May-17-21

CYBER WEEKLY AWARENESS REPORT

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

netSecurity®

INFORMATION WARFARE CENTER

LINUX

ARGOS APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

May 17, 2021

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

Summary

Internet Storm Center Infocon Status

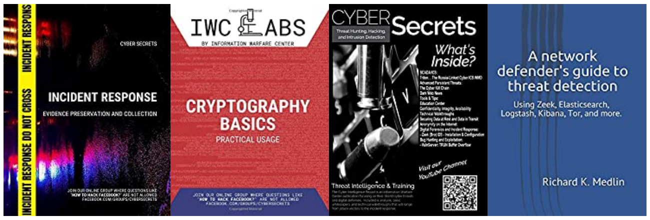
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

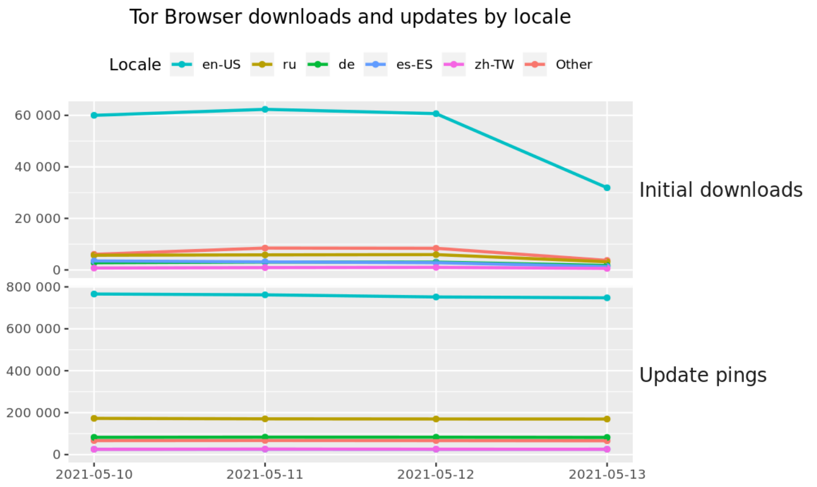
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

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

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


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



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

Interesting News

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

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

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

Index of Sections

LATEST NEWS

Packet Storm Security

* Rapid7 Source Code, Alert Data Accessed In Codecov Supply Chain Attack
* DarkSide Explained: The Ransomware Group Behind The Attack
* US Fuel Pipeline Paid Hackers $5 Million In Ransom
* Toshiba Unit Hacked By DarkSide
* Tesla Stops Accepting Bitcoin Due To Fossil Fuel Use
* US Petrol Supplies Tighten After Colonial Pipeline Hack
* Hacker Manipulates Apple's Find My Network For Data Exfiltration
* FACT SHEET: President Signs Executive Order Charting New Course To Improve The Nation's Cybersecurity
* Hackers Leverage Adobe Zero Day Bug Impacting Adobe Reader
* CISA Warns Over FiveHands File-Encrypting Malware Variant
* Washington DC Police Allegedly Offered $100k To Hackers To Stop Leak
* AWS Configuration Issues Lead To Exposure Of 5 Million Records
* Vulnerability Attacks Weakness In Microsoft Azure VM Extensions
* Colonial Pipeline Ransomware Attack: Everything You Need To Know
* Lemon Duck Cryptojacking Botnet Changes Up Tactics
* Finance Giant Plaid Paid People $500 For Their Employer Payroll Logins
* Major U.S. Pipeline Crippled In Ransomware Attack
* Justice Department Quietly Seized Washington Post Reporters' Phone Records During Trump Era
* Amazon Seized, Destroyed Two Million Fake Products In 2020
* Group Pleads Guilty To Running Bulletproof Hosting Service
* Biggest ISPs Paid For 8.5 Million Fake FCC Comments Opposing Net Neutrality
* Ryuk Ransomware Attack Sprung By Frugal Student
* New Moriya Rootkit Stealthily Backdoors Windows
* Critical Cisco Bugs Threaten Corporate Networks
* Your Own Phone Number Can Be Used To Hack You, Study Finds

Krebs on Security

* DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized
* Microsoft Patch Tuesday, May 2021 Edition
* A Closer Look at the DarkSide Ransomware Gang
* Fintech Startup Offers $500 for Payroll Passwords
* Investment Scammer John Davies Reinvents Himself?
* Malicious Office 365 Apps Are the Ultimate Insiders
* The Wages of Password Re-use: Your Money or Your Life
* Task Force Seeks to Disrupt Ransomware Payments
* Experian API Exposed Credit Scores of Most Americans
* Experian's Credit Freeze Security is Still a Joke

LATEST NEWS

Dark Reading

* Rapid7 Source Code Accessed in Supply Chain Attack
* How Faster COVID-19 Research Is Being Made Possible by Secure Silicon
* Cisco Confirms Plans to Acquire Kenna Security
* Chart: Cybersecurity Now a Top Corporate Priority
* SOC Teams Burdened by Alert Fatigue Explore XDR
* Wi-Fi Design, Implementation Flaws Allow a Range of Frag Attacks
* Security Trends to Follow at RSA Conference 2021
* Software, Incident Response Among Big Focus Areas in Biden's Cybersecurity Executive Order
* 85% of Data Breaches Involve Human Interaction: Verizon DBIR
* Firms Struggle to Secure Multicloud Misconfigurations
* Dragos & IronNet Partner on Critical Infrastructure Security
* When AI Becomes the Hacker
* Microsoft Adds GPS Location to Identity & Access Control in Azure AD
* Adapting to the Security Threat of Climate Change
* Defending the Castle: How World History Can Teach Cybersecurity a Lesson
* Verizon DBIR 2021: "Winners" No Surprise, But All-round Vigilance Essential
* Despite Heightened Breach Fears, Incident Response Capabilities Lag
* Researchers Unearth 167 Fake iOS & Android Trading Apps
* Putting the Spotlight on DarkSide
* 66% of CISOs Feel Unprepared for Cyberattacks

The Hacker News

* U.S. Pipeline Ransomware Attackers Go Dark After Servers and Bitcoin Are Seized
* Hackers Using Microsoft Build Engine to Deliver Malware Filelessly
* Report to Your Management with the Definitive 'Incident Response for Management' Presentation Templat
* Pakistan-Linked Hackers Added New Windows Malware to Its Arsenal
* Magecart Hackers Now hide PHP-Based Backdoor In Website Favicons
* Big Cybersecurity Tips For Remote Workers Who Use Their Own Tech
* Colonial Pipeline Paid Nearly $5 Million in Ransom to Cybercriminals
* Rapid7 Source Code Breached in Codecov Supply-Chain Attack
* Can Data Protection Systems Prevent Data At Rest Leakage?
* Dark Web Getting Loaded With Bogus Covid-19 Vaccines and Forged Cards
* Nearly All Wi-Fi Devices Are Vulnerable to New FragAttacks
* Latest Microsoft Windows Updates Patch Dozens of Security Flaws
* Ransomware Gang Leaks Metropolitan Police Data After Failed Negotiations
* Alert: Hackers Exploit Adobe Reader 0-Day Vulnerability in the Wild
* LIVE Webinar - The Rabbit Hole of Automation

LATEST NEWS

Security Week

* Researchers Abuse Apple's Find My Network for Data Upload
* Rapid7 Source Code Exposed in Codecov Supply Chain Attack
* Vendor Survey vs Reality on SASE Implementation
* Biden to Bring Up Russian Hackers Issue With Putin
* Citrix Patches Vulnerability in Workspace App for Windows
* Verizon DBIR 2021: Ransomware, Web App and Phishing Attacks Dominate
* Microsoft Warns of Attacks on Aerospace, Travel Sectors
* Query.AI Launches With Security Investigations Platform, $4.6 Million Seed Funding
* Security Automation: Data is More Important Than Process
* UK Foreign Secretary Calls for Cooperation on Cybersecurity
* Green Energy Company Volue Hit by Ransomware
* Colonial Pipeline Initiates Restart of Pipeline Operations After Ransomware Attack
* Tech Audit of Colonial Pipeline Found 'Glaring' Problems
* Biden Signs Order to Beef Up Federal Cyber Defenses
* Asset Discovery Provider Panaseer Raises $26.5 Million
* Inside The UK's Active Cyber Defense Program
* Apple Removed 95,000 Fraudulent Applications From App Store in 2020
* Security Researchers Dive Into DarkSide Ransomware
* Industry Reactions to Ransomware Attack on Colonial Pipeline
* Jamf to Acquire Wandera for $400 Million to Bring Zero Trust to Apple Ecosystem

Infosecurity Magazine

* Lemonade Denies "Unforgivably Negligent" Security Gaffe
* US Sentences Cyber-Stalker Who Sent Sex Workers to Family's Home
* Rapid7 Source Code Accessed in Cyber-attack
* Ireland's Healthcare System's IT Offline Following Ransomware Attack
* Microsoft Alerts Aviation and Travel Firms to RAT Campaign
* Quarter of CISOs Self-Medicate as Pandemic Stress Spikes
* Colonial Reportedly Paid $5 Million Ransom
* Cyber-bullying Spawns Artistic Protest
* Cyber-attacks Cost Small US Businesses $25k Annually
* Consumers Unforgiving of Merchants' Data Failings
* Record Number of Breaches Detected Amid #COVID19
* Biden Executive Order Mandates Zero Trust and Strong Encryption

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Paying the Ransom Is Not Just About Decryption
* Kicking You While You're Down: Ransomware Attacks Begin to Adopt a "Triple Extortion" Model
* Ransomware Attack Demands Cause Cyber Insurance Claim Amounts to Skyrocket
* New Verizon DBIR: Credentials Stolen in 85% of Social Engineering Breaches
* FBI Finds Phishing Sites Abusing Search Results and Ads to Steal Banking Credentials
* A New Smishing Trojan is Out and About
* New QuickBooks-Themed Phishing Attack Seeks to Infect Victims with Dridex Malware
* Email-Based Threats Increase 64% as Attacks Grow in Sophistication and Volume
* Phishing Scammers Remove 'External Sender' Email Warnings Impersonating Internal Users
* KnowBe4 Named a Leader in the Spring 2021 G2 Grid Report for Security Awareness Training

ISC2.org Blog

* Do You Have These Top Cyber Security Skills?
* Creating Secure Software Requires More Than Just Motivation
* Unlimited Access to Free Industry Leading Cybersecurity Webinars
* CISSPs from Around the Globe: An Interview with Jason Lau
* Help Shape The HCISPP Exam

HackRead

* Avaddon ransomware gang: 'We stole 3TB of French AXA Group data'
* DarkSide ransomware call it quits after Bitcoin, servers are seized
* Top Certifications for Network Security Administrators in 2021
* Employee training is key to keeping your enterprise safe
* Old bugs exposing all WiFi enabled devices to FragAttacks
* Microsoft shares details of malware attack on aerospace, travel sector
* Babuk ransomware gang leaks DC police data as negotiations fail

Koddos

* Avaddon ransomware gang: 'We stole 3TB of French AXA Group data'
* DarkSide ransomware call it quits after Bitcoin, servers are seized
* Top Certifications for Network Security Administrators in 2021
* Employee training is key to keeping your enterprise safe
* Old bugs exposing all WiFi enabled devices to FragAttacks
* Microsoft shares details of malware attack on aerospace, travel sector
* Babuk ransomware gang leaks DC police data as negotiations fail

LATEST NEWS

Naked Security

* Apple AirTag hacked again - free internet with no mobile data plan!
* Gamers beware! Crooks take advantage of MSI download outage&hellip;
* S3 Ep32: AirTag jailbreak, Dell vulns, and a never-ending scam [Podcast]
* Beware fake online trading apps, on iOS as well as Android
* Apple AirTag jailbroken already - hacked in rickroll attack
* Never say never! Warren Buffett caught up in integer overflow error&hellip;
* S3 Ep31: Apple zero-days, Flubot scammers and PHP supply chain bug [Podcast]
* Firefox for Android gets critical update to block cookie-stealing hole
* Dell fixes exploitable holes in its own firmware update driver - patch now!
* Apple products hit by fourfecta of zero-day exploits - patch now!

Threat Post

* FIN7 Backdoor Masquerades as Ethical Hacking Tool
* DarkSide Ransomware Suffers 'Oh, Crap!' Server Shutdowns
* 'Scheme Flooding' Allows Websites to Track Users Across Browsers
* Verizon: Pandemic Ushers in &#8531; More Cyber-Misery
* Ransomware's New Swindle: Triple Extortion
* How to Get into the Bug-Bounty Biz: The Good, Bad and Ugly
* Colonial Pipeline Shells Out $5M in Extortion Payout, Report
* Ransomware Going for $4K on the Cyber-Underground
* Beyond MFA: Rethinking the Authentication Key
* Fresh Loader Targets Aviation Victims with Spy RATs

Null-Byte

* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks
* Protect Your Browsing with This 10-Year VPN Subscription
* How to Write Your Own Subdomain Enumeration Script for Better Recon
* Learn to Code Today with This $20 Web Development Course
* How to Install Kali Linux as a Portable Live USB for Pen-Testing & Hacking on Any Computer
* Master Python, Django, Git & GitHub with This Bundle
* Clear the Logs & Bash History on Hacked Linux Systems to Cover Your Tracks & Remain Undetected

LATEST NEWS

IBM Security Intelligence

* Social Engineering: How to Keep Security Researchers Safe
* AI Security Threats: The Real Risk Behind Science Fiction Scenarios
* How to Reduce Zero Trust Frustration By Capturing Context
* Cloud Data Privacy: Now, Where Did I Put Those Keys?
* Data Privacy: How the Growing Field of Regulations Impacts Businesses
* Security by Design and NIST 800-160, Part 2: Life Cycle Processes
* What Is SIEM and How Does it Work? The Past, Present and Future
* DevSecOps: Closing the Security Gap With Developers
* Private LTE or 5G: Which Is More Secure?
* Penetration Testing 101: What You Need to Know

InfoWorld

* Scala 3 ushers in 'complete overhaul' of the language
* Don't migrate your problems to the cloud
* Angular 12 arrives with pile of improvements
* Python's creators unveil speedup plans for Python
* Deno 1.10 overhauls test runner
* How to use the Svelte JavaScript framework
* Understanding the process automation landscape
* JDK 17: The new features in Java 17
* Babel project is running out of money
* Get moving with Microsoft's FAST web components

C4ISRNET - Media for the Intelligence Age Military

* Will the cyber mission force soon receive more personnel?
* A hidden potential risk for DoD employees when companies share data
* British Royal Air Force invests in space capabilities
* After more than a decade, agency to retire experimental missile warning satellites
* Biden orders wide cybersecurity changes for government, contractors
* A new constellation? Space Force wants to get into tactical satellite imagery business
* Pentagon tries to 'find the right balance' on JADC2 standards for services
* Congress can't 'take foot off the gas' on DoD electronic warfare
* The Army is making tank upgrades as simple as switching video game cartridges
* New Pentagon directive to manage gobs of data: Make it all sharable

The Hacker Corner

Conferences

* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)
* How To Sponsor Cybersecurity Conferences
* How To Secure Earned Cybersecurity Speaking Engagements
* World RPA & AI Summit | Interview with Ashley Pena
* The State of AI in Cybersecurity | Interview with Jessica Gallagher
* AWSN Women in Security Awards | Interview with Abigail Swabey
* An Introduction to Cybersecurity Call for Papers

Google Zero Day Project

* Designing sockfuzzer, a network syscall fuzzer for XNU
* Policy and Disclosure: 2021 Edition

Capture the Flag (CTF)

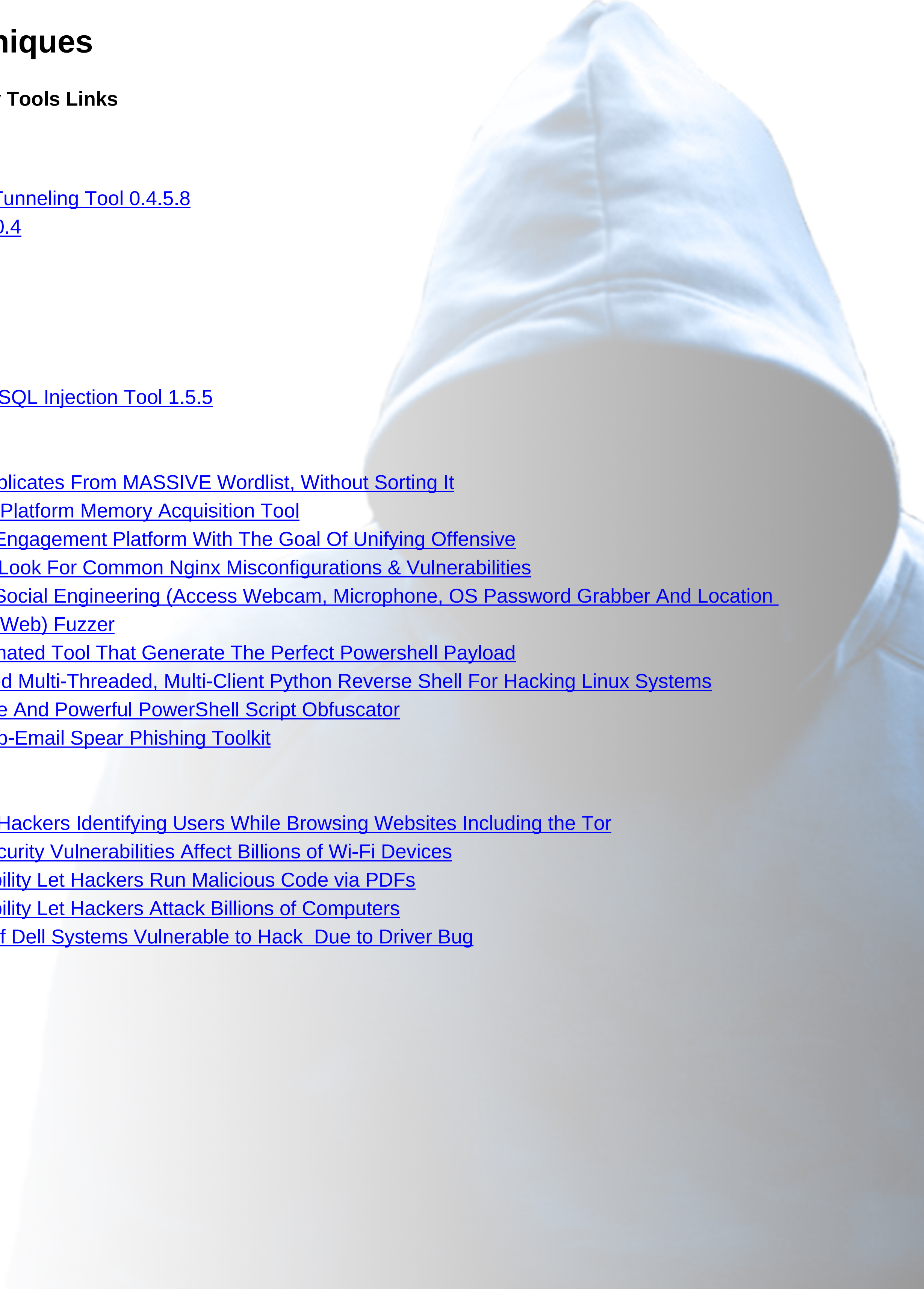
CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

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

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

* Prime (2021): 2
* DriftingBlues: 9 (final)
* AdmX: 1.0.1
* Worst Western Hotel: 1
* Midwest: 1

Tools & Techniques



Packet Storm Security Tools Links

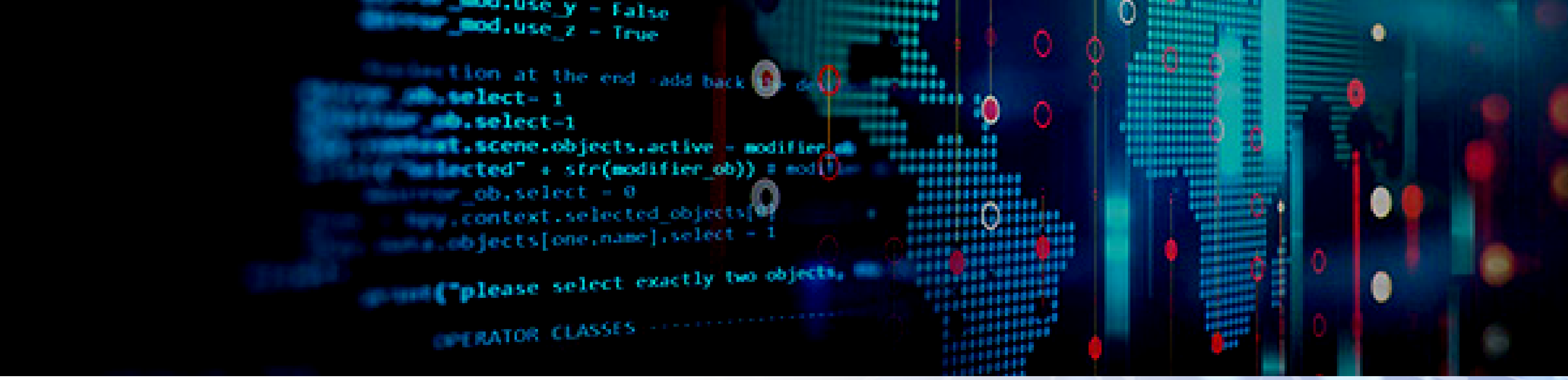
* Global Socket 1.4.30
* Packet Fence 10.3.0
* TOR Virtual Network Tunneling Tool 0.4.5.8
* Lynis Auditing Tool 3.0.4
* TestSSL 3.0.5
* Falco 0.28.1
* jSQL Injection 0.85
* OpenDNSSEC 2.1.9
* OATH Toolkit 2.6.7
* SQLMAP - Automatic SQL Injection Tool 1.5.5

Kali Linux Tutorials

* Duplicut : Remove Duplicates From MASSIVE Wordlist, Without Sorting It
* WinPmem : The Multi-Platform Memory Acquisition Tool
* Paragon : Red Team Engagement Platform With The Goal Of Unifying Offensive
* Nginxpwner : Tool To Look For Common Nginx Misconfigurations & Vulnerabilities
* Storm-Breaker : Tool Social Engineering (Access Webcam, Microphone, OS Password Grabber And Location
* VAF: Very Advanced (Web) Fuzzer
* MeterPwrShell : Automated Tool That Generate The Perfect Powershell Payload
* PwnLnX : An Advanced Multi-Threaded, Multi-Client Python Reverse Shell For Hacking Linux Systems
* Invoke-Stealth : Simple And Powerful PowerShell Script Obfuscator
* SniperPhish : The Web-Email Spear Phishing Toolkit

GBHackers Analysis

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



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 200: The Final Episode
* Kevin Ripa's 3MinMax Series Wrap Up | LIVE STREAM
* Episode 199: Analyzing Mac RAM in AXIOM (Collected with MacQuisition)
* Episode 198: Analyzing Mac RAM in AXIOM

Defcon Conference

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

Hak5

* HakByte: Getting Started with Qubes OS
* Ephemeral Technology - Hack Across America 2021 - Hak5 2906
* Colonial Pipeline Hit With Ransomware; Apple AirTags Hacked - ThreatWire

The PC Security Channel [TPSC]

* Apple Supplier Hacked by REVIL Ransomware: Live Demo & Analysis
* Context in Cybersecurity: Oxford Seminar

Eli the Computer Guy

* Needing an Elevator Pitch - Startup Life
* DOGMA is BAD - Startup Life
* STUPID PROBLEMS - Startup Life
* SOCIAL MEDIA is PERVERTED - Startup Life

Security Now

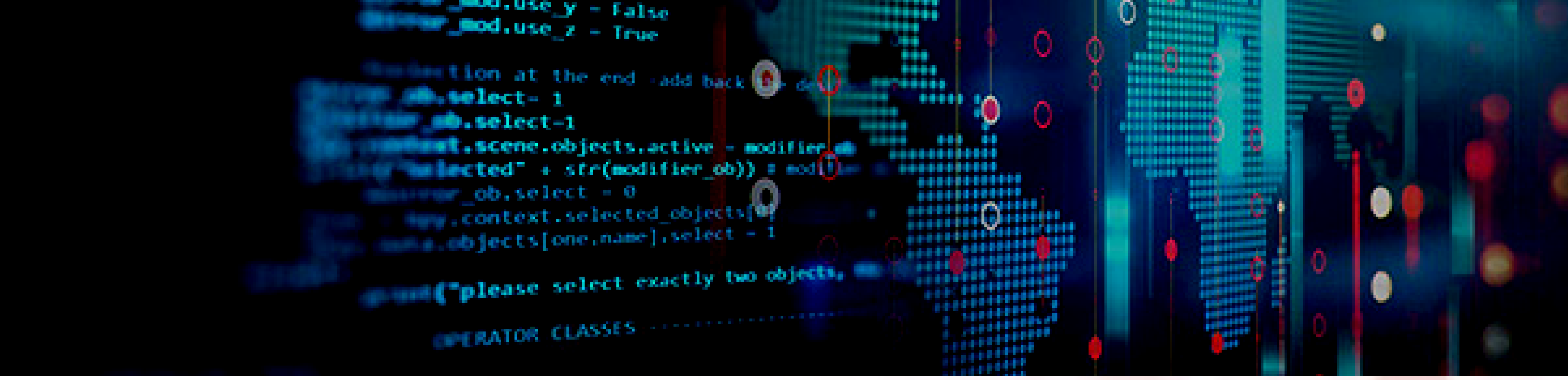
* News From the Darkside - Exim Email Server, Tor's Exit Nodes, TsuNAME, Project Hail Mary
* The Ransomware Task Force - Scripps Health, REvil Hacks Quanta Computer, Emotet Botnet, QNAP

Troy Hunt

* Weekly Update 243

Intel Techniques: The Privacy, Security, & OSINT Show

* 216-The Consequences of Extreme Privacy
* 215-When OSINT Is Abused



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

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

FireEye

* Metasploit Wrap-Up
* Rapid7's 2021 ICER Takeaways: High-Risk Services Among the Fortune 500
* Top Challenges for Security Analytics and Operations, and How a Cloud-Based SIEM Can Help
* Rapid7's Response to Codecov Incident
* [Security Nation] Megan Stifel and Ciaran Martin discuss the sticky issue of ransomware payments
* How ViacomCBS Digital delivers uninterrupted content streaming to millions of fans without compromisi
* Patch Tuesday - May 2021
* Patch Tuesday Dashboard Template Release
* MDR Vendor Must-Haves, Part 10: Included Security Orchestration and Automation
* Metasploit Wrap-Up

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Chrome Array Transfer Bypass
* Student Management System 1.0 Cross Site Scripting
* Podcast Generator 3.1 Cross Site Scripting
* Chamilo LMS 1.11.14 Remote Code Execution
* Internet Explorer jscript9.dll Memory Corruption
* Firefox 72 IonMonkey JIT Type Confusion
* ScadaBR 1.0 / 1.1CE Windows Shell Upload
* Microsoft Internet Explorer 8/11 Use-After-Free
* ScadaBR 1.0 / 1.1CE Linux Shell Upload
* OpenPLC WebServer 3 Remote Code Execution
* Dental Clinic Appointment Reservation System 1.0 SQL Injection
* ZeroShell 3.9.0 Remote Command Execution
* Windows Container Manager Service CmsRpcSrv_MapNamedPipeToContainer Privilege Escalation
* ExifTool DjVu ANT Perl Injection
* Windows Container Manager Service Arbitrary Object Directory Creation Privilege Escalation
* Windows Container Manager Service CmsRpcSrv_MapVirtualDiskToContainer Privilege Escalation
* Windows Container Manager Service CmsRpcSrv_CreateContainer Privilege Escalation
* Backdoor.Win32.Delf.zho Authentication Bypass / Code Execution
* Chevereto 3.17.1 Cross Site Scripting
* Android NFC nfa_rw_sys_disable Type Confusion
* Splinterware System Scheduler Professional 5.30 Privilege Escalation
* Odoo 12.0.20190101 Unquoted Service Path
* Customer Relationship Management (CRM) System 1.0 Shell Upload
* Customer Relationship Management (CRM) System 1.0 Cross Site Scripting
* Customer Relationship Management (CRM) System 1.0 SQL Injection

CXSecurity

* ExifTool DjVu ANT Perl Injection
* OpenPLC WebServer 3 Remote Code Execution
* ScadaBR 1.0 / 1.1CE Windows Shell Upload
* Microweber CMS 1.1.20 Remote Code Execution (Authenticated)
* GravCMS 1.10.7 Unauthenticated Arbitrary YAML Write/Update (Metasploit)
* macOS Gatekeeper Check Bypass
* Human Resource Information System 0.1 Remote Code Execution (Unauthenticated)

Proof of Concept (PoC) & Exploits

Exploit Database

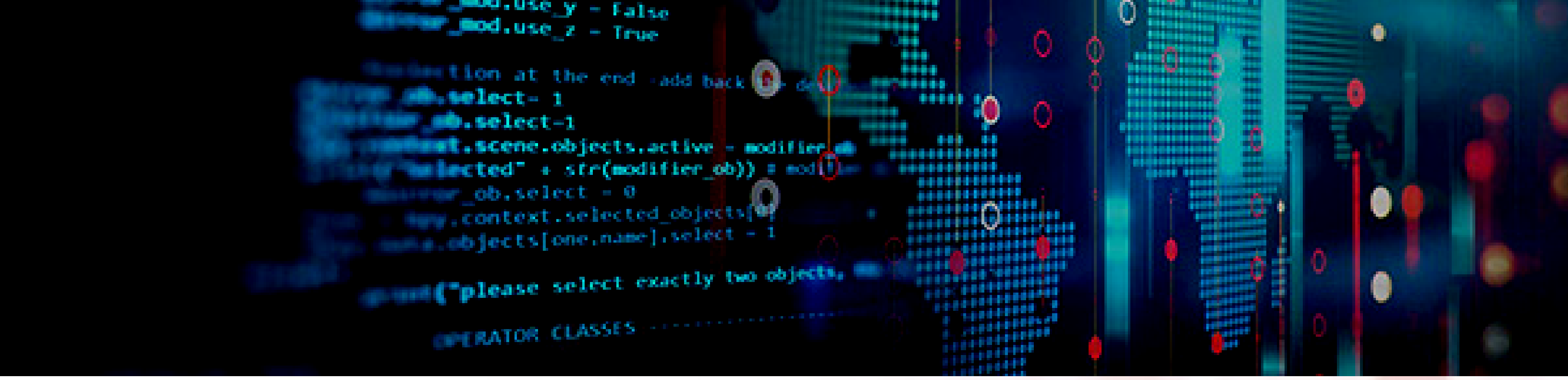
* [webapps] Chamilo LMS 1.11.14 - Remote Code Execution (Authenticated)
* [webapps] Podcast Generator 3.1 - 'Long Description' Persistent Cross-Site Scripting (XSS)
* [webapps] Student Management System 1.0 - 'message' Persistent Cross-Site Scripting (Authenticated)
* [local] Firefox 72 IonMonkey - JIT Type Confusion
* [local] Microsoft Internet Explorer 8/11 and WPAD service 'Jscript.dll' - Use-After-Free
* [webapps] ZeroShell 3.9.0 - Remote Command Execution
* [webapps] Dental Clinic Appointment Reservation System 1.0 - 'date' UNION based SQL Injection (Authen
* [webapps] Dental Clinic Appointment Reservation System 1.0 - Authentication Bypass (SQLi)
* [webapps] Chevereto 3.17.1 - Cross Site Scripting (Stored)
* [local] Splinterware System Scheduler Professional 5.30 - Privilege Escalation
* [local] Odoo 12.0.20190101 - 'nssm.exe' Unquoted Service Path
* [webapps] Microweber CMS 1.1.20 - Remote Code Execution (Authenticated)
* [webapps] Human Resource Information System 0.1 - 'First Name' Persistent Cross-Site Scripting (Aut
* [webapps] PHP Timeclock 1.04 - 'Multiple' Cross Site Scripting (XSS)
* [local] TFTP Broadband 4.3.0.1465 - 'tftpt.exe' Unquoted Service Path
* [local] BOOTP Turbo 2.0.0.1253 - 'bootpt.exe' Unquoted Service Path
* [local] DHCP Broadband 4.1.0.1503 - 'dhcpt.exe' Unquoted Service Path
* [webapps] PHP Timeclock 1.04 - Time and Boolean Based Blind SQL Injection
* [local] Epic Games Rocket League 1.95 - Stack Buffer Overrun
* [webapps] Human Resource Information System 0.1 - Remote Code Execution (Unauthenticated)
* [webapps] Voting System 1.0 - Remote Code Execution (Unauthenticated)
* [local] WifiHotSpot 1.0.0.0 - 'WifiHotSpotService.exe' Unquoted Service Path
* [dos] Sandboxie 5.49.7 - Denial of Service (PoC)
* [webapps] Voting System 1.0 - Authentication Bypass (SQLI)

Exploit Database for offline use

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

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

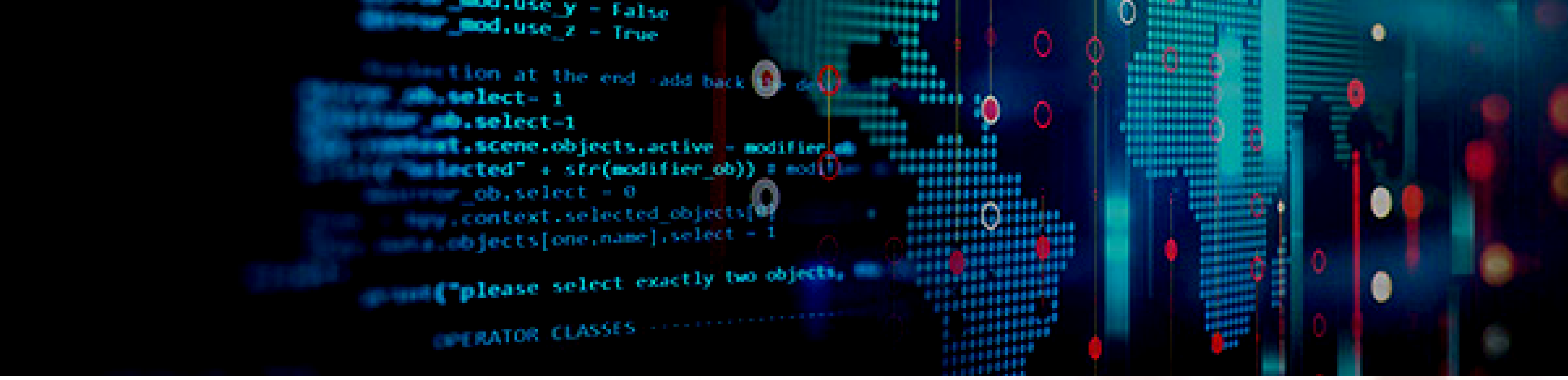
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


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

Latest Hacked Websites

Published on Zone-h.org

http://hangdonghod.go.th/pun10.html
http://hangdonghod.go.th/pun10.html notified by Anonymous_R
http://kudlad.go.th/pun10.html
http://kudlad.go.th/pun10.html notified by Anonymous_R
http://wiangnuepai.go.th/pun10.html
http://wiangnuepai.go.th/pun10.html notified by Anonymous_R
http://banmanglocal.go.th/pun10.html
http://banmanglocal.go.th/pun10.html notified by Anonymous_R
http://tontong.go.th/pun10.html
http://tontong.go.th/pun10.html notified by Anonymous_R
http://thaduea.go.th/pun10.html
http://thaduea.go.th/pun10.html notified by Anonymous_R
http://thakhamlocal.go.th/pun10.html
http://thakhamlocal.go.th/pun10.html notified by Anonymous_R
http://pongyeang.go.th/pun10.html
http://pongyeang.go.th/pun10.html notified by Anonymous_R
http://donpao.go.th/pun10.html
http://donpao.go.th/pun10.html notified by Anonymous_R
http://bantanlocal.go.th/pun10.html
http://bantanlocal.go.th/pun10.html notified by Anonymous_R
http://padad.go.th/pun10.html
http://padad.go.th/pun10.html notified by Anonymous_R
http://paphai.go.th/pun10.html
http://paphai.go.th/pun10.html notified by Anonymous_R
http://tungpheesao.go.th/pun10.html
http://tungpheesao.go.th/pun10.html notified by Anonymous_R
http://songkwae.go.th/pun10.html
http://songkwae.go.th/pun10.html notified by Anonymous_R
http://makhueajae.go.th/pun10.html
http://makhueajae.go.th/pun10.html notified by Anonymous_R
http://thawangthong.go.th/pun10.html
http://thawangthong.go.th/pun10.html notified by Anonymous_R
http://soongnern.go.th/pun10.html
http://soongnern.go.th/pun10.html notified by Anonymous_R



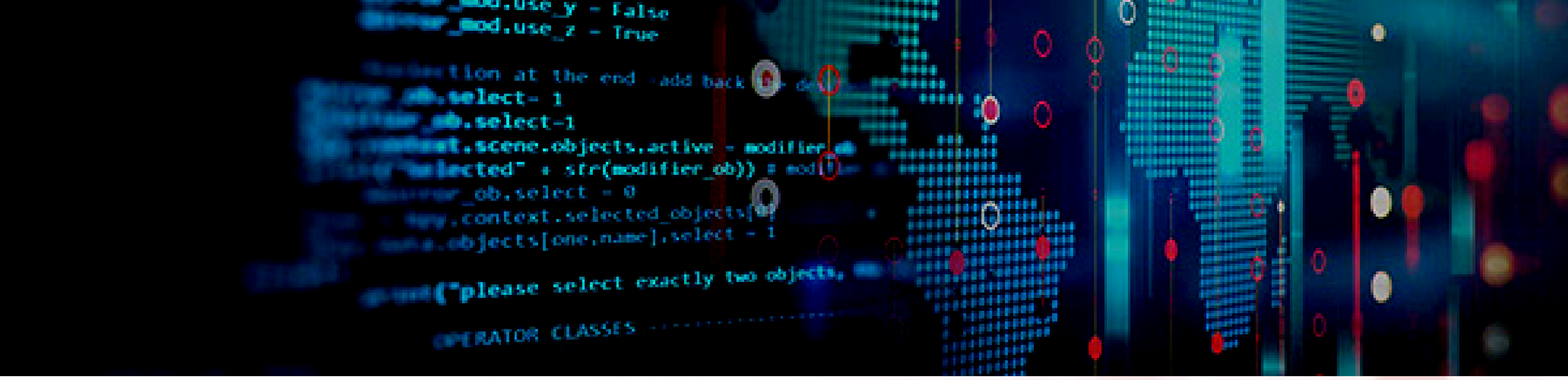
Dark Web News

Darknet Live

[Opioid Vendor "H00k3d" Pleads Guilty to Drug Charges]
A New York man admitted selling more than $1 million worth of opioids and counterfeit currency on darkweb markets. (via darknetlive.com)
Four Arrested in Darkweb Child Abuse Site Investigation
Law enforcement arrested four following an investigation and takedown of one of the largest darkweb child abuse sites. (via darknetlive.com)
Mother and Son Sentenced to Prison for Selling Meth Online
A federal judge sentenced a mother-son duo to a combined 18 years in prison for selling methamphetamine on the darkweb. (via darknetlive.com)
Four Arrested in UK Drug Trafficking Investigation
Authorities in the UK arrested four in a multi-agency investigation into a Â£470,000 drug trafficking operation. (via darknetlive.com)

Dark Web Link

Russian Hacking Forum XSS Has Ruled Out The Ransomware Topics
One of the top-rated Russian speaking hacker forums named &#8220;XSS&#8221; has eventually banned all the topics that were promoting ransomware on its platform. This significant step has been taken to cease unnecessary attention. XSS is a Russia-based hacking forum that was created for sharing knowledge regarding exploits, malware, vulnerabilities and network penetration. As the ransomware [...] The post Russian Hacking Forum XSS Has Ruled Out The Ransomware Topics appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Darknet Drug Lords Jailed For Illegal Narcotics Distribution Of Â£1.3m
Two Scottish darknet drug lords who used the dark web platforms for supplying a significant quantity of narcotics have been put behind bars. The duo had supplied major class A drugs and ran a supply operation. They have been put in Scottish first. The darknet drug lords have been identified as Scott Roddie, aged 29 [...] The post Darknet Drug Lords Jailed For Illegal Narcotics Distribution Of Â£1.3m appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Tor Exit Relays: 27%+ Spied On The Dark Web Activities
A latest study on the dark web infrastructure has revealed that a malicious actor has managed to control over 27% of the complete Tor Network Exit. This has caused malicious Tor Exit Relays. "The entity attacking Tor users is actively exploiting tor users since over a year and expanded the scale of their attacks to a [...] The post Tor Exit Relays: 27%+ Spied On The Dark Web Activities appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* CISA Publishes Eviction Guidance for Networks Affected by SolarWinds and AD/M365 Compromise
* WordPress Releases Security Update
* Adobe Releases Security Updates for Multiple&#8239;Products&#8239;
* Microsoft Releases May 2021 Security Updates
* Citrix Releases Security Updates for Workspace App for Windows
* Juniper Networks Releases Security Updates
* Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware
* Google Releases Security Updates for Chrome
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for
* Vulnerability Summary for the Week of May 3, 2021
* Vulnerability Summary for the Week of April 26, 2021

Zero Day Initiative Advisories

ZDI-CAN-12870: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-12787: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-12784: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-12866: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-12786: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-12871: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or

workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12785: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12869: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12788: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12867: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12868: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13204: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13203: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13207: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13522: 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 'Xavier DANEST' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13744: Fatek Automation

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13741: Foxit

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 'Xu Peng from UCAS and Wang Yanhao from QiAnXin Technology Research Institute ' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13202: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13206: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13703: Siemens

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13743: Fatek Automation

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13656: Schneider Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'David Yesland' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13790: Fatek Automation

A CVSS score 8.8 (AV:N/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: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13201: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2021-05-13, 4 days ago. The vendor is given until 2021-09-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-4953-1

Ubuntu Security Notice 4953-1 - Sean Boran discovered that AWStats incorrectly filtered certain parameters. A remote attacker could possibly use this issue to execute arbitrary code. It was discovered that AWStats incorrectly filtered certain parameters. A remote attacker could possibly use this issue to access sensitive information.

Red Hat Security Advisory 2021-1560-01

Red Hat Security Advisory 2021-1560-01 - Red Hat AMQ Streams, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 1.6.4 serves as a replacement for Red Hat AMQ Streams 1.6.2, and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include a resource exhaustion vulnerability.

Ubuntu Security Notice USN-4952-1

Ubuntu Security Notice 4952-1 - Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues. MySQL has been updated to 8.0.25 in Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.34. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Ubuntu Security Notice USN-4932-2

Ubuntu Security Notice 4932-2 - USN-4932-1 fixed a vulnerability in Django. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that Django incorrectly handled certain filenames. A remote attacker could possibly use this issue to create or overwrite files in unexpected directories. Various other issues were also addressed.

Red Hat Security Advisory 2021-1547-01

Red Hat Security Advisory 2021-1547-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 3.1.115 and .NET Core Runtime 3.1.15. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2021-1546-01

Red Hat Security Advisory 2021-1546-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.203 and .NET Runtime 5.0.6. Issues addressed include a privilege escalation vulnerability.

Ubuntu Security Notice USN-4951-1

Ubuntu Security Notice 4951-1 - Anton Lydike discovered that Flatpak did not properly handle special tokens in desktop files. An attacker could use this to specially craft a Flatpak application that could escape sandbox confinement.

Ubuntu Security Notice USN-4949-1

Ubuntu Security Notice 4949-1 - Ryota Shiga discovered that the eBPF implementation in the Linux kernel did not properly verify that a BPF program only reserved as much memory for a ring buffer as was allocated. A local attacker could use this to cause a denial of service or execute arbitrary code. Manfred Paul discovered that the eBPF implementation in the Linux kernel did not properly track bounds on bitwise operations. A local attacker could use this to cause a denial of service or execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4948-1

Ubuntu Security Notice 4948-1 - Ryota Shiga discovered that the eBPF implementation in the Linux kernel did not properly verify that a BPF program only reserved as much memory for a ring buffer as was allocated. A local attacker could use this to cause a denial of service or execute arbitrary code. Manfred Paul discovered that the eBPF implementation in the Linux kernel did not properly track bounds on bitwise operations. A local attacker could use this to cause a denial of service or execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4950-1

Ubuntu Security Notice 4950-1 - Ryota Shiga discovered that the eBPF implementation in the Linux kernel did not properly verify that a BPF program only reserved as much memory for a ring buffer as was allocated. A local attacker could use this to cause a denial of service or execute arbitrary code. Manfred Paul discovered that the eBPF implementation in the Linux kernel did not properly track bounds on bitwise operations. A local attacker could use this to cause a denial of service or execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-1544-01

Red Hat Security Advisory 2021-1544-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation.

Red Hat Security Advisory 2021-1540-01

Red Hat Security Advisory 2021-1540-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-1538-01

Red Hat Security Advisory 2021-1538-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-4947-1

Ubuntu Security Notice 4947-1 - Kiyin discovered that the x25 implementation in the Linux kernel contained overflows when handling addresses from user space. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the fastrpc driver in the Linux kernel did not prevent user space applications from sending kernel RPC messages. A local attacker could possibly use this to gain elevated privileges. Various other issues were also addressed.

Ubuntu Security Notice USN-4946-1

Ubuntu Security Notice 4946-1 - It was discovered that the DRM subsystem in the Linux kernel contained double-free vulnerabilities. A privileged attacker could possibly use this to cause a denial of service or possibly execute arbitrary code. Olivier Benjamin, Norbert Manthey, Martin Mazein, and Jan H. Schoenherr discovered that the Xen paravirtualization backend in the Linux kernel did not properly propagate errors to frontend drivers in some situations. An attacker in a guest VM could possibly use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4945-1

Ubuntu Security Notice 4945-1 - It was discovered that the Nouveau GPU driver in the Linux kernel did not properly handle error conditions in some situations. A local attacker could use this to cause a denial of service. Jan Beulich discovered that the Xen netback backend in the Linux kernel did not properly handle certain error conditions under paravirtualization. An attacker in a guest VM could possibly use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4944-1

Ubuntu Security Notice 4944-1 - This update fixed multiple vulnerabilities in MariaDB. Ubuntu 18.04 LTS has been updated to MariaDB 10.1.48. Ubuntu 20.04 LTS has been updated to MariaDB 10.3.29. Ubuntu 20.10 has been updated to MariaDB 10.3.29. Ubuntu 21.04 has been updated to MariaDB 10.5.10.

MikroTik RouterOS Memory Corruption

MikroTik's RouterOS suffers from multiple memory corruption vulnerabilities. Various versions are affected.

Red Hat Security Advisory 2021-1532-01

Red Hat Security Advisory 2021-1532-01 - 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 buffer overflow and out of bounds read vulnerabilities.

Red Hat Security Advisory 2021-1531-01

Red Hat Security Advisory 2021-1531-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, out of bounds read, and out of bounds write vulnerabilities.

Ubuntu Security Notice USN-4943-1

Ubuntu Security Notice 4943-1 - Zhihong Tian and Hui Lu found that XStream was vulnerable to remote code execution. A remote attacker could run arbitrary shell commands by manipulating the processed input stream. This issue affected only affected Ubuntu 20.10. It was discovered that XStream was vulnerable to server-side forgery attacks. A remote attacker could request data from internal resources that are not publicly available only by manipulating the processed input stream. This issue only affected Ubuntu 20.10. Various other issues were also addressed.

Ubuntu Security Notice USN-4942-1

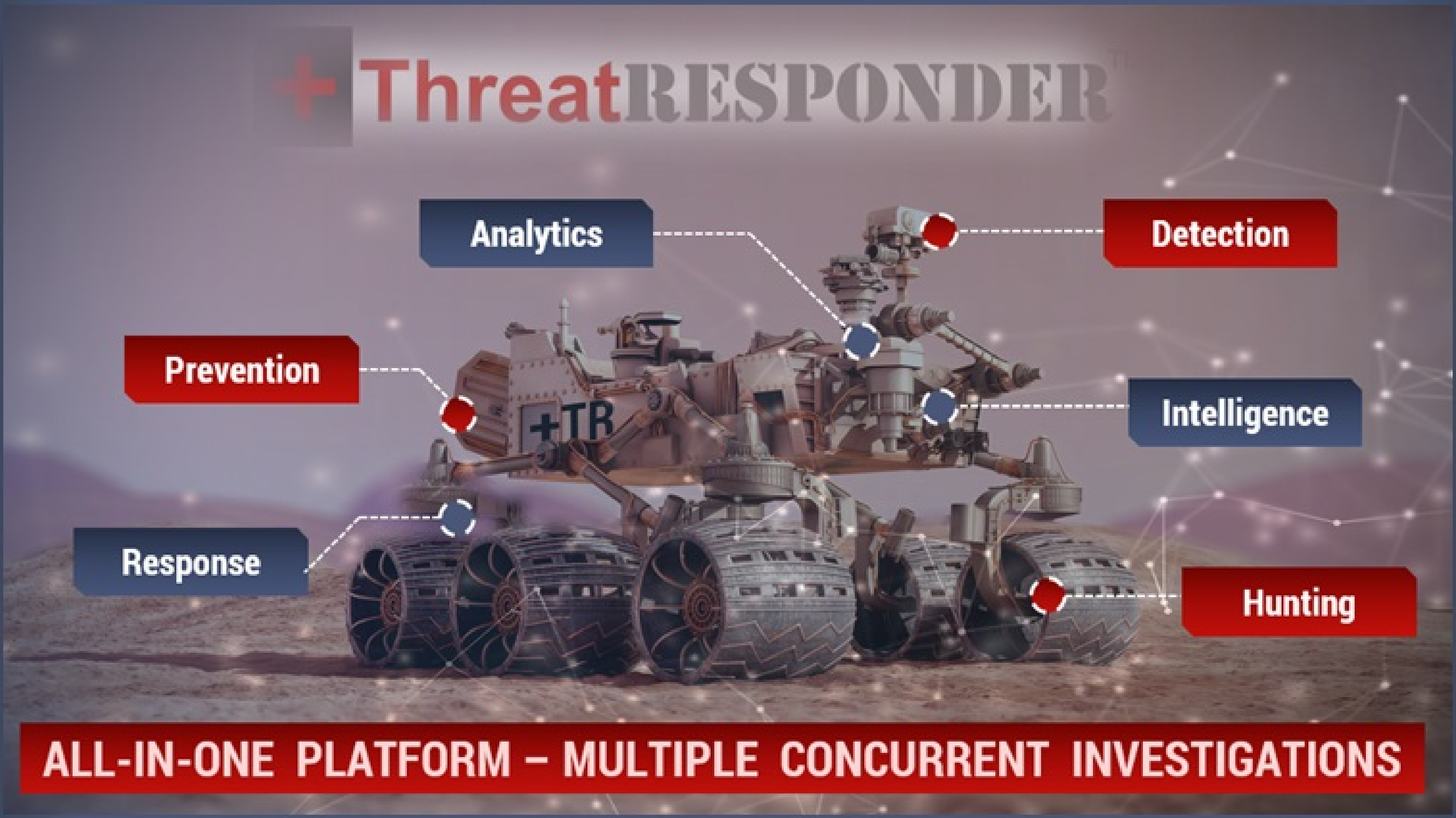
Ubuntu Security Notice 4942-1 - A race condition was discovered in Web Render Components. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit this to execute arbitrary code.

Ubuntu Security Notice USN-4941-1

Ubuntu Security Notice 4941-1 - It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to cause a denial of service. It was discovered that Exiv2 incorrectly handled certain images. An attacker could possibly use this issue to execute arbitrary code or cause a crash. Various other issues were also addressed.

Ubuntu Security Notice USN-4940-1

Ubuntu Security Notice 4940-1 - It was discovered that PyYAML incorrectly handled untrusted YAML files with the FullLoader loader. A remote attacker could possibly use this issue to execute arbitrary code.



ThreatRESPONDER
Analytics
Detection
Prevention
+TR
Intelligence
Response
Hunting
ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

Sponsored Products

CSI Linux: Current Version: 2021.1

Download here.

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

CSI Linux 2021.1 has been rebuilt from the ground up on Ubuntu 20.04 LTS to provide long term support for the backend OS and has become a powerful Investigation environment that comes in both the traditional Virtual Machine option and a bootable image that you can install onto an external drive or USB to use as your daily driver or DFIR triage drive. The SIEM has been given an evolution boost with capability while being encapsulated into a Docker container

CSI Linux 2021.2 BETA Release:

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

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

CSI Linux Tutorials for 2021.1:

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

Cyber Secrets

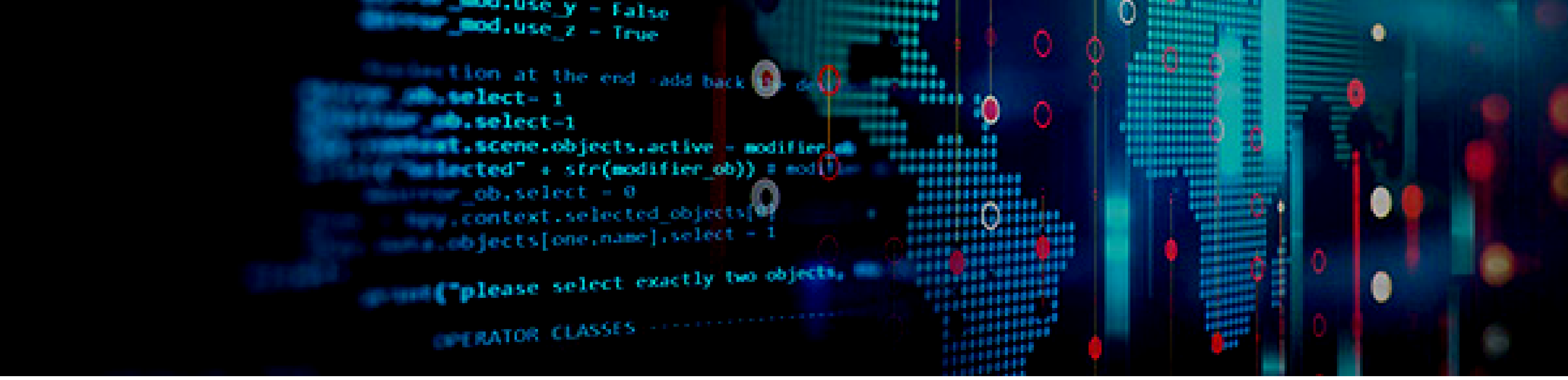
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

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

Printed / Kindle Publications:

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



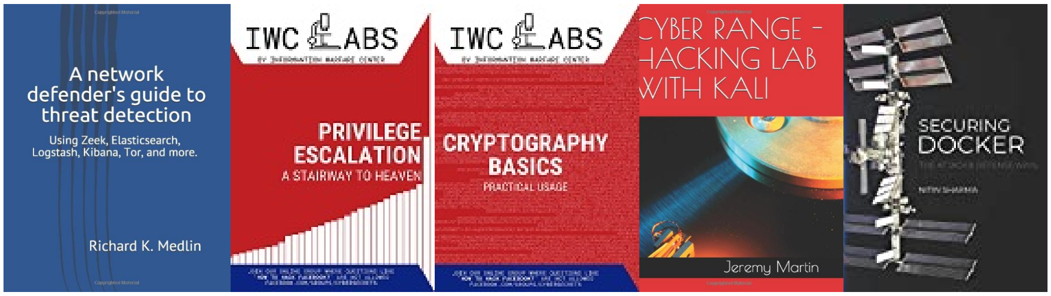
The Cyber Secrets publications on Amazon

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

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

CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
CYBER SECRETS
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
SOCRANGE
LINUX
CYBER SECRETS
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
CYBER SECRETS
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
CYBER SECRETS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

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