U.S.



Weekly Cyber Security Video and Podcasts

SANS DFIR

* [FOR509:Cloud Forensics & Incident Response Course Preview]
* [Getting started in DFIR: Testing 1,2,3]
* [DFIR Summit 2021]
* [STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign]

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: Gather WiFi Reconnaissance on this $5 MicroController]
* [The Biggest Cryptocurrency Hack Ever - Why Did It Happen? - ThreatWire]
* [HakByte: Practice Hash Recovery Online with Google Colab]

The PC Security Channel [TPSC]

* [BlackMatter Ransomware]
* [Discord Ransomware]

Eli the Computer Guy

* [eBeggar Wednesday - MASK MANDATES are BACK edition]
* [Arduino Introduction]
* [Text Analysis with Azure Cognitive Services]
* [Cyber Security Introduction]

Security Now

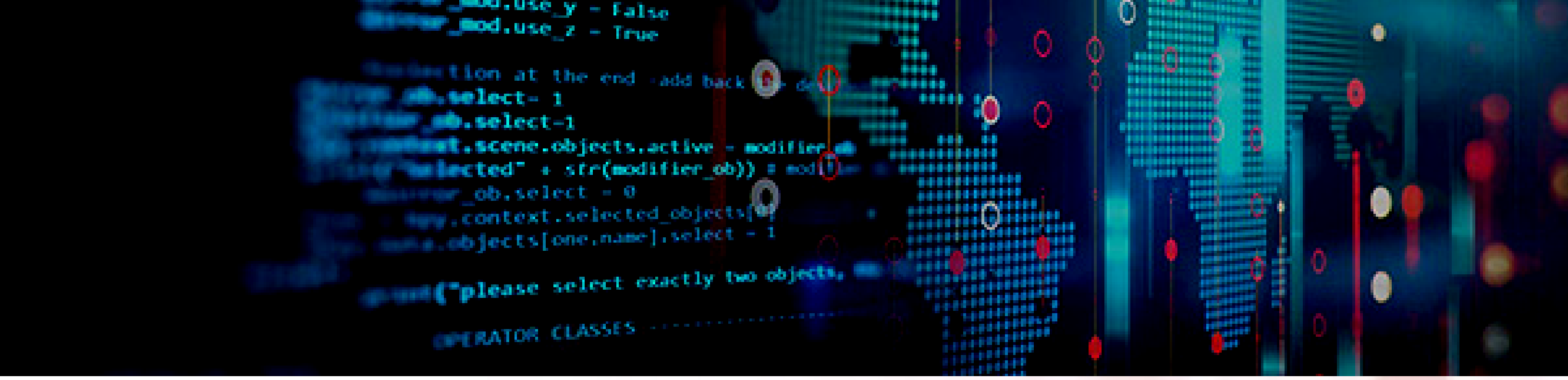
* [Microsoft's Culpable Negligence - Firefox Update, Magniber, Merger of Avast and NortonLifeLock]
* [Apple's CSAM Mistake - Flawed Random Number Generator, Super Duper Secure Mode, TCP Stack Error]

Troy Hunt

* [Weekly Update 257]

Intel Techniques: The Privacy, Security, & OSINT Show

* [231-This Week In Privacy, Security, & OSINT]
* [230-Personal Data Removal Revisited]



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

* 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
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies

FireEye

* 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
* [Security Nation] Daniel Crowley on Running a Cybersecurity Internship
* Fortinet FortiWeb OS Command Injection
* [The Lost Bots] Episode 3: Stories From the SOC
* Metasploit Wrap-Up
* When One Door Opens, Keep It Open: A New Tool for Physical Security Testing
* Energize Your Incident Response and Vulnerability Management With Crowdsourced Automation Workflows

Proof of Concept (PoC) & Exploits

Packet Storm Security

* 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
* Cyberoam NetGenie Cross Site Scripting
* SonicWall NetExtender 10.2.0.300 Unquoted Service Path
* COMMAX CVD-Axx DVR 5.1.4 Weak Default Credentials Stream Disclosure
* COMMAX Smart Home Ruvie CCTV Bridge DVR Service Unauthenticated Config Write / DoS
* COMMAX Smart Home Ruvie CCTV Bridge DVR Service RTSP Credential Disclosure
* COMMAX UMS Client ActiveX Control 1.7.0.2 Buffer Overflow
* COMMAX WebViewer ActiveX Control 2.1.4.5 Buffer Overflow
* COMMAX Smart Home IoT Control System CDP-1020n SQL Injection

CXSecurity

* 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
* Chikitsa 2.0.0 Cross Site Scripting
* PluXML 5.8.7 Cross Site Scripting

Proof of Concept (PoC) & Exploits

Exploit Database

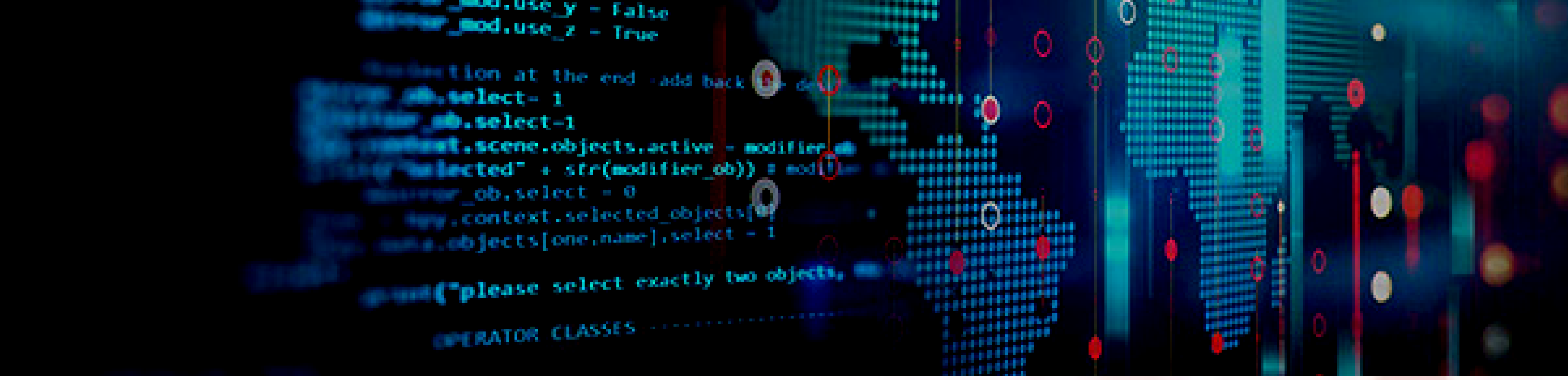
* [webapps] RaspAP 2.6.6 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Simple Phone book/directory 1.0 - 'Username' SQL Injection (Unauthenticated)
* [webapps] Online Traffic Offense Management System 1.0 - Remote Code Execution (RCE) (Unauthenticated
* [webapps] Laundry Booking Management 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
* [webapps] COMMAX Smart Home Ruvie CCTV Bridge DVR Service - Config Write / DoS (Unauthenticated)
* [webapps] COMMAX Smart Home Ruvie CCTV Bridge DVR Service - RTSP Credentials Disclosure
* [webapps] COMMAX Smart Home IoT Control System CDP-1020n - SQL Injection Authentication Bypass
* [webapps] COMMAX Biometric Access Control System 1.0.0 - Authentication Bypass
* [webapps] Simple Water Refilling Station Management System 1.0 - Remote Code Execution (RCE) through
* [webapps] Simple Water Refilling Station Management System 1.0 - Authentication Bypass
* [webapps] NetGear D1500 V1.0.0.21_1.0.1PE - 'Wireless Repeater' Stored Cross-Site Scripting (XSS)
* [webapps] CentOS Web Panel 0.9.8.1081 - Stored Cross-Site Scripting (XSS)
* [webapps] RATES SYSTEM 1.0 - Authentication Bypass
* [webapps] Simple Image Gallery System 1.0 - 'id' SQL Injection

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

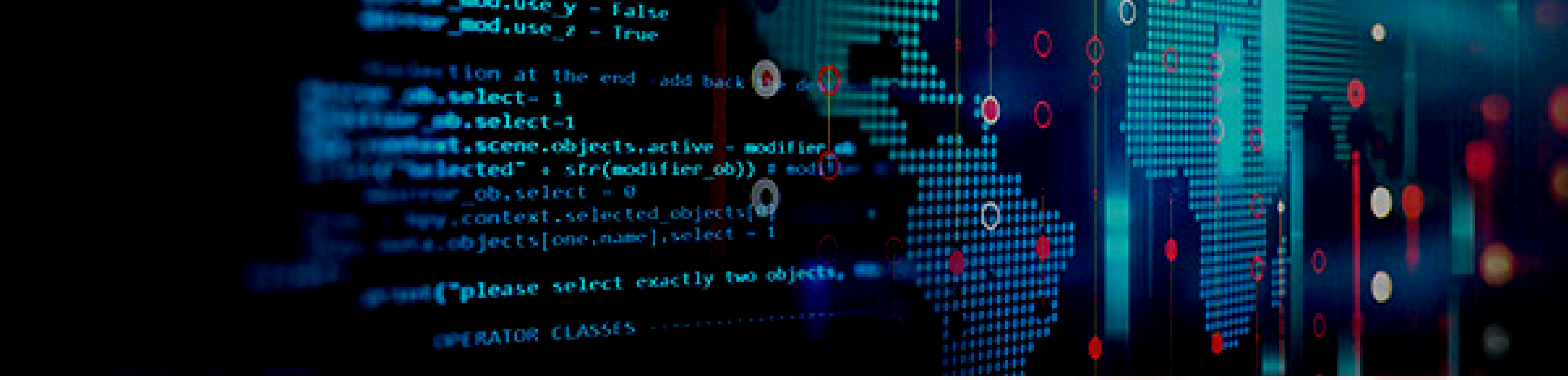
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.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.


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_ob
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects
OPERATOR CLASSES

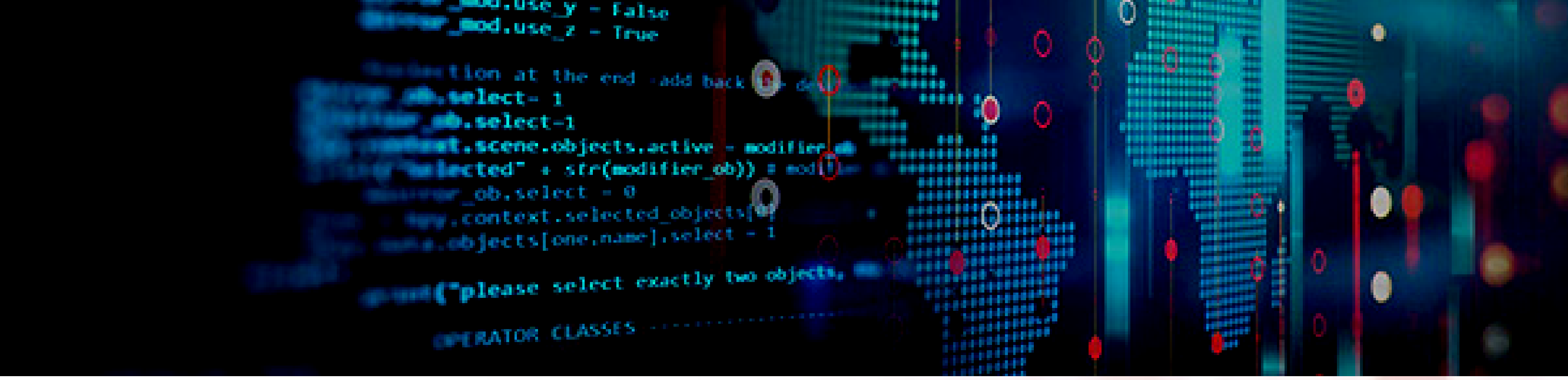
Dark Web News

Darknet Live

Grams Admin Admits Laundering $300 Million in Bitcoin
The administrator of Grams, one of the first darkweb search engines, pleaded guilty to money laundering charges. (via darknetlive.com)
Australian Man Arrested for Importing 5 Kilos of Meth
Authorities in Australia arrested a suspect for allegedly importing five kilos of meth from the United States. (via darknetlive.com)
"Eastcoastcartelkings" Admits Selling Counterfeit Oxy Pills
A man living in Connecticut pleaded guilty to selling counterfeit oxycodone pills through the darkweb. (via darknetlive.com)
Dream Vendor "1nolefb1" Found Guilty of Drug Distribution
A jury found a Connecticut man guilty of distributing fentanyl analogues through the darkweb. (via darknetlive.com)

Dark Web Link

Dark Web: Dreamland Of False Digital Certificates
AppViewX continually monitors cyber-attack events occuring all around the world in the realm of cyber security. The funny thing about cyber-attacks is that they don't appear to be real until they happen to us. Due to a lack of knowledge, you may be unaware of how large the cybercrime business is. However, keep in mind [...] The post Dark Web: Dreamland Of False Digital Certificates appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
As Vaccine Passport Programs Crush, Black Market For Fake Vaccine Certificates Does Thriving Business
Since proof of vaccination was adopted by many countries as a means of satisfying Covid-19 entry requirements, fake vaccine certificates is been obtainable for purchase, nonetheless the market use to have exploded as the idea of &#8220;vaccine passports&#8221; has spread to domestic life and everyday activities. The market for fake vaccine certificates happens to be [...] The post As Vaccine Passport Programs Crush, Black Market For Fake Vaccine Certificates Does Thriving Business appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Ohio Resident Appeals Guilty To Operating Darknet-Based Bitcoin 'Mixer' That Fraudedover $300 Million
Helix, a Darknet-based cryptocurrency laundering service, was operated by an Ohio man who pleaded guilty towards a money laundering intrigue today. Larry Dean Harmon, 38, of Akron, admitted to operating Helix between 2014 and 2017, according to court documents.Helix was a bitcoin&#8221;tumbler&#8221; or &#8220;mixer,&#8221; letting customers to send bitcoin to chosen recipients in a way [...] The post Ohio Resident Appeals Guilty To Operating Darknet-Based Bitcoin 'Mixer' That Fraudedover $300 Million 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_ob
"Selected" + str(modifier_ob)) # modi
ob.select = 0
.context.selected_objects[
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Advisories

US-Cert Alerts & bulletins

* Hurricane-Related Scams
* Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities
* ISC Releases Security Advisory for BIND
* &#8239;Cisco Releases Security Updates&#8239;for Multiple Products
* Mozilla Releases Security Updates
* Adobe Releases Multiple Security Updates
* Google Releases Security Updates for Chrome
* CISA Provides Recommendations for Protecting Information from Ransomware-Caused Data Breaches
* AA21-229A: BadAlloc Vulnerability Affecting BlackBerry QNX RTOS
* AA21-209A: Top Routinely Exploited Vulnerabilities
* Vulnerability Summary for the Week of August 9, 2021
* Vulnerability Summary for the Week of August 2, 2021

Zero Day Initiative Advisories

ZDI-CAN-14578: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14580: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13664: SolarWinds
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 '@fkadibs' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14719: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14718: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public

advisory.

ZDI-CAN-14720: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14722: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14581: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14582: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14579: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14595: 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 'Francis Provencher {PRL}' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14621: Linux

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Ryota Shiga(@Ga_ryo_) of Flatt Security' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14689: Linux

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Ryota Shiga(@Ga_ryo_) of Flatt Security' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15055: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15054: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15058: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15063: Oracle

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 'Guy Lederfein of Trend Micro Security Research' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14974: 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 'Anonymous' was reported to the affected vendor on: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15057: 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: 2021-08-20, 3 days ago. The vendor is given until 2021-12-18 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14575: 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: 2021-08-18, 5 days ago. The vendor is given until 2021-12-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14470: Electronic Arts

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 'brsn (@brsn76945860)' was reported to the affected vendor on: 2021-08-18, 5 days ago. The vendor is given until 2021-12-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14771: Oracle

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: 2021-08-18, 5 days ago. The vendor is given until 2021-12-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14576: 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: 2021-08-18, 5 days ago. The vendor is given until 2021-12-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14577: 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: 2021-08-18, 5 days ago. The vendor is given until 2021-12-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

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.

Red Hat Security Advisory 2021-3178-01

Red Hat Security Advisory 2021-3178-01 - The System Security Services Daemon service provides a set of daemons to manage access to remote directories and authentication mechanisms. It also provides the Name Service Switch and the Pluggable Authentication Modules interfaces toward the system, and a pluggable back-end system to connect to multiple different account sources. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-3177-01

Red Hat Security Advisory 2021-3177-01 - The cloud-init packages provide a set of init scripts for cloud instances. Cloud instances need special scripts to run during initialization to retrieve and install SSH keys, and to let the user run various scripts.

Red Hat Security Advisory 2021-3158-01

Red Hat Security Advisory 2021-3158-01 - Exiv2 is a C++ library to access image metadata, supporting read and write access to the Exif, IPTC and XMP metadata, Exif MakerNote support, extract and delete methods for Exif thumbnails, classes to access Ifd, and support for various image formats. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-3160-01

Red Hat Security Advisory 2021-3160-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.13.0. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-3157-01

Red Hat Security Advisory 2021-3157-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-3155-01

Red Hat Security Advisory 2021-3155-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.13.0. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-3152-01

Red Hat Security Advisory 2021-3152-01 - Exiv2 is a C++ library to access image metadata, supporting read and write access to the Exif, IPTC and XMP metadata, Exif MakerNote support, extract and delete methods for Exif thumbnails, classes to access Ifd, and support for various image formats. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-3153-01

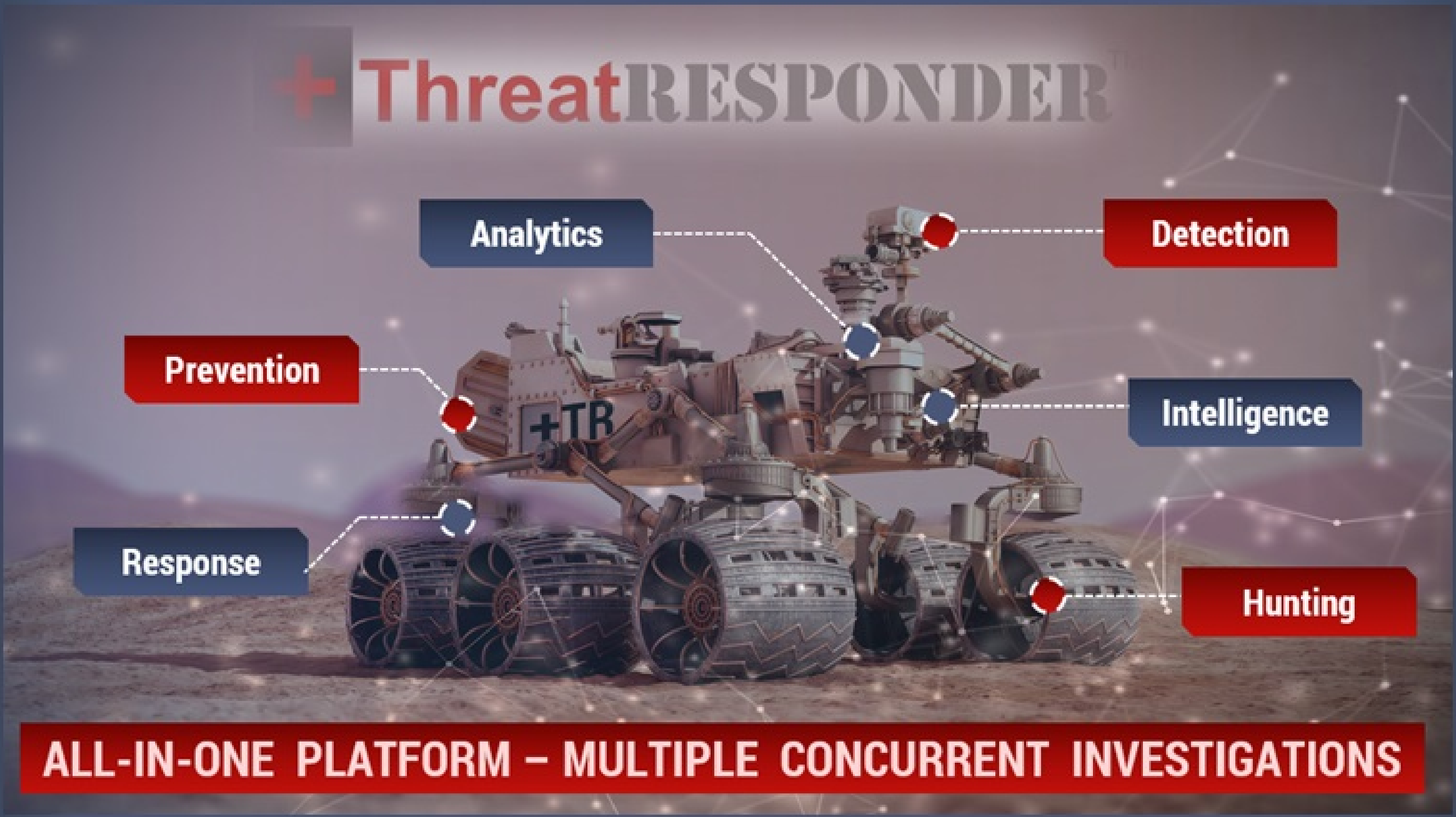
Red Hat Security Advisory 2021-3153-01 - Exiv2 is a C++ library to access image metadata, supporting read and write access to the Exif, IPTC and XMP metadata, Exif MakerNote support, extract and delete methods for Exif thumbnails, classes to access Ifd, and support for various image formats. Issues addressed 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

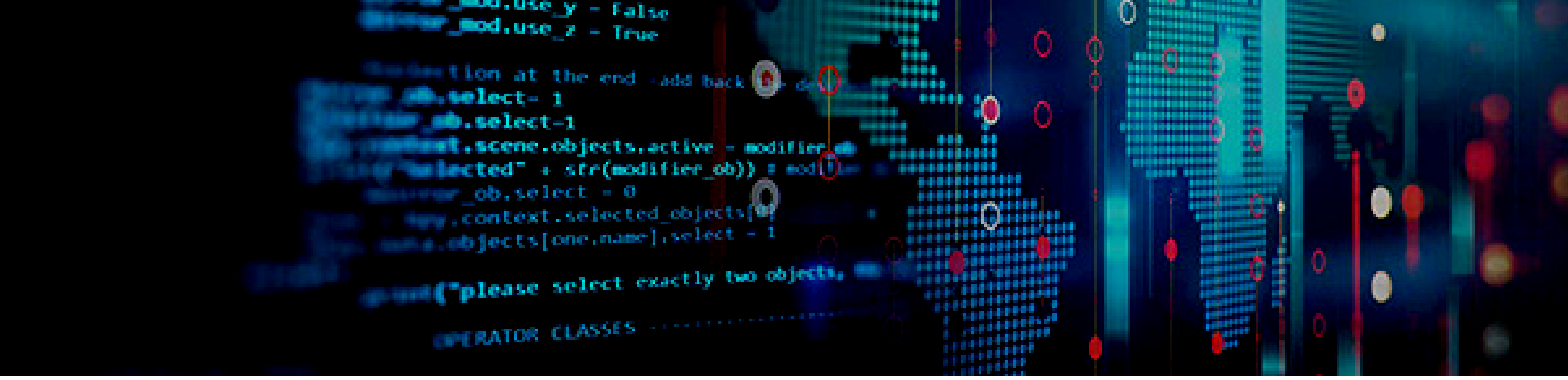
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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

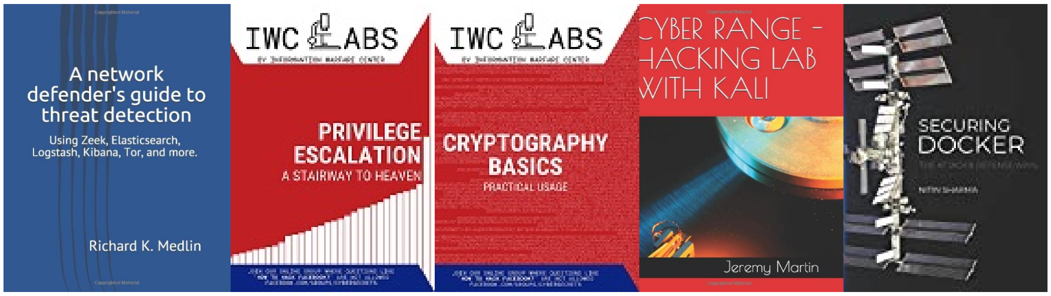

mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier
"elected" + str(modifier_ob)) # mod
ob.select = 0
context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP