Dec-20-21

CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

December 20, 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

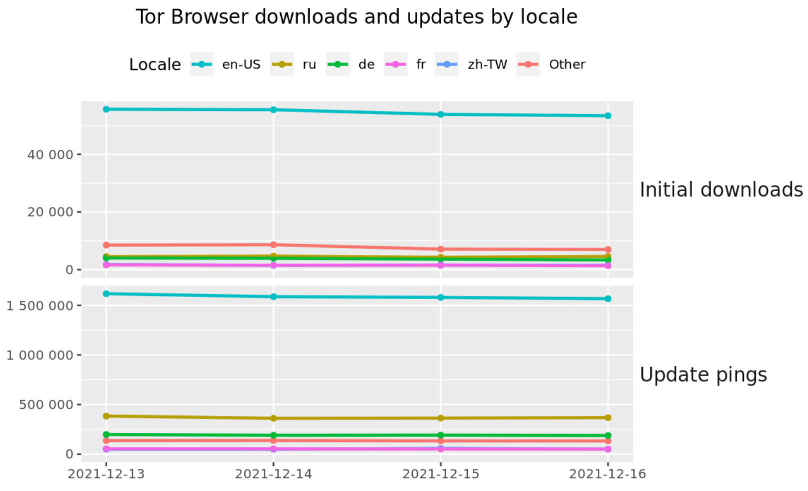
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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.



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

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

Index of Sections

Current News

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

The Hacker Corner:

* Security Conferences
* Google Zero Day Project

Cyber Range Content

* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques

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

InfoSec Media for the Week

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

Exploits and Proof of Concepts

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

Cyber Crime & Malware Files/Links Latest Identified

* CyberCrime-Tracker

Advisories

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

Information Warfare Center Products

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

LATEST NEWS

Packet Storm Security

* Sainbury's Payroll Hit By Kronos Attack
* DHS Moves To Make Bug Bounties A Permanent Fixture
* Facebook Exposes Mercenary Spy Firms That Targeted 50,000 People
* Backdoor Gives Hackers Complete Control Over Federal Agency Network
* Documents Link Huawei To Uyghur Surveillance Projects
* Log4shell: US Demands Christmas Eve Deadline For Hack Fix
* DarkWatchman RAT Shows Evolution In Fileless Malware
* Russia Proposes Holding Security Talks With EU-TASS
* Oregon Medical Group Notifies 750,000 Patients Of Data Breach
* Grindr Fine Cut To $7 Million In Norway Data Privacy Case
* MS Warns State Based Hackers Are Using Log4j Flaw
* New PS4 Exploit Points To Similar PS5 Hacks To Come
* Apple iOS Update Fixes Cringey iPhone 13 Jailbreak Exploit
* Actively Attacked Microsoft Zero Day Allows App Spoofing
* Apache Takes Off, Nukes Insecure Feature At The Heart Of Log4j From Orbit With 2.16
* Brazilian Ministry Of Health Hit By Second Attack In Same Week
* The Latest On The Log4j Remote Code Execution Nightmare
* Seedworm Attackers Target Telcos In Asia, Middle East
* Hackers Steal $140 Million From Users Of Crypto Gaming Company
* Polish Regulator To Investigate Apple's Privacy Policy
* Are Your Home Security Cameras Vulnerable To Hacking?
* Indian PM Modi's Twitter Hacked With Bitcoin Tweet
* Log4j Zero Day Flaw: What You Need To Know And How To Protect Yourself
* Julian Assange Can Be Extradited To US, Court Rules
* 300,000 MikroTik Routers Are Security Ticking Timebombs, Say Researchers

Krebs on Security

* NY Man Pleads Guilty in $20 Million SIM Swap Theft
* Microsoft Patch Tuesday, December 2021 Edition
* Inside Ireland's Public Healthcare Ransomware Scare
* Canada Charges Its "Most Prolific Cybercriminal"
* Who Is the Network Access Broker 'Babam'?
* Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach"
* The Internet is Held Together With Spit & Baling Wire
* Arrest in 'Ransom Your Employer' Email Scheme
* The 'Zelle Fraud' Scam: How it Works, How to Fight Back
* Tech CEO Pleads to Wire Fraud in IP Address Scheme

LATEST NEWS

Dark Reading

* How Risky Is the Log4J Vulnerability?
* Meta Acts Against 7 Entities Found Spying on 50,000 Users
* Executive Partnerships Are Critical for Cybersecurity Success
* Timely Questions for Log4j Response Now - And for the Future
* PseudoManuscrypt Malware Targeted Government & ICS Systems in 2021
* Time to Reset the Idea of Zero Trust
* CISA Issues Emergency Directive on Log4j
* Is Data Security Worthless if the Data Life Cycle Lacks Clarity?
* Mobile App Developers Keep Fraudulent Traffic at Bay with Anti-Fraud API
* Why Log4j Mitigation Is Fraught With Challenges
* Phorpiex Botnet Variant Spread Across 96 Countries
* Log4Shell: The Big Picture
* Dear Congress: It's Complicated. Please Consider This When Crafting New Cybersecurity Legislation
* Rise in API-Based Attacks Underscore Investments in New Tools
* Original Fix for Log4j Flaw Fails to Fully Protect Against DoS Attacks, Data Theft
* Companies Must Assess Threats to AI & ML Systems in 2022: Microsoft
* Dept. of Homeland Security Launches 'Hack DHS' Program
* Analysis: Log4j Vulnerability Highlights the Value of Defense-in-Depth, Accurate Inventory
* Meta Expands Bug-Bounty Program to Include Data Scraping
* Cybereason Announces Availability of AI-Driven Cybereason XDR and EDR on Google Cloud Marketplace

The Hacker News

* Over 500,000 Android Users Downloaded a New Joker Malware App from Play Store
* New Local Attack Vector Expands the Attack Surface of Log4j Vulnerability
* Apache Issues 3rd Patch to Fix New High-Severity Log4j Vulnerability
* Facebook Bans 7 'Cyber Mercenary' Companies for Spying on 50,000 Users
* New PseudoManuscrypt Malware Infected Over 35,000 Computers in 2021
* How to Prevent Customer Support Help Desk Fraud Using VPN and Other Tools
* New Phorpiex Botnet Variant Steals Half a Million Dollars in Cryptocurrency
* Researchers Uncover New Coexistence Attacks On Wi-Fi and Bluetooth Chips
* The Guide to Automating Security Training for Lean Security Teams
* New Fileless Malware Uses Windows Registry as Storage to Evade Detection
* Hackers Begin Exploiting Second Log4j Vulnerability as a Third Flaw Emerges
* Facebook to Pay Hackers for Reporting Data Scraping Bugs and Scraped Datasets
* Cynet's MDR Offers Organizations Continuous Security Oversight
* Hackers Using Malicious IIS Server Module to Steal Microsoft Exchange Credentials
* Microsoft Issues Windows Update to Patch 0-Day Used to Spread Emotet Malware

LATEST NEWS

Security Week

* Ransomware Persists Even as High-Profile Attacks Have Slowed
* Chinese Hackers Spotted Targeting Transportation Sector
* Citizen Lab Exposes Cytrox as Vendor Behind 'Predator' iPhone Spyware
* Russian Cyberspy Groups Start Exploiting Log4Shell Vulnerability
* Phorpiex Botnet Hijacked 3,000 Cryptocurrency Transactions
* VMware Patches Critical Flaw in Workspace ONE UEM Console
* Virginia Museum Shuts Down Website Amid IT Breach
* MobileIron Users Targeted in Log4Shell Attacks as Exploit Activity Surges
* Sophisticated Noberus Ransomware First to Be Coded in Rust
* Spyware Find Highlights Depth of Hacker-for-Hire Industry
* Meta Targets 'Cyber Mercenaries' Using Facebook to Spy
* Google Says NSO Pegasus Zero-Click 'Most Technically Sophisticated Exploit Ever Seen'
* Corellium Lands $25 Million Investment for Virtualization Tech
* Thousands of Industrial Systems Targeted With New 'PseudoManuscrypt' Spyware
* Upskilling Cyber Defenders Requires a Readiness Environment
* Iran-Linked APT Abuses Slack in Attacks on Asian Airline
* SecurityWeek Announces Virtual Cybersecurity Event Schedule for 2022
* CISA Calls for Improved Critical Infrastructure Security
* North American Propane Distributor 'Superior Plus' Discloses Ransomware Attack
* Threat Groups Reportedly Working on Log4Shell Worm
* Iran-Linked Hackers Attack Israeli Targets: Company
* Noname Security Raises $135 Million at 'Unicorn' Valuation
* Microsoft Spots Multiple Nation-State APTs Exploiting Log4j Flaw
* Investors Bet Big on Cloud Security Startups Ermetic, Dazz
* US, Australia Agree to Share Phone, Text Records in Criminal Probes

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* [EYE OPENER] New EU Phishing Study Shows That Crowd-sourcing Phishing Defense Is Successful
* $148 Million Lost to Gift Card Scams in 2021 (So Far)
* NSA: Cyberattacks are Putting the "Security of our Nation" at Stake
* The Evolving State of Cyber Insurance May Indicate More Scrutiny for IT and Security Teams
* Over 1000 Arrests and $27 Million Intercepted in Massive INTERPOL Sting Operation
* Netflix is the Latest Impersonated Brand in Ongoing Subscriber Targeting Scams
* Wall Street Journal article: "Shaming Employees For Phishing is Counterproductive"
* Log4j vulnerability - KnowBe4 Not Affected
* Answer 4 Simple Questions To Avoid a Social Engineering Attack
* CyberheistNews Vol 11 #49 [HEADS UP] Tricky New TSA PreCheck Scam Steals Your Personal and Credit Car

ISC2.org Blog

* The Other Type of Shadow IT
* The Cybersecurity Role as a Business Partner
* Cloud Security Complements Data Privacy
* Top Books to Prepare You for CISSP Exam
* CCSP vs. Microsoft Azure Certified Security Engineer Associate - How Does Vendor Focus Factor In?

HackRead

* Everything You Need to Know About Amazon Fire TV Stick
* Grim Finance hacked - $30 million worth of tokens stolen
* German audio tech giant Sennheiser exposed 55GB of customers' data
* Conti Ransomware Group Exploiting Log4j Vulnerability
* Spider-Man: No Way Home exploited to push phishing and malware scams
* Gumtree exposed users' personal and GPS location via source code
* Anubis malware resurfaces targeting crypto wallets and banking apps

Koddos

* Everything You Need to Know About Amazon Fire TV Stick
* Grim Finance hacked - $30 million worth of tokens stolen
* German audio tech giant Sennheiser exposed 55GB of customers' data
* Conti Ransomware Group Exploiting Log4j Vulnerability
* Spider-Man: No Way Home exploited to push phishing and malware scams
* Gumtree exposed users' personal and GPS location via source code
* Anubis malware resurfaces targeting crypto wallets and banking apps

LATEST NEWS

Naked Security

* Serious Security: OpenSSL fixes "error conflation" bugs - how mixing up mistakes can lead to trouble
* S3 Ep63: Log4Shell (what else?) and Apple kernel bugs [Podcast+Transcript]
* Apple security updates are out - and not a Log4Shell mention in sight
* Log4Shell explained - how it works, why you need to know, and how to fix it
* "Log4Shell" Java vulnerability - how to safeguard your servers
* S3 Ep62: The S in IoT stands for security (and much more) [Podcast+Transcript]
* Firefox update brings a whole new sort of security sandbox
* Cryptocurrency startup fails to subtract before adding, loses $31m
* Mozilla patches critical "BigSig" cryptographic bug: Here's how to track it down and fix it
* S3 Ep61: Call scammers, cloud insecurity, and facial recognition creepiness [Podcast+Transcript]

Threat Post

* Facebook Bans Spy-for-Hire Firms for Targeting 50K People
* Spider-Man Movie Release Frenzy Bites Fans with Credit-Card Harvesting
* Malicious Joker App Scores Half-Million Downloads on Google Play
* Brand-New Log4Shell Attack Vector Threatens Local Hosts
* Convergence Ahoy: Get Ready for Cloud-Based Ransomware
* Conti Gang Suspected of Ransomware Attack on McMenamins
* 'Tropic Trooper' Reemerges to Target Transportation Outfits
* 'PseudoManuscrypt' Mass Spyware Campaign Targets 35K Systems
* 'DarkWatchman' RAT Shows Evolution in Fileless Malware
* Relentless Log4j Attacks Include State Actors, Possible Worm

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

* Log4Shell Vulnerability Risks for OT Environments - and How You Can Better Protect Against Them
* Why We Need To Beat 'Breach Fatigue' - At Work and at Home
* It's Not Too Soon to Start Talking About 6G
* Zero Trust and DNS Security: Better Together
* Starting From Scratch: How to Build a Small Business Cybersecurity Program
* Nation State Threat Group Targets Airline with Aclip Backdoor
* A Journey in Organizational Resilience: Geopolitical and Socio-Economic Trends and Threats
* One-Time Password Security Might Fail 80% of the Time. IAM is Better
* How Log4j Vulnerability Could Impact You
* How to Include Cybersecurity Training in Employee Onboarding

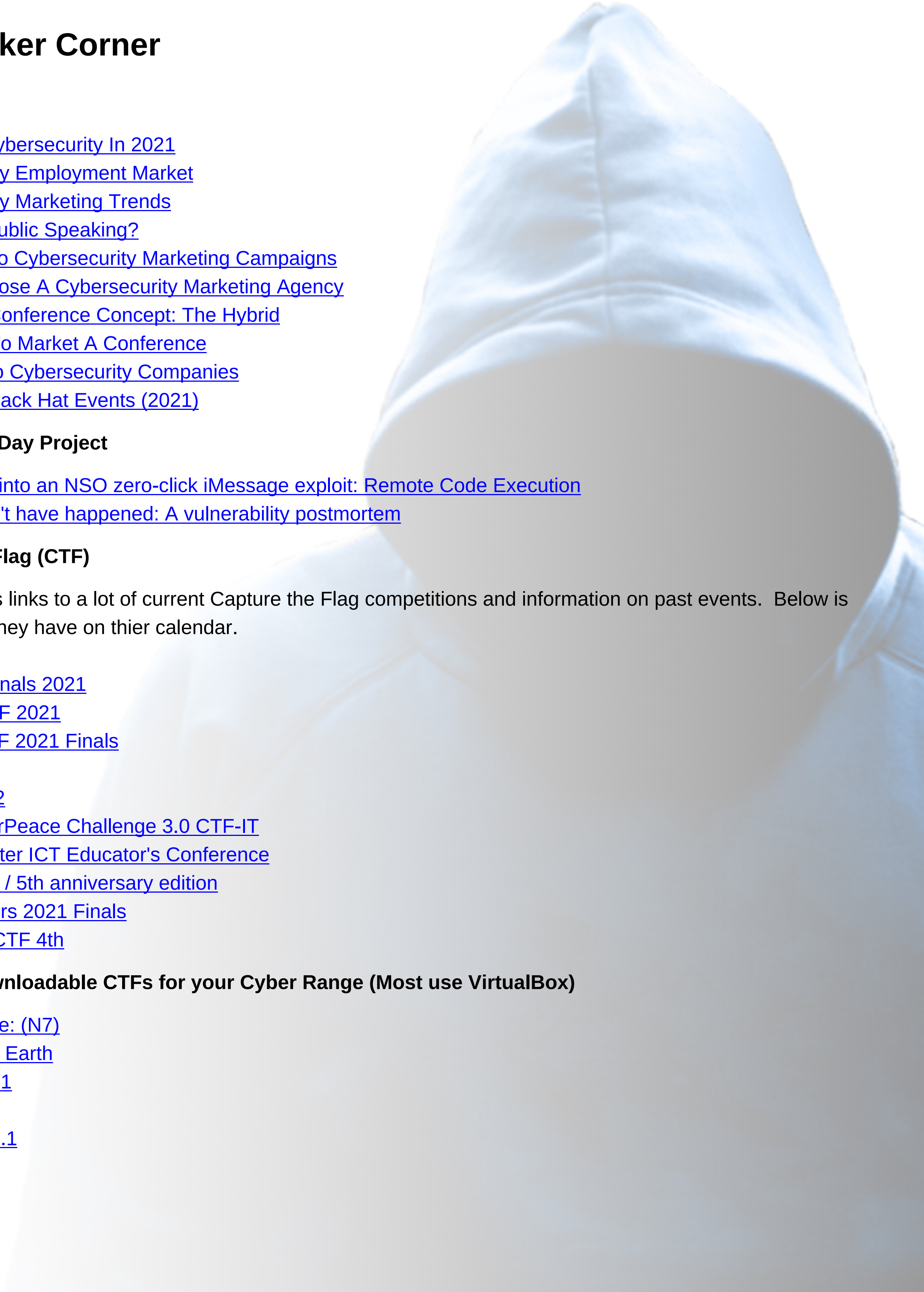
InfoWorld

* Microsoft reveals plans for Entity Framework 7.0
* 2 cloud computing predictions you won't hear anywhere else
* Ruby on Rails 7 rejiggers JavaScript support
* How developers scrambled to secure the Log4j vulnerability
* How to use the minimal hosting model in ASP.NET Core 6
* The future of the operational data warehouse
* Hands-on with the Marko JavaScript framework
* Go language adds generics
* Azul brings Java compilation to the cloud
* Securing the Kubernetes software supply chain

C4ISRNET - Media for the Intelligence Age Military

* US Space Force awards $67M deal to Raytheon to test prototype weather satellite
* Orbital Insight to build AI for intelligence community based on artificial data
* Russia unveils upgraded S-70 Hunter drone, with plans for fielding in 2024
* US Air Force cyber team demonstrates first ever in-flight mission
* Public-private team in Turkey unveils drone with laser gun
* US Army assigns data, tactical cloud experiments to multidomain task forces
* NATO looking at holistic path to boost cyber defense arsenal
* The Navy is testing this adorable sailboat drone
* US Army officials: Service needs 'true data fabric'
* Officials say US Army armored brigades need a stronger network

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

* A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution
* This shouldn't have happened: A vulnerability postmortem

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.

* ASIS CTF Finals 2021
* BackdoorCTF 2021
* ISITDTU CTF 2021 Finals
* SCTF 2021
* TetCTF 2022
* Global CyberPeace Challenge 3.0 CTF-IT
* WASTC Winter ICT Educator's Conference
* #kksctf open / 5th anniversary edition
* BSides Algiers 2021 Finals
* Real World CTF 4th

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

* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1
* Napping: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

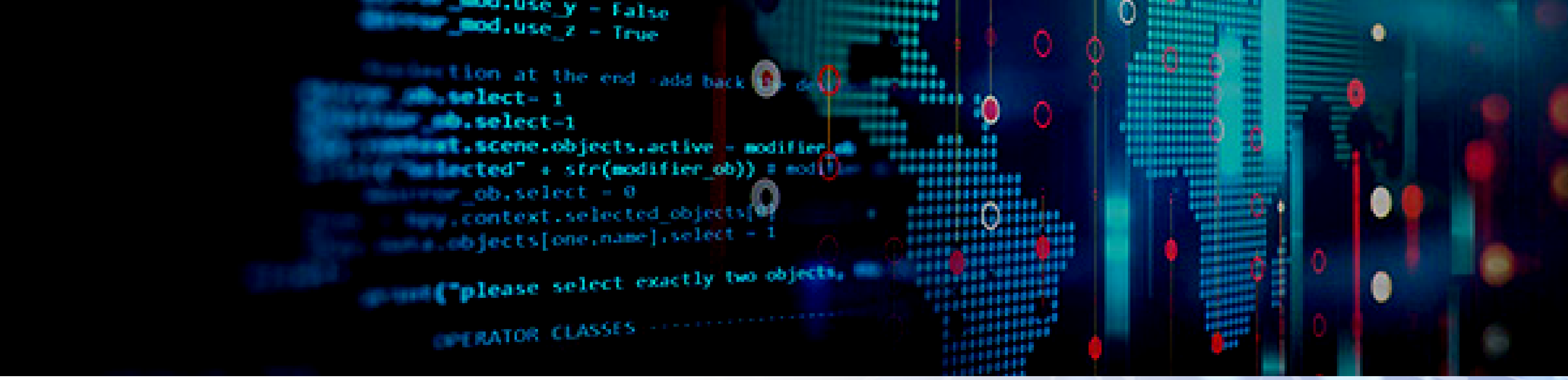
* TOR Virtual Network Tunneling Tool 0.4.6.9
* Google OSS Fuzz
* Log4j Recognizer
* OpenSSL Toolkit 1.1.1m
* Zed Attack Proxy 2.11.1 Cross Platform Package
* nfstream 6.4.0
* ETS5 Password Recovery Tool
* I2P 1.6.1
* Wapiti Web Application Vulnerability Scanner 3.0.8
* Stegano 0.10.1

Kali Linux Tutorials

* RottenPotatoNG : A C++ DLL And Standalone C++ Binary - No Need For Meterpreter Or Other Tools
* Private Set Membership (PSM) : Cryptographic Protocol That Allows Clients To Privately Query
* Ddosify : High-performance Load Testing Tool
* Koppeling : Adaptive DLL Hijacking / Dynamic Export Forwarding
* What You Need To Know About the World's First Cybersecurity Experience (CSX) Platform: Perimeter 81
* The Ultimate Guide to Web Testing: Types and Key Areas
* FakeDataGen : Full Valid Fake Data Generator
* The Definitive Guide to Web Security Testing: Vulnerabilities and Password Management
* ELFXtract : An Automated Analysis Tool Used For Enumerating ELF Binaries
* Nanobrok : Web Service For Control And Protect Your Android Device Remotely

GBHackers Analysis

* Lenovo Laptop Flaws Let Attackers Gain Admin Privileges
* Oxeye Identifies Vulnerabilities Cloud Native Applications with CNAST Platform
* Printing Shellz - New Vulnerabilities That Affects 150 Different Multifunction Printers
* North Korean Hackers Group Posed as Samsung Recruiters To Target Security Firms
* Two Iranian Hackers Charged For Gaining Access to Confidential Voter Information



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS STAR Live Stream
* Join us for the FREE Virtual Cyber Threat Intelligence Summit 2022!
* Wrap Up Panel
* Open Threat Research - The Hunt for Red Apples: How to threat hunt and emulate Ocean Lotus on macOS

Defcon Conference

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

Hak5

* How Hackers Exploit Log4J to Get a Reverse Shell (Ghidra Log4Shell Demo) | HakByte
* Log4Shell & Log4j Explained - ThreatWire
* Keep Computers From Locking with a CircuitPython Mouse Jiggler | HakByte

The PC Security Channel [TPSC]

* Antivirus Tierlist: Best Antivirus in 2021
* Phobos Ransomware

Eli the Computer Guy

* SHURE MV7 USB C - OLD MAN SCREAMING AT CLOUDS
* Asshole or Grape? - I might need a pop filter...
* OMICRON SURGES in NEW YORK CITY
* FRANCE SHUTS BORDER WITH UK over OMICRON COVID

Security Now

* Log4j & Log4Shell - Apple AirTag Abuse, Amazon Outage and Cloud Dependence, New WordPress Threats
* XSinator - NSS Has a Bug, Botnet on the Blockchain, HP's Vulnerable Printers, Microsoft Edge Relief

Troy Hunt

* Weekly Update 274

Intel Techniques: The Privacy, Security, & OSINT Show

* 244-2021 Show Review & Updates
* 243-Emergency Bags

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Android VM_MAYWRITE Access To Shared Zygote JIT Mapping
* Backdoor.Win32.Mellpon.b Information Disclosure
* Backdoor.Win32.BNLite Buffer Overflow
* Chrome NavigationPreloadRequest Site Isolation Bypass
* Chrome ThreadedIconLoader::DecodeAndResizeImageOnBackgroundThread Heap Use-After-Free
* Chrome blink::NativeIOFile::DoRead Heap Use-After-Free
* Cibele Thinfinity VirtualUI 2.5.41.0 User Enumeration
* Croogo 3.0.2 Shell Upload
* Croogo 3.0.2 Cross Site Scripting
* Arunna 1.0.0 Cross Site Request Forgery
* Child's Day Care Management System 1.0 SQL Injection
* log4j-scan Extensive Scanner
* Log4j Remote Code Execution Word Bypassing
* L4sh Log4j Remote Code Execution
* SAP Netweaver IUUC_GENERATE_ACPLAN_DELIMITER ABAP Code Injection
* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG ABAP Code Injection
* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG SQL Injection
* OpenEMR 6.0.0 / 6.1.0-dev SQL Injection
* Simple Cold Storage Management System 1.0 SQL Injection
* Oliver Library Server 5 Arbitrary File Download
* Log4j Payload Generator
* Log4j2 Log4Shell Regexes
* Sofico Miles RIA 2020.2 Build 127964T Cross Site Scripting
* Laravel Valet 2.0.3 Privilege Escalation
* WordPress Typebot 1.4.3 Cross Site Scripting

CXSecurity

* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG ABAP Code Injection
* SAP Netweaver IUUC_GENERATE_ACPLAN_DELIMITER ABAP Code Injection
* SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG SQL Injection
* Apache Log4j2 2.14.1 Information Disclosure
* GNU gdbserver 9.2 Remote Command Execution
* Booked Scheduler 2.7.5 Remote Command Execution (RCE) (Authenticated)
* WebHMI 4.0 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

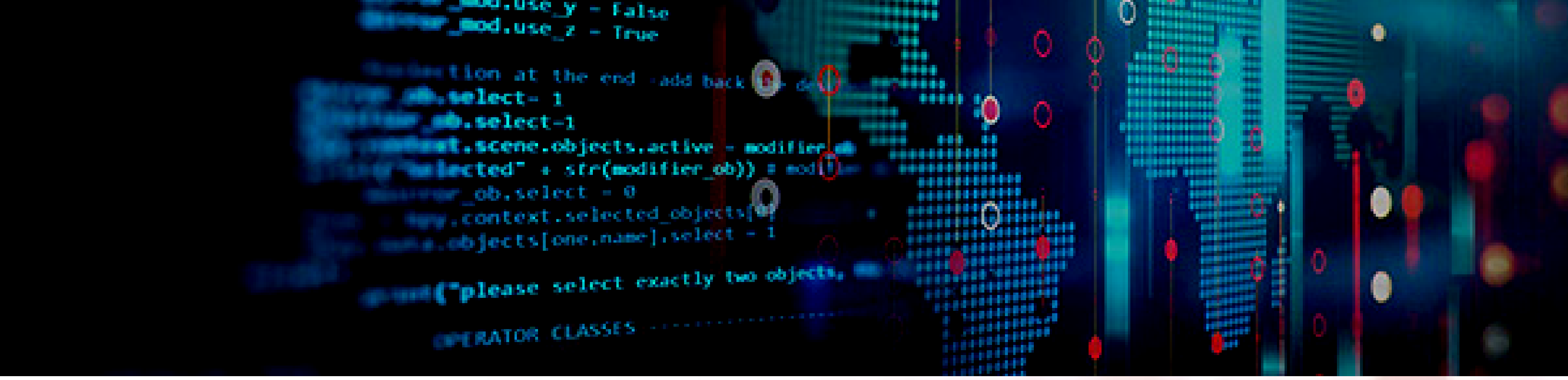
* [webapps] Arunna 1.0.0 - 'Multiple' Cross-Site Request Forgery (CSRF)
* [webapps] Croogo 3.0.2 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Croogo 3.0.2 - Unrestricted File Upload
* [webapps] Cibele Thinfinity VirtualUI 2.5.41.0 - User Enumeration
* [remote] Oliver Library Server v5 - Arbitrary File Download
* [local] Microsoft Internet Explorer / ActiveX Control - Security Bypass
* [webapps] Online Thesis Archiving System 1.0 - SQLi Authentication Bypass
* [webapps] meterN v1.2.3 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Zucchetti Axess CLOKI Access Control 1.64 - Cross Site Request Forgery (CSRF)
* [webapps] Booked Scheduler 2.7.5 - Remote Command Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin Typebot 1.4.3 - Stored Cross Site Scripting (XSS) (Authenticated)
* [remote] Apache Log4j 2 - Remote Code Execution (RCE)
* [local] Laravel Valet 2.0.3 - Local Privilege Escalation (macOS)
* [remote] Apache Log4j2 2.14.1 - Information Disclosure
* [webapps] WebHMI 4.0 - Remote Code Execution (RCE) (Authenticated)
* [remote] HD-Network Real-time Monitoring System 2.0 - Local File Inclusion (LFI)
* [webapps] Free School Management Software 1.0 - Remote Code Execution (RCE)
* [webapps] Free School Management Software 1.0 - 'multiple' Stored Cross-Site Scripting (XSS)
* [webapps] OpenCATS 0.9.4 - Remote Code Execution (RCE)
* [webapps] Employees Daily Task Management System 1.0 - 'multiple' Cross Site Scripting (XSS)
* [webapps] Employees Daily Task Management System 1.0 - 'username' SQLi Authentication Bypass
* [webapps] Grafana 8.3.0 - Directory Traversal and Arbitrary File Read
* [webapps] Wordpress Plugin Catch Themes Demo Import 1.6.1 - Remote Code Execution (RCE) (Authenticate
* [webapps] Student Management System 1.0 - SQLi Authentication Bypass
* [webapps] TestLink 1.19 - Arbitrary File Download (Unauthenticated)

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

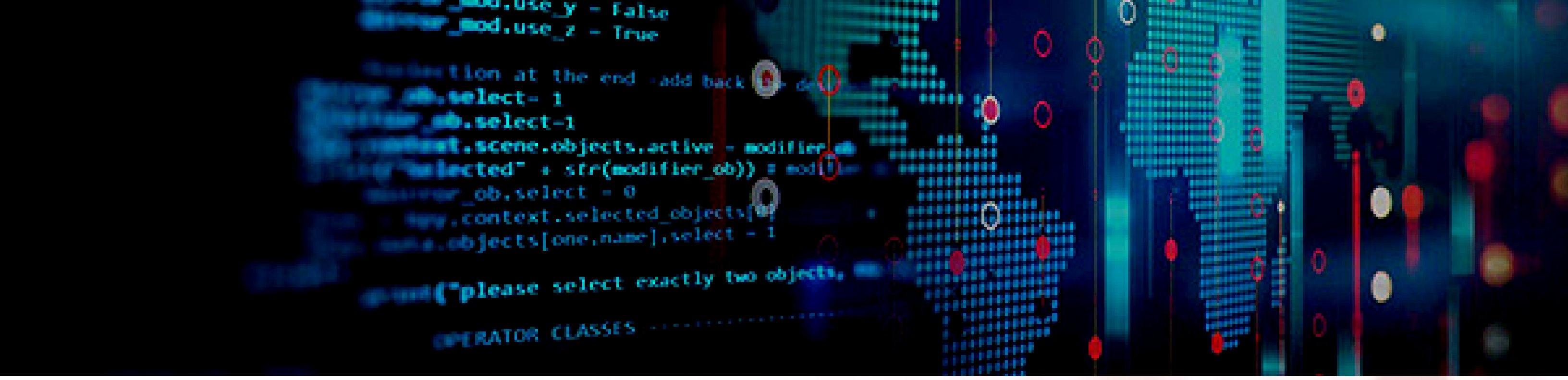
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://dpmptsp.inhilkab.go.id
https://dpmptsp.inhilkab.go.id notified by We Are BRITISH EMPIRE (Turkey, Indonesia, Kurdistan, etc)
https://hospitalpepillosalcedo.gob.do
https://hospitalpepillosalcedo.gob.do notified by We Are BRITISH EMPIRE (United States of America, Brazil, Colombi
http://banten.bkkbn.go.id/b4.html
http://banten.bkkbn.go.id/b4.html notified by 0x1998
http://sumut.bkkbn.go.id/b4.html
http://sumut.bkkbn.go.id/b4.html notified by 0x1998
https://capivari.sp.gov.br
https://capivari.sp.gov.br notified by Paran&aacute; Cyber Mafia
https://gg.gov.kn/wh.html
https://gg.gov.kn/wh.html notified by Mr.Kro0oz.305
https://diaspora.gov.kn/wh.html
https://diaspora.gov.kn/wh.html notified by Mr.Kro0oz.305
http://kaziuwekezajismz.go.tz/krd.html
http://kaziuwekezajismz.go.tz/krd.html notified by 0x1998
http://pusbindiklatren.bappenas.go.id/readme.html
http://pusbindiklatren.bappenas.go.id/readme.html notified by UnknownSec
https://prodeuteq.gob.ec/Anon403.html
https://prodeuteq.gob.ec/Anon403.html notified by ifactoryx
https://setdprd.bantenprov.go.id/indo.html
https://setdprd.bantenprov.go.id/indo.html notified by ONE HAT CYBER TEAM
http://aceh.lan.go.id
http://aceh.lan.go.id notified by 1877
http://ppid.lan.go.id
http://ppid.lan.go.id notified by 1877
https://www.perpustakaan.pa-bengkayang.go.id/santa.html
https://www.perpustakaan.pa-bengkayang.go.id/santa.html notified by Foursdeath Team
http://pa-bengkayang.go.id/santa.html
http://pa-bengkayang.go.id/santa.html notified by Foursdeath Team
https://cts2.pn-buntok.go.id/sec.txt
https://cts2.pn-buntok.go.id/sec.txt notified by I Love BRITISH EMPIRE
http://arsipperkara.pn-buntok.go.id/70.txt
http://arsipperkara.pn-buntok.go.id/70.txt notified by I Love BRITISH EMPIRE



Dark Web News

Darknet Live

ToRReZ Market is Retiring

ToRReZ Market is retiring, according to an announcement from the market's administrators. In October 2021, White House Market announced their retirement after a successful run. Less than two months later, ToRReZ Market, which launched as the "first community-driven market,&rdquo; announced their retirement as well. Mr. Blonde, the ToRReZ administrator who signed the farewell message, hinted at the possibility of a return in the future. In the message, the administrator warned against using established marketplaces; they said that markets grow closer to collapse as they age. Traditionally, retiring markets have suggested users migrate to certain "friendly&rdquo; markets or equally well-established markets. Mr. White, the administrator of White House Market, encouraged users to migrate to Monopoly Market or Versus Market. He highlighted Monopoly Market's walletless system and Versus' enforced multi-sig. The message is available on the ToRReZ homepage. My demo account on the marketplace is "NickiMinaj&rdquo; Unrelated Warning About Market Shutdowns As with any market shutdown, there is a slim chance that law enforcement is controlling the entire narrative in a repeat of Operation Bayonet. Operation Bayonet, for newcomers, was a law enforcement operation in 2017 that thoroughly disrupted the darkweb market ecosystem. International law enforcement agencies collaborated to secretly take control of the second-largest marketplace at the time, Hansa Market. LEOs had taken control of the market's servers and had posed as the market's administrators for several weeks before the reveal. The banners used for Alphabay and Hansa Investigators made subtle changes to Hansa Market in an attempt to identify careless vendors and customers. Last I checked, these methods by themselves resulted in very few arrests. Per Wikipedia: All user passwords were recorded in plaintext (allowing police to log into other markets if users had re-used passwords). Vendors and buyers would communicate via PGP-encrypted messages. However, the website provided a PGP encryption convenience feature which the police modified to record a plaintext copy. The website's automatic photo metadata removal tool was modified to record metadata (such as geolocation) before being stripped off by the website. Police wiped the photo database, which enticed vendors to re-upload photos (now capturing metadata). Multisignature bitcoin transactions were sabotaged, which at shutdown would allow police to confiscate a larger amount of illicit funds. Police enticed users to download a Microsoft Excel file (disguised as a text file) that, when opened, would attempt to ping back to a police webserver and unmask the user's IP address. I have one of the .xlsx/.zip files somewhere provided by a former Hansa Market vendor. I will upload it for your viewing pleasure if I can find it. The onion service deployed by LE after the Hansa bust. Once law enforcement had set the stage at Hansa Market, other law enforcement agencies shut down AlphaBay Market, the largest marketplace at the time. They seized AlphaBay servers and arrested the alleged administrator, Alexandre Cazes in Thailand. While in a jail in Thailand, Cazes hanged himself rather than spend his life behind bars in a U.S. prison. As law enforcement had predicted, former users of AlphaBay flocked to the second-largest marketplace at the time: Hansa Market. Law enforcement had control of Hansa at this time and gathered as much information as they could. After several weeks had passed, law enforcement pulled the rug out from underneath Hansa users, replacing the marketplace with a seizure banner similar to the one used during the AlphaBay seizure. Law enforcement operations targetting marketplaces, at least as we understand them, have not involved such intricate and dramatic steps since the AlphaBay and Hansa seizures. Law enforcement in the Netherlands knocked on hundreds of doors of alleged customers who had neglected to encrypt their addresses when completing a purchase on Hansa Market. However, the infiltration of Hansa Market resulted in very few instances of vendor deanonymization. Why the warning is unrelated Although ToRReZ is undoubtedly a large market by today's standards, it is not the largest market nor is it the most well established. If law enforcement agencies were to attempt a repeat of Operation Bayonet, they would presumably seize the larger market first and push people to the smaller market second. ToRReZ, in their retirement message, explicitly encouraged users to move to a newer marketplace. All newer marketplaces are significantly smaller than the current well-established marketplaces. The ToRReZ announcement Below is the ToRReZ announcement. Dear Users. After 675 days of presence on the darknet, we have decided to close our door for good. Please read the following statement to understand the market's closure process. From 2021-12-17 certain functions of the market has been disabled: registering, upgrading to vendor account, purchasing, featured items auctions, support. Market wallets are working fine and are ready to get your withdrawals requests. Because we use fully automated system, please be ready for queues when it comes to the withdraw. We especially expect the queue on XMR withdrawals (because of how XMR is built). Market will be left online for at least two to three weeks until all orders are finalized and disputes are closed. We will review the disputes on the daily basis so you can withdraw your funds as quick as possible. Buyers and vendors - please work with us on your disputes. Please provide information about the package status. Do not be a dick to each other. We give you an opportunity to leave the market with your gear or funds so help us to achieve that. Vendors trying to use this opportunity to exit scam will be banned. We also share our vendor's data with Recon. If you forgot your mnemonic / pin / password / pgp - there is nothing we can do about it. If your deposit did not come - it is because you got phished and there is nothing we can do about it. If you paid for the order and it is not on the list - it is because you got phished and there is nothing we can do about it. It has been a great pleasure to work with most vendors and users. We are aware that we leave quite a big gap in darknet markets but we hope most of you will find a new home. While choosing a new market, please use your common sense. I would personally avoid any "established&rdquo; market as older they get, bigger chance of collapsing is. Please give a chance to the smaller markets, which are not that loud as others. This is exactly how we became no 1 - being quiet and doing our job, serving customers 24/7 for 675 fucking days. While ToRReZ will be gone for good, we might (or not) come back at some stage with something different. The whole world goes green. Maybe we will join the trend at some stage ;] When we decide to be back, we will definitely sign the message with one of the known keys so watch out for any copycats. If you have anything to say to me, you can use Dread's system but I give no warranty that any of your messages will be read, not to mention that they will not get answered. Thanks for supporting us. mrblonde ToRReZ Market Team --ToRReZ market news: yxuy5oau7nugw4kpb4lclrqdbixp3wvc4iuiad23ebyp2q3gx7rtrgqd.onion/news Signed Message -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA512 Dear Users. After 675 days of presence on the darknet, we have decided to close our door for good. Please read the following statement to understand the market's closure process. - From 2021-12-17 certain functions of the market has been disabled: registering, upgrading to vendor account, purchasing, featured items auctions, support. Market wallets are working fine and are ready to get your withdrawals requests. Because we use fully automated system, please be ready for queues when it comes to the withdraw. We especially expect the queue on XMR withdrawals (because of how XMR is built). Market will be left online for at least two to three weeks until all orders are finalized and disputes are closed. We will review the disputes on the daily basis so you can withdraw your funds as quick as possible. Buyers and vendors - please work with us on your disputes. Please provide information about the package status. Do not be a dick to each other. We give you an opportunity to leave the market with your gear or funds so help us to achieve that. Vendors trying to use this opportunity to exit scam will be banned. We also share our vendor's data with Recon. If you forgot your mnemonic / pin / password / pgp - there is nothing we can do about it. If your deposit did not come - it is because you got phished and there is nothing we can do about it. If you paid for the order and it is not on the list - it is because you got phished and there is nothing we can do about it. It has been a great pleasure to work with most vendors and users. We are aware that we leave quite a big gap in darknet markets but we hope most of you will find a new home. While choosing a new market, please use your common sense. I would personally avoid any "established" market as older they get, bigger chance of collapsing is. Please give a chance to the smaller markets, which are not that loud as others. This is exactly how we became no 1 - being quiet and doing our job, serving customers 24/7 for 675 fucking days. While ToRReZ will be gone for good, we might (or not) come back at some stage with something different. The whole world goes green. Maybe we will join the trend at some stage ;] When we decide to be back, we will definitely sign the message with one of the known keys so watch out for any copycats. If you have anything to say to me, you can use Dread's system but I give no warranty that any of your messages will be read, not to mention that they will not get answered. Thanks for supporting us. mrblonde ToRReZ Market Team

```
-----BEGIN PGP SIGNATURE-----
iQIzBAEBCgAdFiEE4DNkCTAjr9sqIxybuRj8IbVCmCgFAmG7TLwACgkQuRj8IbVC
mCgpkA/7B5epE8i9NyF4cdafbvBnxUkPGW1xqFIPI2xECLpvfAGbDsLBobG7ugj1
MqvwQHa2EO0YE8T2wleiVwcQuPKN0I2Gp3+tJ/ElkiV4haMSenKGu/hayw9k6wCH
vKw6yz6lIB99rfl0Mzf2hu0ILBFsetDCamHsTlkGPm0SzCdlzOI67V1qiY0I8C5B
5fVNtfZK1QRbS7YA+56PY6ZlCVrXJTgSU0IWczjP5+OzUiPOFKU77mMixT/uWlHs
gWbbgAPJigEjbYZ6kWOgHydyAZr3GdmCNkLmfBWU3IMeCUXSglaBtjMf3Rxl5/EH
kQ5Jqy9MyC1f7rZLDNrTt5uVP/5RTW/DsnU7VEsVs2Hjw3xXeu4VUTlyaVziQU/1
qCcGVDd9PbfC5NJtiVfwgSbxrkwF2ZCp3oO2whjroFFLz3qC7tKxWQJem9OIkLe7
DTfWJPjqMq9CsczKgk444kmAIoLlEG6LF8neDqoKXILo/WqwDl0r/V3YEe+HHvwx
mLHGJxz/G+iqP9xnNwVc1ja9EPcZ8gDT1czVJOzVv6SrjErzt/6NHATxNXiOTG9A
qJNzlSUBQ05xFZZZXtKdzAT4HPU8FjWgUMa9cTYZAdSxDHhFXJnumZVfJeFQ9Fhh
VsnCKm5q0+CsWXuBKIvKSWaeJvUMXO2I/wMrJbuwHFfwDgbvS/g= =zk/f -----END PGP SIGNATURE-----
```

The amazing thing is that currently, one of the "established&rdquo; markets for general criminal activity is Dark0de which was a new market taking loads of criticism not too lon ago. Eventually, we will inevitably be in the same situation with only the strange reboot of Alphabay remaining as an "established market.&rdquo; Filering out search engine results for specialty markets and ToRReZ, Monopoly, Versus, and Dark0de lead. ToRReZ is technically still higher than all three but that will soon drop. However, these metrics can hardly be considered reliable traffic metrics; no sensible darkweb user searches Google to find the address of a darkweb marketplace. The majority of users who make more than a single purchase presumably bookmark the market's address, this site, or Dark.Fail (or perhaps one of the many phishing clones of our sites). Additionally, just because someone searched Google for a site and visited Darknetlive as a result does not mean they stuck with the market they searched. I have no analytics available for traffic metrics. No tracking whatsoever. Nginx access logs are disabled. I realize this is no longer the right way to eliminate error logging. Regardless, it should not matter over Tor as I am unable to identify different users. With that said, I will upload something and an on-site PoC for fingerprinting users even with javascript off. Far from a novel concept but certainly something worth considering for those with less experience in this sector.

The DarkMarket Trial Started Today

The trial for the alleged administrators of DarkMarket began this week, nearly one year after German law enforcement shut down the market. The trial for the alleged creators of DarkMarket began on Thursday, December 16, at the Trier District Court. The duo, a 35-year-old man and a 33-year-old woman, are charged with aiding and abetting in the distribution of narcotics in almost 1,500 cases. _ The DarkMarket seizure banner was not as creative as previous banners. Both defendants are Australian nationals who crossed into Germany from Denmark as a part of a long trip through Europe. The case is being tried at the Trier District Court because one of the largest vendors on DarkMarket was from the region, according to prosecutors. According to public prosecutor Sebastian H&uuml;binger, the defendant's, through DarkMarket, facilitated more than 170,000 drug transactions. Europol: DarkMarket, the world's largest illegal marketplace on the dark web, has been taken offline in an international operation involving Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (the National Crime Agency), and the USA (DEA, FBI, and IRS). Europol supported the takedown with specialist operational analysis and coordinated the cross-border collaborative effort of the countries involved. DarkMarket in figures: almost 500 000 users; more than 2 400 sellers; over 320 000 transactions; more than 4 650 bitcoin and 12 800 monero transferred.   At the current rate, this corresponds to a sum of more than â‚¬140 million. The vendors on the marketplace mainly traded all kinds of drugs and sold counterfeit money, stolen or counterfeit credit card details, anonymous SIM cards and malware. _ There is certainly a creative twist, though. Europol: professional fly-swatters.   DarkMarket used CyberBunker as a hosting provider for the marketplace until law enforcement shut down the hosting provider. Multiple I.P. addresses associated with DarkMarket, including 185.35.137.66, leaked after German law enforcement had seized the CyberBunker infrastructure. However, the administrators quickly moved the market to servers located in Moldova and Ukraine. The seized CyberBunker servers were the basis of the investigation into the marketplace. This should be an interesting trial. We do not know much about the investigation yet. However, many online have indicated that the administrator of DarkMarket lacked the skills to safely run a criminal marketplace. They did very well for a market based on a freely-available marketplace script and had nearly monopolized the sector at the time of their arrest.

Eight Sentenced to Prison in CyberBunker Trial

A court in Germany sentenced eight defendants to prison for running the bulletproof hosting service Cyberbunkner. _ CyberBunker advertised servers located within a renovated NATO bunker.   The court heard how the hosting service catered to platforms that facilitated the illicit distribution of drugs, child pornography, and stolen information. [Dnl note: Although all eight cases ended in guilty verdicts, the prosecutors could not prove the defendants had aided any of the criminal sites hosted at CyberBunker. There was not any proof that CyberBunker employees were complicit in any specific crime related to the content hosted on CyberBunker infrastructure. This, as the public prosecutor said, is "new legal ground."] _ Indeed.   Nevertheless, all defendants were convicted of being members of a criminal organization. The defendants operated the web-hosting service from a former NATO bunker in Rhineland-Palatinate, Germany. The defendants ran CyberBunker for almost six years and advertised "bulletproof hosting&rdquo; where they permitted everything except child pornography and terrorism. The defendants were sentenced on December 13, 2021, following a more than one-year trial. A 62-year-old Dutchman and main defendant, accused of purchasing the NATO bunker and setting up the web-hosting services, was sentenced to five years and nine months in prison. Six of the other defendants were sentenced to prison sentences ranging from two years and four months to four years and three months. The eighth defendant received a suspended sentence of one year. _ Many CyberBunker servers were originally located within the bunker.   The defendants were arrested on September 26, 2019, as a result of investigations by the State Central Office for Cybercrime (LZC) of the General Public Prosecutor's Office in Koblenz and the Rhineland-Palatinate State Criminal Police Office. The investigations reportedly took nearly five years. Related: The Cyberbunker Trial Began This Week Investigators revealed that CyberBunker had provided hosting for the administrators of Cannabis Road, Wall Street Market, and a generation of Flugsvamp. The prosecutor charged the defendants for their membership in a criminal organization (CyberBunker) and with aiding and abetting in the more than 250,000 illicit transactions that took place through the darkweb marketplaces hosted on CyberBunker servers. However presiding judge G&uuml;nther Koehler said that having a general understanding that some of their customers had hosted illicit content is not enough to prove intent to assist in the criminal activity. _ The majority of the defendants have been in custody for some time now.   [DNL again: It seems as if the prosecution failed to provide evidence that all eight defendants had participated in a criminal organization, especially if they failed to link the defendants to any of the crimes of their customers. In a country with a sensible legal system (non-existent), one would think that the defendant who worked as a customer service representative, at the very least, would successfully appeal this verdict. This case is the opposite of the Freedom Hosting case where the defendant allowed child abuse forums to use his servers and provided them assistance and discounts.]

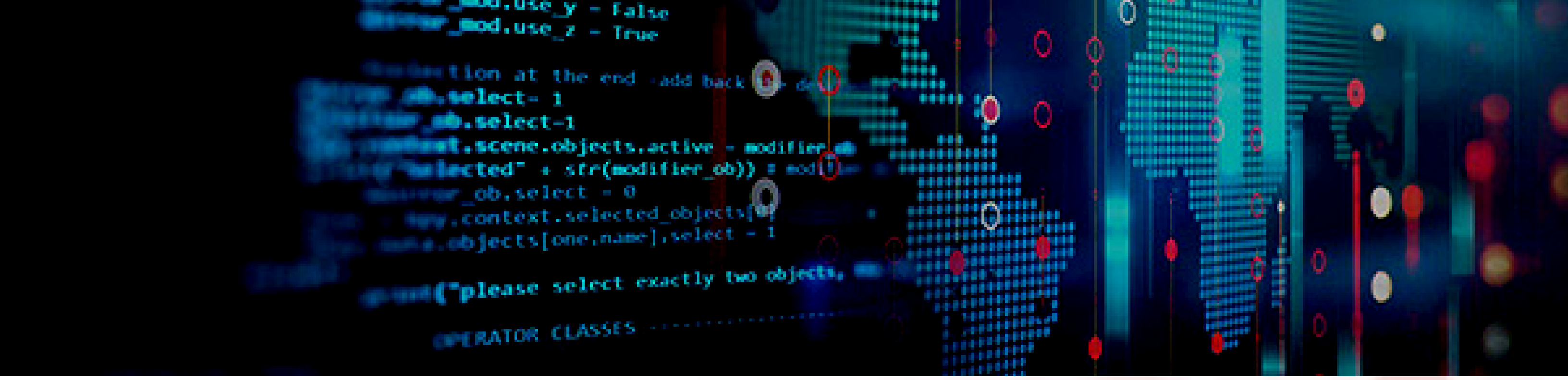
Quad9 Must Block DNS Queries to a Piracy Site in Germany

A court in Germany ruled that the DNS-resolver Quad9 must stop resolving DNS queries to an alleged piracy website unaffiliated with Quad9. Earlier this year, Sony Music obtained an injunction against Quad9 in the lower court of Hamburg, Germany, that required the DNS-resolver to block DNS resolution of the domain or domains of a site that allegedly violates Sony's copyrights. TorrentFreak, a site that is obviously more capable of reporting on piracy-related news than Darknetlive, identified the likely subject of the case as CannaPower, a well-known music-sharing website. __ From the name of the site, one might think it belonged to a online marijuana vendor. I will operate under the assumption that TorrentFreak is correct. A cursory examination of the injunction as well as the CUII initial action against the site indicates that TorrentFreak is likely right. However, Quad9 does not apparently have a record of blocking CannaPower-at least via the domain name provided in the TorrentFreak article. No variant of CannaPower's URLs appear to be blocked by Quad9. __ It appears as if both CannaPower and the subject site use the same backend. PHP Fusion? Prior to Sony's case against the site, Internet Service Providers (ISPs) in Germany voluntarily agreed to block the resolution of DNS queries to sites hosting allegedly pirated content. CannaPower, which quickly added a set of mirrors to circumvent the DNS block, noted that the ISPs 1&1, Vodafone, and Telekom had already blocked their site. After the establishment of the Clearingstelle Urheberrecht im Internet (CUII) in early 2021, Vodafone grew increasingly aggressive in blocking access to websites. The provider voluntarily blocked access to Libgen, a huge online repository of free books and academic articles. __ Of course, Germany is an awful country for uncensored internet access, perhaps only behind New Zealand and Russia and tied with the United States and the United Kingdom. As a result of Germany's aggressive censorship policies, users of "piracy&rdquo; sites are familiar with the process of switching to a better DNS resolver. CannaPower guides its users to switch to Cloudflare, censurfridns.dk, Google, or simply DNS-over-TLS. (By the way, you should most likely do this regardless of the country you live in.) Sony, a company that aggressively pursues perceived Copywrite violations, has caught on to this tactic. Sony Music received an injunction in Germany against Quad9 which stopped the Swiss-based DNS-resolver from resolving the target site. __ It is not clear if Quad9's database simply has not been updated to reflect recent additions to the blocklist. "We're disappointed that this first set of hearings ended in what we think is an outcome that is not consistent with the legislative intentions of the German government,&rdquo; said John Todd, General Manager of Quad9. "There are a large number of Internet-based services which we think ultimately are put at serious risk by this ruling, and we will not stop our legal challenges on this injunction. We object to the decision not just for ourselves but for all of our end-users, network operators, software developers, and network services that we believe are the targets of this ruling in its much wider context.&rdquo; As for the block being inconsistent with the legislative intentions of the German government, Todd might be correct. The German government wants to prevent so-called offensive content. Sites impacted by Germany's laws, according to HumanRightsWatch, "include a leader of the far-right Alternative for Germany party, a satire magazine, and a political street artist.&rdquo; (Imagine thinking AfD is actually "far-right&rdquo; lol.) The blocking of piracy websites is something done at the behest of corporations. Quad9 appealed this injunction. As reported by TorrentFreak on December 6, the Regional Court in Hamburg chose to uphold the previous ruling, ordering Quad9 to continue blocking the site in question. Mostly Off-Topic/CW:Intentionally Antagonistic Many will argue about how terrible the censorship in China is or the censorship in Russia for that matter. And the censorship in both countries is directed by the government and is a model directly incompatible with people living in what they believe are free countries. Neither China nor Russia block CannaPower. __ Canna is not blocked in China either. Russia's block lists, which are also mandated by the government's internet police, function in a similar fashion to China's firewall. For example, Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media asked DeepDotWeb to remove a guide on how to use a Russian darkweb marketplace. Prihar ignored the request. As a result, Russia's internet police blocked access to the specific guide, leaving the rest of the site accessible to users in Russia. __ I do not blame them. China, for the most part, blocks websites the government considers socially harmful, such as Darknetlive.com, and pornography sites, such as xhamster.com. Content that brings shame to the national identity of the country or

its government, criticism of the government although not necessarily criticism over policy, etc. Or the "Strict Management to Effectively Prevent Minors from Addiction to Online Games&rdquo; that forces online gaming companies to only allow minors to play for one hour from 8:00 to 9:00 PM on Friday, Saturday, and Sunday. The gaming services must prevent minors from accessing online video games at any other times.
_ kek Chinese citizens should be thankful the government has saved them from the invasive services offered by Google or Twitter. (I am mostly joking about that last part as the Chinese government has filled the invasive role of those private companies. But, this is far out of the scope of this article and Darknetlive articles are the wrong place to discuss this issue.) Since this site explicitly does not encourage anti-social behavior such as drug abuse or fraud, I am guessing China blocked Darknetlive to prevent citizens from accessing a repository of links to hidden services. I feel like this was far too long for an article about the blocking of a piracy website. However, the censorship at the ISP level and third-party DNS resolver is very important and will undoubtedly become a form of lawfare against other sites. Injunction (pdf) via Quad9.

Dark Web Link

White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats
Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from &#8220;Dark web&#8221; persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that &#8220;you didn't take any shit from anyone.&#8221; During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug
Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

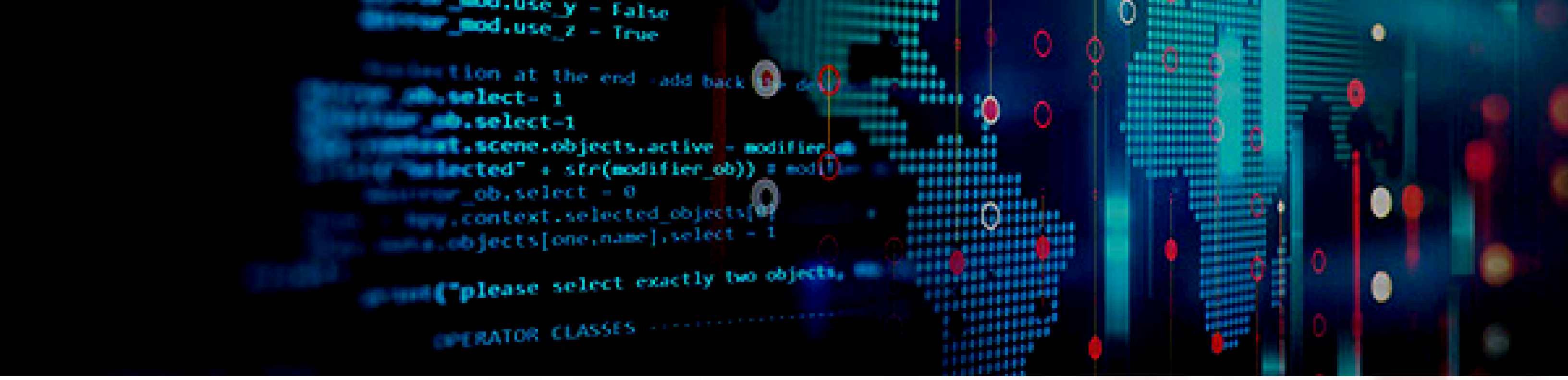
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management
* Discord CDN Abuse Found to Deliver 27 Unique Malware Types
* The Threat Landscape is Dynamic and Ever-Changing - Can You Keep Up?
* Mana Tools: A Malware C2 Panel with a Past

FireEye

* Metasploit Wrap-Up
* The Everyperson's Guide to Log4Shell (CVE-2021-44228)
* How to Protect Your Applications Against Log4Shell With tCell
* Patch Tuesday - December 2021
* Log4Shell Makes Its Appearance in Hacker Chatter: 4 Observations
* Using InsightVM to Find Apache Log4j CVE-2021-44228
* Update on Log4Shell's Impact on Rapid7 Solutions and Systems
* Hacky Holidays: Celebrating the Best of Security Nation [Video]
* Driver-Based Attacks: Past and Present
* Metasploit Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Issues ED 22-02 Directing Federal Agencies to Mitigate Apache Log4j Vulnerabilities
* VMware Releases Security Advisory
* NSA and CISA Release Final Part IV of Guidance on Securing 5G Cloud Infrastructures
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Immediate Steps to Strengthen Critical Infrastructure against Potential Cyberattacks
* Adobe Releases Security Updates for Multiple Products
* SAP Releases December 2021 Security Updates
* Microsoft Releases December 2021 Security Updates
* AA21-336A: APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus
* AA21-321A: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet V
* Vulnerability Summary for the Week of December 6, 2021
* Vulnerability Summary for the Week of November 29, 2021

Zero Day Initiative Advisories

ZDI-CAN-16119: Apache
A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-16, 4 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16115: Foxit
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 'Ashfaq Ansari and Krishnakant Patil - HackSys Inc' was reported to the affected vendor on: 2021-12-16, 4 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15696: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-16, 4 days ago. The vendor is given until 2022-04-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15986: Microsoft
A CVSS score 4.2 (AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15914: 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: 2021-12-15, 5 days ago. The vendor is given until

2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15294: Microsoft

A CVSS score 8.4 (AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nils Ole Timm (@firzen14)' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16027: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14943: Schneider Electric

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 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14942: Schneider Electric

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 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15082: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15341: Omron

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: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15592: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15193: Schneider Electric

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15118: Schneider Electric

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15593: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at psbc' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15198: Schneider Electric

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 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15119: Schneider Electric

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15420: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15589: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at psbc' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15690: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15934: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15933: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15763: 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 'Rich' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15931: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-12-15, 5 days ago. The vendor is given until 2022-04-14 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5199-1

Ubuntu Security Notice 5199-1 - It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex with a quadratic worst-case time complexity. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. It was discovered that the Python urllib http client could enter into an infinite loop when incorrectly handling certain server responses. Specially crafted traffic from a malicious HTTP server could cause a denial of service condition for a client. Various other issues were also addressed.

Ubuntu Security Notice USN-5201-1

Ubuntu Security Notice 5201-1 - It was discovered that the Python urllib http client could enter into an infinite loop when incorrectly handling certain server responses. Specially crafted traffic from a malicious HTTP server could cause a denial of service condition for a client.

Ubuntu Security Notice USN-5200-1

Ubuntu Security Notice 5200-1 - It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex allowing for catastrophic backtracking. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. It was discovered that the urllib.request.AbstractBasicAuthHandler class in Python contains regex with a quadratic worst-case time complexity. Specially crafted traffic from a malicious HTTP server could cause a regular expression denial of service condition for a client. Various other issues were also addressed.

Apple Security Advisory 2021-12-15-7

Apple Security Advisory 2021-12-15-7 - Safari 15.2 addresses buffer overflow, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-6

Apple Security Advisory 2021-12-15-6 - watchOS 8.3 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-5

Apple Security Advisory 2021-12-15-5 - tvOS 15.2 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-4

Apple Security Advisory 2021-12-15-4 - Security Update 2021-008 Catalina addresses buffer overflow, bypass, code execution, heap corruption, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-3

Apple Security Advisory 2021-12-15-3 - macOS Big Sur 11.6.2 addresses buffer overflow, bypass, code execution, heap corruption, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-2

Apple Security Advisory 2021-12-15-2 - macOS Monterey 12.1 addresses buffer overflow, bypass, code execution, heap corruption, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-12-15-1

Apple Security Advisory 2021-12-15-1 - iOS 15.2 and iPadOS 15.2 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5192-2

Ubuntu Security Notice 5192-2 - USN-5192-1 fixed a vulnerability in Apache Log4j 2. This update provides the corresponding update for Ubuntu 16.04 ESM. Chen Zhaojun discovered that Apache Log4j 2 allows remote attackers to run programs via a special crafted input. An attacker could use this vulnerability to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5202-1

Ubuntu Security Notice 5202-1 - Varnavas Papaioannou discovered that the FTP client implementation in OpenJDK accepted alternate server IP addresses when connecting with FTP passive mode. An attacker controlling an FTP server that an application connects to could possibly use this to expose sensitive information. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. Markus Loewe discovered that OpenJDK did not properly handle JAR files containing multiple manifest files. An attacker could possibly use this to bypass JAR signature verification. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04. Various other issues were also addressed.

Red Hat Security Advisory 2021-5186-04

Red Hat Security Advisory 2021-5186-04 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-5183-06

Red Hat Security Advisory 2021-5183-06 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-5184-04

Red Hat Security Advisory 2021-5184-04 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-5107-06

Red Hat Security Advisory 2021-5107-06 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-5179-02

Red Hat Security Advisory 2021-5179-02 - PostgreSQL is an advanced object-relational database management system. Issues addressed include a man-in-the-middle vulnerability.

Red Hat Security Advisory 2021-5176-04

Red Hat Security Advisory 2021-5176-04 - Go Toolset provides the Go programming language tools and libraries. Go is alternatively known as golang.

Red Hat Security Advisory 2021-5195-02

Red Hat Security Advisory 2021-5195-02 - Red Hat Identity Management is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments.

Red Hat Security Advisory 2021-5192-04

Red Hat Security Advisory 2021-5192-04 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Red Hat Security Advisory 2021-5171-03

Red Hat Security Advisory 2021-5171-03 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include HTTP request smuggling and denial of service vulnerabilities.

Red Hat Security Advisory 2021-5191-02

Red Hat Security Advisory 2021-5191-02 - Red Hat 3scale API Management delivers centralized API management features through a distributed, cloud-hosted layer. It includes built-in features to help in building a more successful API program, including access control, rate limits, payment gateway integration, and developer experience tools. This advisory is intended to use with Container Images, for Red Hat 3scale API Management 2.11.1. Issues addressed include an XML injection vulnerability.

Red Hat Security Advisory 2021-5197-03

Red Hat Security Advisory 2021-5197-03 - PostgreSQL is an advanced object-relational database management system. Issues addressed include a man-in-the-middle vulnerability.

VMware Security Advisory 2021-0029

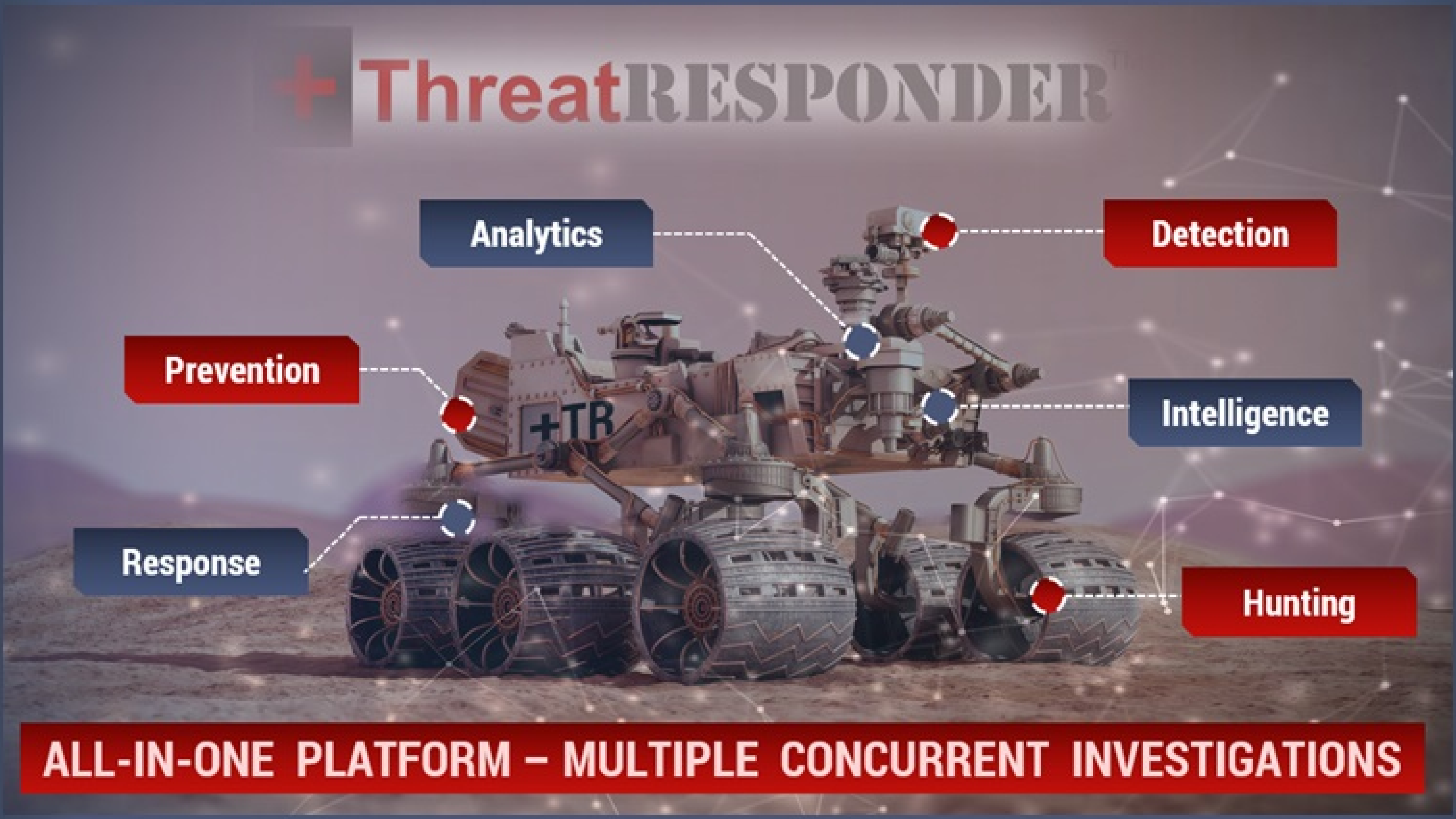
VMware Security Advisory 2021-0029 - VMware Workspace ONE UEM console patches address a server-side request forgery (SSRF) vulnerability.

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



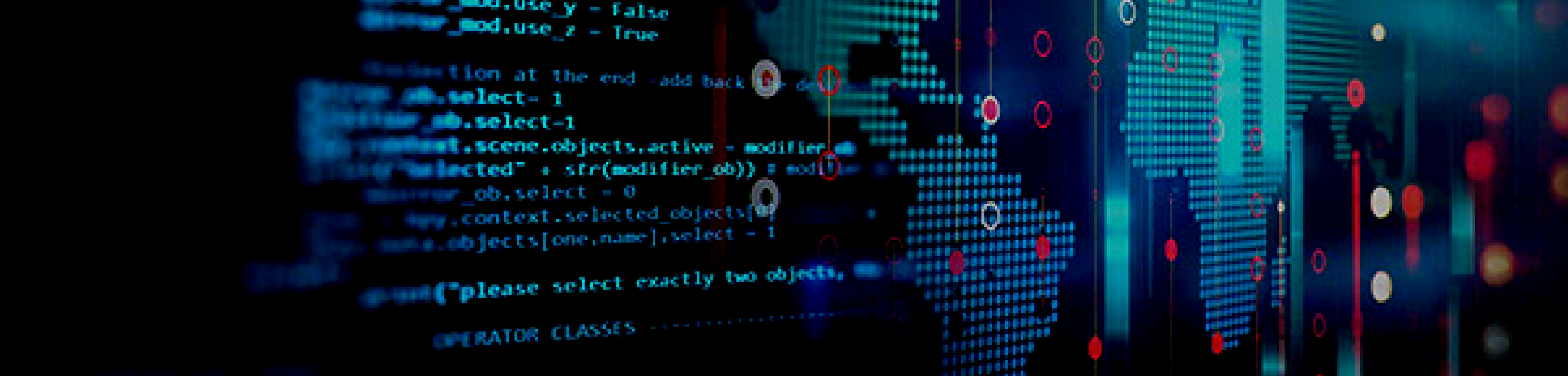
The Solution – ThreatResponder® Platform

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



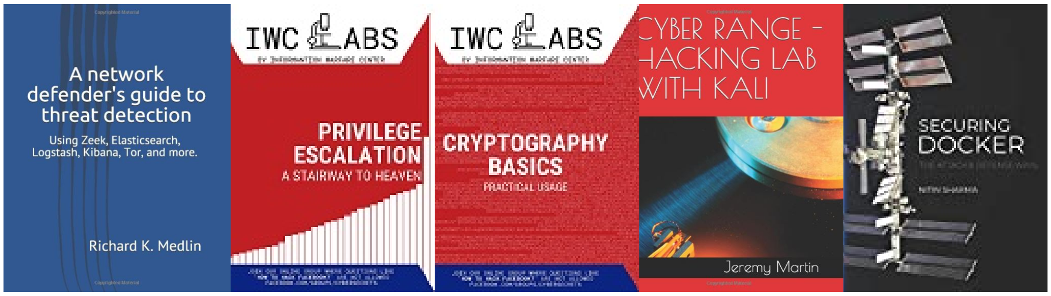
The Cyber Secrets publications on Amazon

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
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS
OF THE OSI CAKE
A FORENSIC TASTE
OF EACH LAYER
LAUNCHING
EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
SOCRANGE
LINUX
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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP