May-10-21

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

May 10, 2021

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

Summary

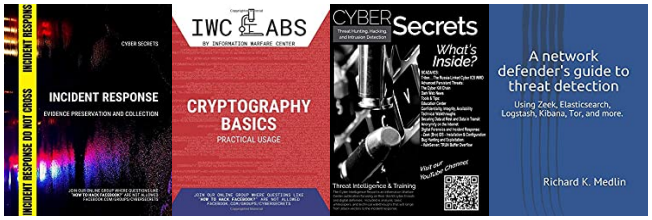
Internet Storm Center Infocon Status

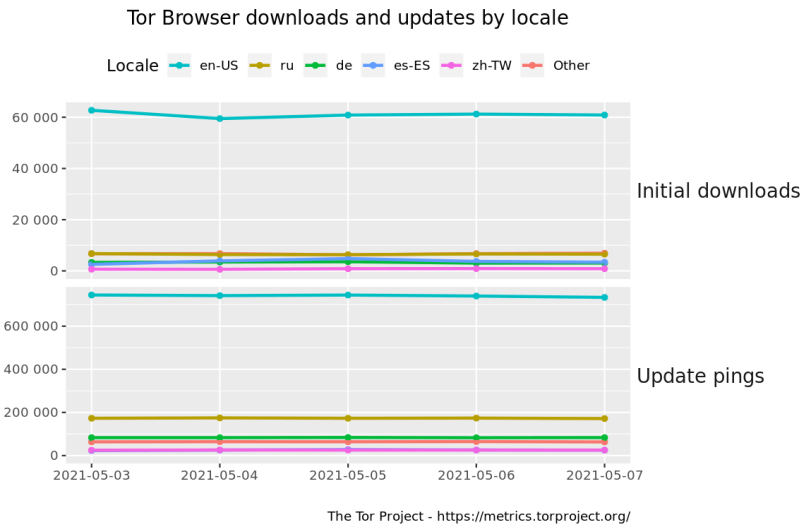
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

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

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





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 is working on an updated set of tools. If you have any suggestions for additional capability or cahnges, please let the team know at support@csilinux.com

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

Index of Sections

Packet Storm Security

* 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
* Dogecoin Has To Be Taken Seriously Now
* New Crypto Stealer Panda Spread Via Discord
* JET Engine Flaws Can Crash Microsoft IIS And SQL Servers
* Data Leak Makes Peloton's Horrible, No-Good, Really Bad Day Even Worse
* Americans Turn To VPNs To Prevent Online Fraud And Hacking
* Scammer Used Fake Court Order To Take Over Dark Web Drug Market Directory
* Qualys Puts 21 Nails Into Exim Mail Server
* Dell Patches Vulnerable Driver For Over A Decade Of Products
* Deepfake Attacks Are About To Surge, Experts Warn
* 4,700 Amazon Employees Had Unauthorized Access To Private Seller Data
* Three New Malware Families Found In Global Finance Phish
* New Buer Malware Downloader Rewritten In E-Z Rust Language
* Experian API Leaks Most Americans' Credit Scores
* An Ambitious Plan To Tackle Ransomware Faces Long Odds
* You Should Update Your iPhone And iPad To iOS 14.5.1 Right Away
* Ransomware Group Targeted SonicWall Vulnerability Pre-Patch
* Multi-Gov Task Force Plans To Take Down The Ransomware Economy
* Australia Proposes Teaching Cybersecurity To 5 Year Olds
* The IRS Wants Help Hacking Cryptocurrency Hardware Wallets
* Chase Bank Phish Swims Past Exchange Email Protections

Krebs on Security

* 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
* Note to Self: Create Non-Exhaustive List of Competitors
* Did Someone at the Commerce Dept. Find a SolarWinds Backdoor in Aug. 2020?
* Microsoft Patch Tuesday, April 2021 Edition
* ParkMobile Breach Exposes License Plate Data, Mobile Numbers of 21M Users

Dark Reading

* How North Korean APT Kimsuky Is Evolving Its Tactics
* Most Organizations Feel More Vulnerable to Breaches Amid Pandemic
* FBI, NSA, CISA & NCSC Issue Joint Advisory on Russian SVR Activity
* The Edge Pro Quote: Password Empowerment
* Defending Against Web Scraping Attacks
* 11 Reasons Why You Sorta Love Passwords
* Black Hat Asia Speakers Share Secrets About Sandboxes, Smart Doors, and Security
* Troy Hunt: Organizations Make Security Choices Tough for Users
* New Techniques Emerge for Abusing Windows Services to Gain System Control
* Google Plans to Automatically Enable Two-Factor Authentication
* CISA Publishes Analysis on New 'FiveHands' Ransomware
* Cloud-Native Businesses Struggle With Security
* Securing the Internet of Things in the Age of Quantum Computing
* Biden's Supply Chain Initiative Depends on Cybersecurity Insights
* How to Move Beyond Passwords and Basic MFA
* Attackers Seek New Strategies to Improve Macros' Effectiveness
* Gap Between Security and Networking Teams May Hinder Tech Projects
* DoD Lets Researchers Target All Publicly Accessible Info Systems
* Wanted: The (Elusive) Cybersecurity 'All-Star'
* Debating Law Enforcement's Role in the Fight Against Cybercrime

The Hacker News

* Over 25% Of Tor Exit Relays Spied On Users' Dark Web Activities
* Is it still a good idea to require users to change their passwords?
* Four Plead Guilty to Aiding Cyber Criminals with Bulletproof Hosting
* Ransomware Cyber Attack Forced the Largest U.S. Fuel Pipeline to Shut Down
* Facebook Will Limit Your WhatsApp Features For Not Accepting Privacy Policy
* Top 12 Security Flaws Russian Spy Hackers Are Exploiting in the Wild
* 4 Major Privacy and Security Updates From Google You Should Know About
* 6 Unpatched Flaws Disclosed in Remote Mouse App for Android and iOS
* New TsuNAME Flaw Could Let Attackers Take Down Authoritative DNS Servers
* New Stealthy Rootkit Infiltrated Networks of High-Profile Organizations
* CISO Challenge: Check Your Cybersecurity Skills On This New Competition Site
* Critical Flaws Hit Cisco SD-WAN vManage and HyperFlex Software
* New Qualcomm Chip Bug Could Let Hackers Spy On Android Devices
* New Spectre Flaws in Intel and AMD CPUs Affect Billions of Computers
* New Study Warns of Security Threats Linked to Recycled Phone Numbers

Security Week

* WhatsApp Delays Enforcing New Privacy Terms
* City of Chicago Hit by Data Breach at Law Firm Jones Day
* SolarWinds Shares More Information on Cyberattack Impact, Initial Access Vector
* Cyberattack on US Pipeline is Linked to Criminal Gang
* Colonial Pipeline Struggles to Restart After Ransomware Attack
* Cyberattack Forces Shutdown of Major U.S. Pipeline
* US-UK Gov Warning: SolarWinds Attackers Add Open-Source PenTest Tool to Arsenal
* Under the Microscope: ISACA Survey on Cybersecurity Workforce, Resources and Budgets
* CISA Analyzes FiveHands Ransomware
* Android App Developers Required by Google to Share More Info on Data Handling
* TsuNAME Vulnerability Can Be Exploited for DDoS Attacks on DNS Servers
* VMware Patches Critical Flaw Reported by Sanctioned Russian Security Firm
* Insurer AXA Halts Ransomware Crime Reimbursement in France
* Qualcomm Modem Chip Flaw Exploitable From Android: Researchers
* Russian 'Evil Corp' Cybercriminals Possibly Evolved Into Cyberspies
* Google to Automatically Enable Two-Step Verification for Some Accounts
* MDR Firm Huntress Raises $40 Million in Series B Funding Round
* Cisco Patches Critical Flaws in SD-WAN, HyperFlex HX Products
* Cybersecurity Experts Share Thoughts for World Password Day
* Microsoft Pledges to Store European Cloud Data in EU

Infosecurity Magazine

* Malicious UK Website Takedowns Surge 15-Fold in 2020
* UK/US: Patch These 11 Bugs Now to Thwart Russian Spies
* Ransomware Takes Down East Coast Fuel Pipeline
* Three Marylanders Indicted Over BEC Scam
* Lawsuit Filed Over Contact Tracing Data Breach
* Bot Attacks a Top Cybersecurity Concern
* NCSC Sets Out Security Principles for Smart Cities
* Millions of Households at Risk from Outdated Routers
* #COVID19 Researchers Lose a Week's Work to Ryuk Ransomware
* Misconfigured Database Exposes 200K Fake Amazon Reviewers
* "Unusually Unhinged" Cyber-stalker Jailed for 10 Years
* CaptureRx Data Breach Impacts Healthcare Providers

KnowBe4 Security Awareness Training Blog RSS Feed

* Student's Attempt to Pirate Software Leads to Ryuk Ransomware Attack
* KnowBe4 Fresh Content Updates from April: Including New AI-Driven Phishing Feature
* [NEW FEATURE] AI-Driven Phishing Helps Admins Deliver a Personalized Simulated Phishing Experien
* Strange Chinese APT Interest in Buying Batches of AV Products
* New IceID Phishing Attack Targets Website Owners Using Image Copyright Infringement as The Hook
* W-2 Form Office 365 Credential Scam Creatively Uses Typeform Service to Bypass Security Checks
* Cybersecurity Spend Is Now More Than 20% of the Average IT Budget As 91% of Organizations Suffering a
* [HEADS UP] New Malware Families Found in Phishing Campaign
* Genesis Market: a Study in the C2C Economy
* A Snapshot of the Ransomware Landscape

ISC2.org Blog

* CISSPs from Around the Globe: An Interview with Jason Lau
* Help Shape The HCISPP Exam
* Keeping Excess Out of Access
* Report: (ISC)2 Cybersecurity Career Pursuers Study Provides Insights From Professionals and Jobseeker
* These Roles Require Cybersecurity Training

HackRead

* Major ransomware attack cripples largest gas pipeline in the US
* WhatsApp is reportedly working on web version without connected phone
* $2 million lost as WallStreetBets forum members fall for crypto scam
* Leaky database exposes fake Amazon product reviews scam
* The growing security problem of Bring Your Own Device (BYOD)
* 5 PDF Tricks You Should Know To Improve Document Productivity
* How chat platforms are using Machine Learning for content moderation?

Koddos

* Major ransomware attack cripples largest gas pipeline in the US
* WhatsApp is reportedly working on web version without connected phone
* $2 million lost as WallStreetBets forum members fall for crypto scam
* Leaky database exposes fake Amazon product reviews scam
* The growing security problem of Bring Your Own Device (BYOD)
* 5 PDF Tricks You Should Know To Improve Document Productivity
* How chat platforms are using Machine Learning for content moderation?

Naked Security

* 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!
* Naked Security Live - Beware 'Flubot': the home delivery scam with a difference
* PHP community sidesteps its third supply chain attack in three years
* S3 Ep30: AirDrop worries, Linux pests and ransomware truths [Podcast]
* Gamers update! Nvidia patches GPU driver kernel escalation bugs
* Ransomware: don't expect a full recovery, however much you pay
* Naked Security Live - Just how (un)safe is AirDrop?

Threat Post

* Major U.S. Pipeline Crippled in Ransomware Attack
* iPhone Hack Allegedly Used to Spy on China's Uyghurs
* 80% of Net Neutrality Comments to FCC Were Fudged
* Qualcomm Chip Bug Opens Android Fans to Eavesdropping
* Critical Cisco SD-WAN, HyperFlex Bugs Threaten Corporate Networks
* Ryuk Ransomware Attack Sprung by Frugal Student
* Massive DDoS Attack Disrupts Belgium Parliament
* New Crypto-Stealer 'Panda' Spread via Discord
* Anti-Spam WordPress Plugin Could Expose Website User Data
* Raft of Exim Security Holes Allow Linux Mail Server Takeovers

Null-Byte

* 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
* Master Python, Linux & More with This Training Bundle
* Make Spoofed Calls Using Any Phone Number You Want Right from Your Smartphone

IBM Security Intelligence

* How a Firewall Can Foster Zero Trust
* 3 Ways to Reduce the Cost of a Government Data Breach
* What is Ghimob Malware?
* Health Care Data: It's Your Personal 'National Security' Information
* Security by Design and NIST 800-160, Part 1: Managing Change
* Zero Trust and Insider Threats: Was Brutus the Original Bad Actor?
* Does Multifactor Authentication Keep Your Remote Workers Safe?
* Improving Data Security in Schools: Remote Learning Increases Security Threats
* Zero Trust: Confidently Secure Your Business to Grow Fearlessly
* Adopting Microsegmentation Into Your Zero Trust Model, Part 2

InfoWorld

* How companies are moving on from Cobol
* What to look for (and look out for) in container registries
* Kotlin 1.5.0 arrives with JVM records, sealed interfaces
* When not to use edge computing
* Visual Studio Code 1.56 improves hover feedback, debugging
* Instagram open sources high-performance Python fork
* Pyston project open sources its faster Python
* How a digital integration hub transforms the mainframe
* How Kubernetes works
* Microsoft fleshes out Power Apps

C4ISRNET - Media for the Intelligence Age Military

* House Defense leader: Space Force hasn't met expectations for speedy tech
* DIU looking for new multifactor authentication tool
* Air Force once again asks Congress to let it mothball oldest RQ-4 Global Hawk drones
* Want better AI for the DOD? Stop treating data like currency
* Bill seeks to bolster National Guard's role in cyber response
* Hughes and OneWeb working to fill military's Arctic communication gap
* Space Force wants to be the world's first fully digital service
* How commercial satellite constellations fit into the Army's future tactical network designs
* The Air Force's first Skyborg autonomous drone prototype made its first flight
* Air Force cyber school will add online training tool

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.

* DCTF 2021
* m0leCon CTF 2021 Teaser
* FarEastCTF - 2021
* 3kCTF-2021
* OMH 2021 CTF
* NorzhCTF 2021
* Pwn2Win CTF 2021
* ICHSA CTF 2021
* Zh3r0 CTF V2
* S.H.E.L.L. CTF

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

* HarryPotter: Nagini
* HarryPotter: Aragog
* Clover: 1
* HarryPotter: Fawkes
* Momentum: 1

Tools & Techniques

Packet Storm Security Tools Links

* 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
* GRAudit Grep Auditing Tool 3.0
* nfstream 6.3.1
* Wireshark Analyzer 3.4.5
* Zeek 4.0.1
* nfstream 6.3.0

Kali Linux Tutorials

* SniperPhish : The Web-Email Spear Phishing Toolkit
* M365_Groups_Enum : Enumerate Microsoft 365 Groups In A Tenant With Their Metadata
* Tscopy : Tool to parse the NTFS $MFT file to locate and copy specific files
* Cook : A Customizable Wordlist And Password Generator
* Invoke-Stealth : Simple And Powerful PowerShell Script Obfuscator
* Profil3r : OSINT Tool That Allows You To Find A Person'S Accounts And Emails + Breached Emails
* Fav-Up : IP Lookup By Favicon Using Shodan
* Ldsview : Offline search tool for LDAP directory dumps in LDIF format
* Posta : Cross-document Messaging Security Research Tool
* OverRide : Binary Exploitation And Reverse-Engineering

GBHackers Analysis

* New Spectre Vulnerability Let Hackers Attack Billions of Computers
* Hundreds of Millions of Dell Systems Vulnerable to Hack_Due to Driver Bug
* Linux kernel Bug Let Attackers Insert Malicious Code Into The Kernel Address Space
* NSA Released Top 5 Vulnerabilities That Exploited by Russian Hackers to Hack US Based Networks
* Critical Zero-day Vulnerability in Desktop Window Manager (DWM) Let Attackers to Escalate Privilege

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: How to find anything on the internet with Google Dorks
* Hacking Time to Live - the many roads of Hack Across America 2021
* Two Year Old Linux Backdoor Found, Microsoft Finds IoT Vulnerabilities - ThreatWire

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* SOCIAL MEDIA is DANGEROUS - Startup Life
* ASK for HELP - Startup Life
* Value of LIVED EXPERIENCE - Startup Life
* Building a BUSINESS or CHARITY - Startup Life

Security Now

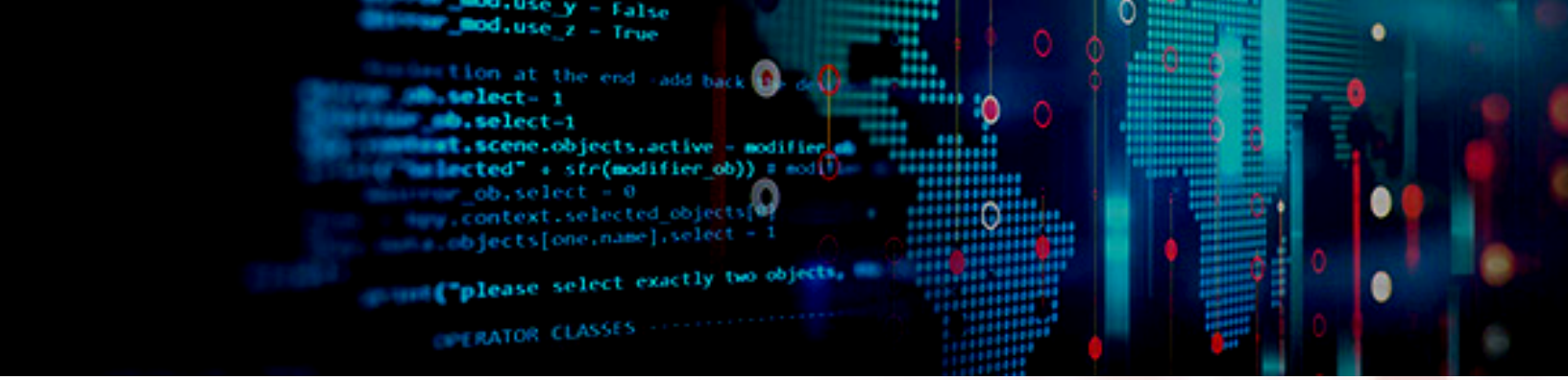
* The Ransomware Task Force - Scripps Health, REvil Hacks Quanta Computer, Emotet Botnet, QNAP
* The Mystery of AS8003 - Remembering Dan Kaminski, Project Zero, Unethical Security Research

Troy Hunt

* Weekly Update 242

Intel Techniques: The Privacy, Security, & OSINT Show

* 215-When OSINT Is Abused
* 214-Offense/Defense: The Capitol Siege



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

* 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
* Microsoft Exchange Server Remote Code Execution Vulnerability: RiskIQ's Response

FireEye

* Metasploit Wrap-Up
* The Evolution of DevOps in 2021
* Rapid7's 2021 ICER Takeaways: Version Complexity Among the Fortune 500
* MDR Vendor Must-Haves, Part 9: Assigned Analyst Pods and Security Program Advisors
* Rapid7 Releases New Industry Cyber-Exposure Report (ICER): ASX 200
* 4 DevOps Challenges to Cloud Security and Compliance-and How IaC Can Help
* Kubernetes Security Is Not Container Security
* Securing Kubernetes Deployments From Runway to Takeoff
* Grow, Develop, and Impact More Than Just Your Career: Software Engineering at Rapid7 Belfast
* Metasploit Wrap-Up

Proof of Concept (PoC) & Exploits

Packet Storm Security

* macOS Gatekeeper Check Bypass
* Epic Games Easy Anti-Cheat 4.0 Local Privilege Escalation
* WifiHotSpot 1.0.0.0 Unquoted Service Path
* Android Memory Disclosure / Out-Of-Bounds Write / Double-Free
* Voting System 1.0 Shell Upload
* Human Resource Information System 0.1 Remote Code Execution
* Voting System 1.0 SQL Injection
* Sandboxie Plus 0.7.4 Unquoted Service Path
* Sandboxie 5.49.7 Denial Of Service
* b2evolution 7-2-2 SQL Injection
* WordPress WP Super Edit 2.5.4 Arbitrary File Upload
* Schlix CMS 2.2.6-6 Remote Code Execution
* Schlix CMS 2.2.6-6 Cross Site Scripting
* Xmind 2020 Cross Site Scripting / Code Execution
* Tagstoo 2.0.1 Cross Site Scripting / Code Execution
* Marky 0.0.1 Cross Site Scripting / Code Execution
* StudyMD 0.3.2 Cross Site Scripting / Code Execution
* SnipCommand 0.1.0 Cross Site Scripting / Code Execution
* Moeditor 0.2.0 Cross Site Scripting / Code Execution
* Markdownify 1.2.0 Cross Site Scripting / Code Execution
* Freeter 1.2.1 Cross Site Scripting / Code Execution
* Markdown-Explorer 0.1.1 Cross Site Scripting / Code Execution
* Markright 1.0 Cross Site Scripting / Code Execution
* Anote 1.0 Cross Site Scripting / Code Execution
* Backdoor.Win32.NinjaSpy.c Code Execution

CXSecurity

* GravCMS 1.10.7 Unauthenticated Arbitrary YAML Write/Update (Metasploit)
* macOS Gatekeeper Check Bypass
* Human Resource Information System 0.1 Remote Code Execution (Unauthenticated)
* b2evolution 7-2-2 SQL Injection
* IGEL OS Secure VNC/Terminal Command Injection
* TYPO3 6.2.1 SQL Injection
* Piwigo 11.3.0 language SQL

Proof of Concept (PoC) & Exploits

Exploit Database

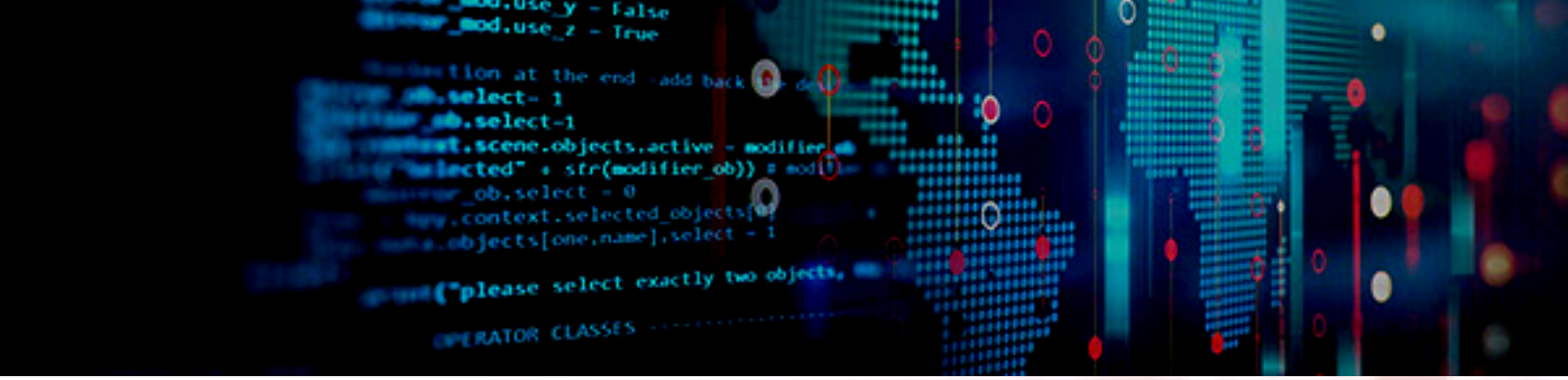
* [webapps] Microweber CMS 1.1.20 - Remote Code Execution (Authenticated)
* [webapps] Human Resource Information System 0.1 - 'First Name' Persistent Cross-Site Scripting (Aut
* [webapps] PHP Timeclock 1.04 - 'Multiple' Cross Site Scripting (XSS)
* [local] TFTP Broadband 4.3.0.1465 - 'tftpt.exe' Unquoted 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)
* [local] Sandboxie Plus 0.7.4 - 'SbieSvc' Unquoted Service Path
* [local] Epic Games Easy Anti-Cheat 4.0 - Local Privilege Escalation
* [webapps] b2evolution 7-2-2 - 'cf_name' SQL Injection
* [webapps] Wordpress Plugin WP Super Edit 2.5.4 - Remote File Upload
* [webapps] Schlix CMS 2.2.6-6 - Remote Code Execution (Authenticated)
* [webapps] Schlix CMS 2.2.6-6 - 'title' Persistent Cross-Site Scripting (Authenticated)
* [webapps] Anote 1.0 - XSS to RCE
* [webapps] Markdownify 1.2.0 - XSS to RCE
* [webapps] Markright 1.0 - XSS to RCE
* [webapps] Freeter 1.2.1 - XSS to RCE
* [webapps] StudyMD 0.3.2 - XSS to RCE

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*

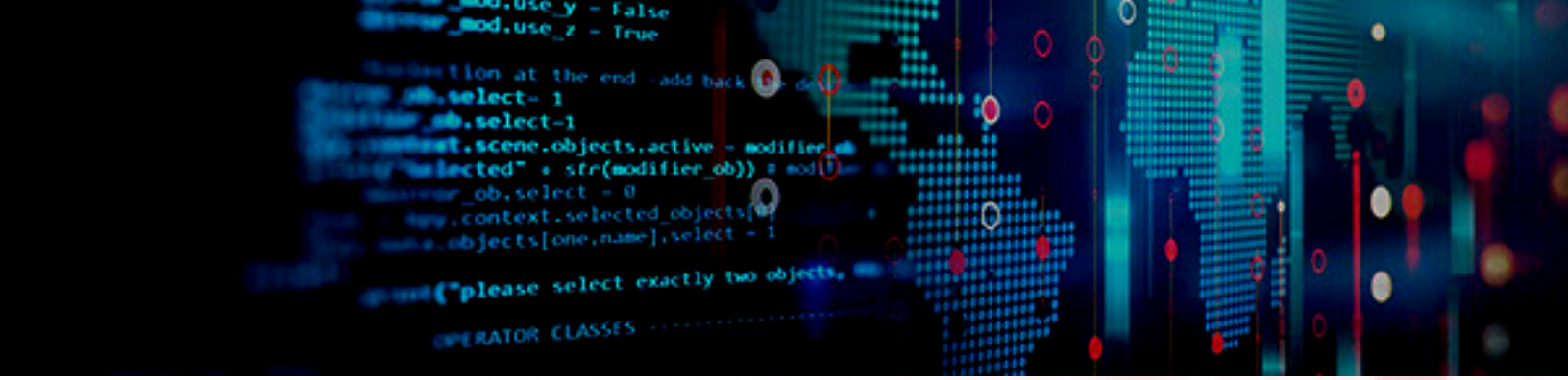
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.vladatk.gov.ba/fsfs.htm
http://www.vladatk.gov.ba/fsfs.htm notified by Trenggalek Cyber Army
http://www.dpv.misiones.gov.ar/fuck.html
http://www.dpv.misiones.gov.ar/fuck.html notified by 0x1998
https://jamalpurtsc.gov.bd
https://jamalpurtsc.gov.bd notified by Cyber Lion
http://www.manangdalam.go.th/ngenk.htm
http://www.manangdalam.go.th/ngenk.htm notified by Xyp3r2667
https://www.maracaibo.gob.ve
https://www.maracaibo.gob.ve notified by Crystal_MSF
http://ephesus.gov.tr/f12.html
http://ephesus.gov.tr/f12.html notified by Moroccan Revolution
http://efestr.gov.tr/f12.html
http://efestr.gov.tr/f12.html notified by Moroccan Revolution
http://swatpolice.gov.pk/ghi.html
http://swatpolice.gov.pk/ghi.html notified by Ghost Hunter Illusion
https://www.jandira.sp.gov.br/FroggBaba.html
https://www.jandira.sp.gov.br/FroggBaba.html notified by phr099 8484
http://saae.boaesperanca.mg.gov.br/Team_Ti74N5.php
http://saae.boaesperanca.mg.gov.br/Team_Ti74N5.php notified by Team Ti74N5
https://cabanatuancity.gov.ph/very-un-secured-website.txt
https://cabanatuancity.gov.ph/very-un-secured-website.txt notified by Anonymous Philippines
http://www.sylhetbetar.gov.bd
http://www.sylhetbetar.gov.bd notified by ./Anon666Txploit
https://pa-pangkalpinang.go.id/images/krz.txt
https://pa-pangkalpinang.go.id/images/krz.txt notified by Mr.Kro0oz.305
http://www3.ibatiba.es.gov.br/arquivo/
http://www3.ibatiba.es.gov.br/arquivo/ notified by Arch1999
http://www3.prodnorte.es.gov.br/arquivo/
http://www3.prodnorte.es.gov.br/arquivo/ notified by Arch1999
http://www3.laranjadaterra.es.gov.br/arquivo/
http://www3.laranjadaterra.es.gov.br/arquivo/ notified by Arch1999
http://www3.camarasooretama.es.gov.br/arquivo/
http://www3.camarasooretama.es.gov.br/arquivo/ notified by Arch1999



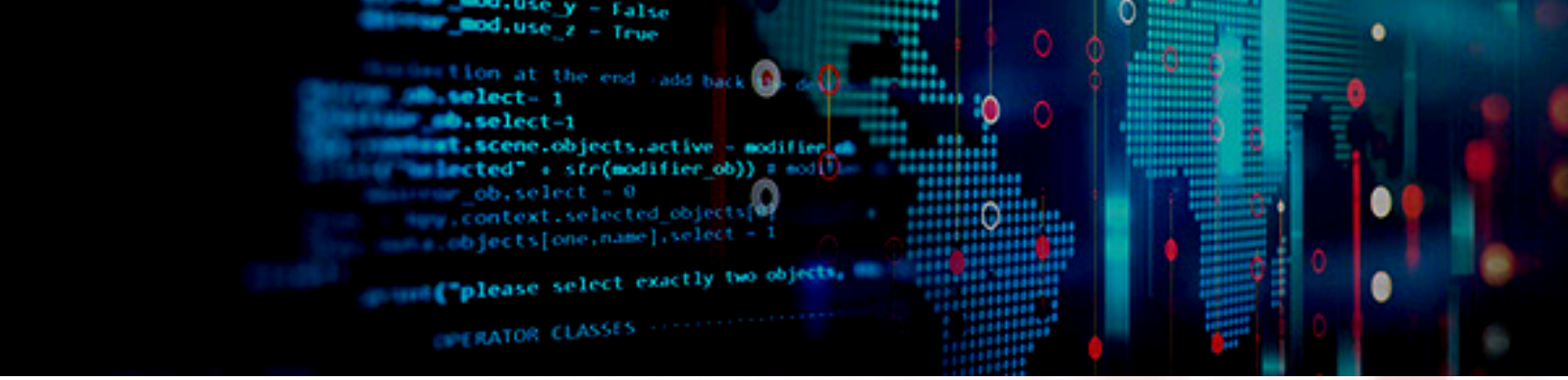
Dark Web News

Darknet Live

[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)
[Duo Behind "LetsWork" Vendor Account Sentenced to Prison]
Two drug dealers responsible for earning more than Â£3.7 million through the darkweb vendor account "LetsWork" were sentenced to a total of 24 years in prison. (via darknetlive.com)
[Meth Dealer Sentenced to 10 Years of Fed Time]
A federal judge sentenced a California-based methamphetamine dealer to 121 months in prison. (via darknetlive.com)
[Here Is Njalla's Take on the Domain Hijack]
Someone stole the domain darknetlive.com and used it to share phishing links. Njalla just answered some of the questions about what happened. (via darknetlive.com)

Dark Web Link

[Dogecoin Spike: Robinhood Crypto Trading Platform Suddenly Crashed Heavily]
The famous Cryptocurrency trading platform Robinhood is currently facing issues processing the cryptocurrency trades this morning. The sudden crash was caused as a result of the Dogecoin spike in price. The sudden soar in the Dogecoin price had sent flocks of users to the app. A website in this regard, DownDetector, has revealed the trading [...] The post Dogecoin Spike: Robinhood Crypto Trading Platform Suddenly Crashed Heavily appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Boystown: Dark Web Child Abuse Image Site Immediately Taken Down]
The German cops have been successful in arresting four members of a child abuse gang. The team members were suspected to be running one of the world's largest child abuse image websites named "Boystown”. The website housed over 400,000 members worldwide, the prosecutors and the police had stated on Monday. A police operation had been [...] The post Boystown: Dark Web Child Abuse Image Site Immediately Taken Down appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Tor V2 Onion Support To be Discontinued From October 2021]
The Tor Project had released a timeline back in July 2020 of deprecating the Tor V2 Onion support/services (The Onion Router Version 3 services). This step has been taken to integrate the more secure version of Tor's onion services called Version 3 or V3. The short encrypted services or the V2 services of Tor will [...] The post Tor V2 Onion Support To be Discontinued From October 2021 appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Exim Releases Security Update
* Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory on Russian SVR Activity
* Cisco Releases Security Updates for Multiple Products
* Mozilla Releases Security Updates for Firefox
* VMware Releases Security Update
* CISA Releases Analysis Reports on New FiveHands Ransomware
* Apple Releases Security Updates
* Ivanti Releases Pulse Secure Security Update
* AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for
* AA21-110A: Exploitation of Pulse Connect Secure Vulnerabilities
* Vulnerability Summary for the Week of April 26, 2021
* Vulnerability Summary for the Week of April 19, 2021

Zero Day Initiative Advisories

ZDI-CAN-13682: Microsoft
A CVSS score 3.5 (AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N) severity vulnerability discovered by 'mr_me' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13584: Microsoft
A CVSS score 7.1 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Steven Seeley (mr_me) of Source Incite' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13578: Apple
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 'hjy79425575' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13627: Apple
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13681: Microsoft
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 'kdot' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13812: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend

Micro Zero Day Initiative' was reported to the affected vendor on: 2021-05-07, 3 days ago. The vendor is given until 2021-09-04 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-13362: Apple

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 'Jzhu' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13807: Apple

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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13479: Apple

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 'Anonymous' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13360: Apple

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 'Jzhu' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13268: Apple

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 'hjy79425575' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13541: Apple

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 'Anonymous' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13505: Apple

A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'tr3e' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13540: Apple

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 'Anonymous' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13232: Apple

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 'Jzhu' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13453: SolarWinds

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13461: 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 'kimiya' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13486: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Abdelhamid Naceri (halov)' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13504: Microsoft
A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Abdelhamid Naceri (halov)' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13618: 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 'nghiadt12 from Viettel Cyber Security' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13325: NETGEAR
A CVSS score 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'LAME on that real gang yee' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13577: Apple
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 'hjy79425575' was reported to the affected vendor on: 2021-05-05, 5 days ago. The vendor is given until 2021-09-02 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-13695: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-04-30, 10 days ago. The vendor is given until 2021-08-28 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-13731: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-04-30, 10 days ago. The vendor is given until 2021-08-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-1515-01

Red Hat Security Advisory 2021-1515-01 - Openshift Logging Bug Fix Release. Issues addressed include code execution, denial of service, and deserialization vulnerabilities.

Ubuntu Security Notice USN-4938-1

Ubuntu Security Notice 4938-1 - It was discovered that Unbound contained multiple security issues. A remote attacker could possibly use these issues to cause a denial of service, inject arbitrary commands, execute arbitrary code, and overwrite local files.

Ubuntu Security Notice USN-4936-1

Ubuntu Security Notice 4936-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. It was discovered that Thunderbird may keep key material in memory in some circumstances. A local attacker could potentially exploit this to obtain private keys. Various other issues were also addressed.

Red Hat Security Advisory 2021-1511-01

Red Hat Security Advisory 2021-1511-01 - Red Hat AMQ Clients enable connecting, sending, and receiving messages over the AMQP 1.0 wire transport protocol to or from AMQ Broker 6 and 7. This update provides various bug fixes and enhancements in addition to the client package versions previously released on Red Hat Enterprise Linux 7 and 8. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-1512-01

Red Hat Security Advisory 2021-1512-01 - PostgreSQL is an advanced object-relational database management system.

Ubuntu Security Notice USN-4937-1

Ubuntu Security Notice 4937-1 - Ondrej Holy discovered that GNOME Autoar could extract files outside of the intended directory. If a user were tricked into extracting a specially crafted archive, a remote attacker could create files in arbitrary locations, possibly leading to code execution.

Ubuntu Security Notice USN-4934-2

Ubuntu Security Notice 4934-2 - USN-4934-1 fixed several vulnerabilities in Exim. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. CVE-2020-28026 only affected Ubuntu 16.04 ESM. It was discovered that Exim contained multiple security issues. An attacker could use these issues to cause a denial of service, execute arbitrary code remotely, obtain sensitive information, or escalate local privileges. Various other issues were also addressed.

Red Hat Security Advisory 2021-1509-01

Red Hat Security Advisory 2021-1509-01 - Jetty is a 100% Java HTTP Server and Servlet Container. Issues addressed include a resource exhaustion vulnerability.

Red Hat Security Advisory 2021-1429-01

Red Hat Security Advisory 2021-1429-01 - 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 an XML injection vulnerability.

Red Hat Security Advisory 2021-1499-01

Red Hat Security Advisory 2021-1499-01 - Red Hat Advanced Cluster Management for Kubernetes 2.2.3 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console—with security policy built in. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-1366-01

Red Hat Security Advisory 2021-1366-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.9. Issues addressed include a denial of service vulnerability.

Gentoo Linux Security Advisory 202105-01

Gentoo Linux Security Advisory 202105-1 - Multiple vulnerabilities have been found in Exim, the worst of which allows remote attackers to execute arbitrary code. Versions less than 4.94.2 are affected.

Ubuntu Security Notice USN-4935-1

Ubuntu Security Notice 4935-1 - It was discovered that the NVIDIA GPU display driver for the Linux kernel incorrectly performed access control. A local attacker could use this issue to cause a denial of service, expose sensitive information, or escalate privileges. It was discovered that the NVIDIA GPU display driver for the Linux kernel incorrectly performed reference counting. A local attacker could use this issue to cause a denial of service. Various other issues were also addressed.

Apple Security Advisory 2021-05-03-3

Apple Security Advisory 2021-05-03-3 - watchOS 7.4.1 addresses a code execution vulnerability.

Apple Security Advisory 2021-05-03-4

Apple Security Advisory 2021-05-03-4 - macOS Big Sur 11.3.1 addresses code execution and integer overflow vulnerabilities.

Apple Security Advisory 2021-05-03-1

Apple Security Advisory 2021-05-03-1 - iOS 14.5.1 and iPadOS 14.5.1 addresses code execution and integer overflow vulnerabilities.

Apple Security Advisory 2021-05-03-2

Apple Security Advisory 2021-05-03-2 - iOS 12.5.3 addresses buffer overflow, code execution, integer overflow, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-4934-1

Ubuntu Security Notice 4934-1 - It was discovered that Exim contained multiple security issues. An attacker could use these issues to cause a denial of service, execute arbitrary code remotely, obtain sensitive information, or escalate local privileges.

Ubuntu Security Notice USN-4932-1

Ubuntu Security Notice 4932-1 - 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.

Ubuntu Security Notice USN-4933-1

Ubuntu Security Notice 4933-1 - It was discovered that OpenVPN incorrectly handled certain data channel v2 packets. A remote attacker could possibly use this issue to inject packets using a victim's peer-id. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. It was discovered that OpenVPN incorrectly handled deferred authentication. When a server is configured to use deferred authentication, a remote attacker could possibly use this issue to bypass authentication and access control channel data. Various other issues were also addressed.

Ubuntu Security Notice USN-4918-3

Ubuntu Security Notice 4918-3 - USN-4918-1 fixed vulnerabilities in ClamAV. The updated package could fail to properly scan in some situations. This update fixes the problem. It was discovered that ClamAV incorrectly handled parsing Excel documents. A remote attacker could possibly use this issue to cause ClamAV to hang, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4931-1

Ubuntu Security Notice 4931-1 - Steven French discovered that Samba incorrectly handled ChangeNotify permissions. A remote attacker could possibly use this issue to obtain file name information. Bas Alberts discovered that Samba incorrectly handled certain winbind requests. A remote attacker could possibly use this issue to cause winbind to crash, resulting in a denial of service. Francis Brosnan Blázquez discovered that Samba incorrectly handled certain invalid DNS records. A remote attacker could possibly use this issue to cause the DNS server to crash, resulting in a denial of service. Various other issues were also addressed.

Kernel Live Patch Security Notice LSN-0076-1

It was discovered that the overlayfs implementation in the Linux kernel did not properly validate the application of file system capabilities with respect to user namespaces. A local attacker could use this to gain elevated privileges. Piotr Krysiuk discovered that the BPF JIT compiler for x86 in the Linux kernel did not properly validate computation of branch

displacements in some situations. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code.

Red Hat Security Advisory 2021-1478-01

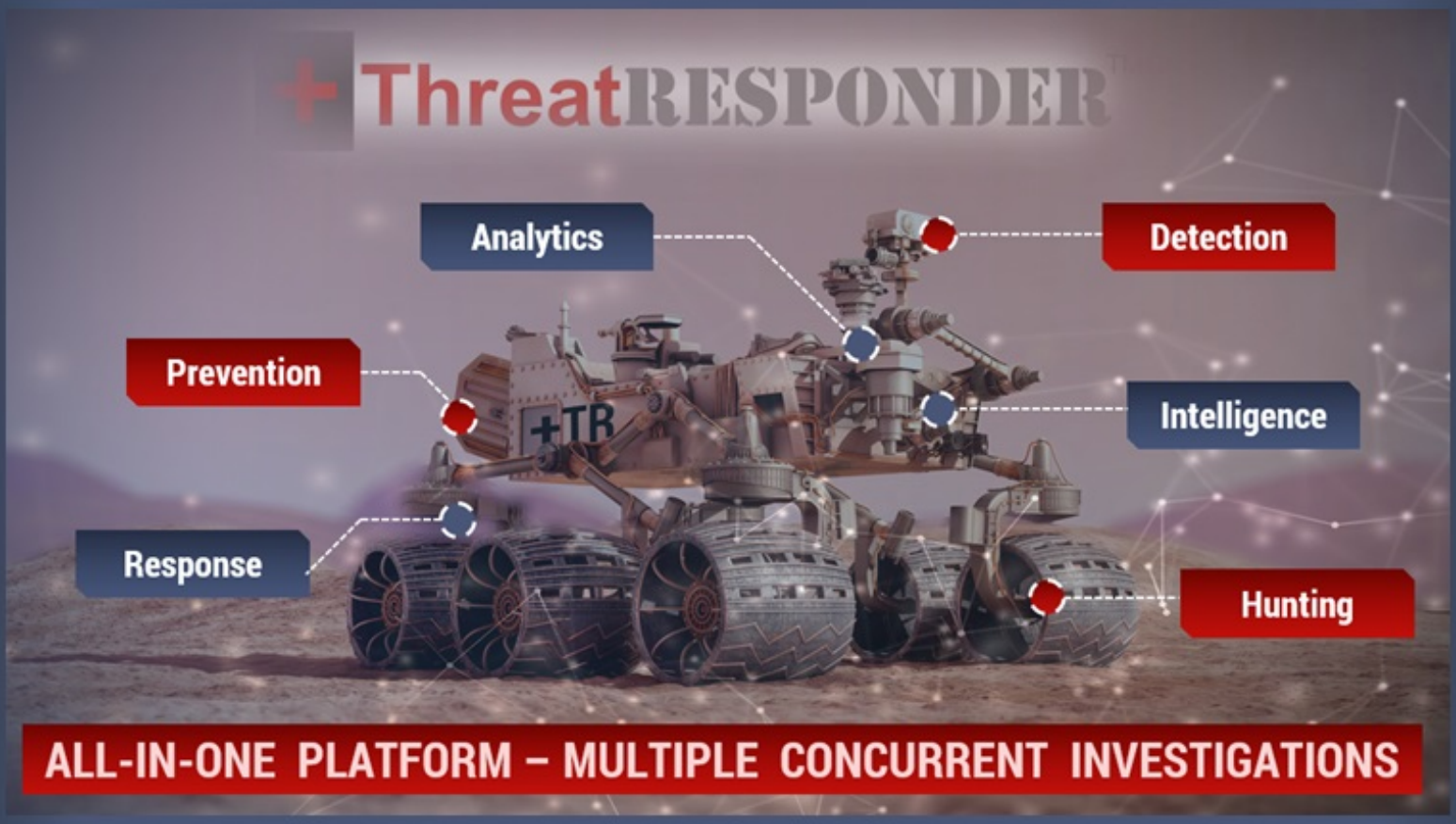
Red Hat Security Advisory 2021-1478-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly.

Are You...

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

Do DFIR Investigations Better

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



The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.1

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 Tutorials for 2021.1:

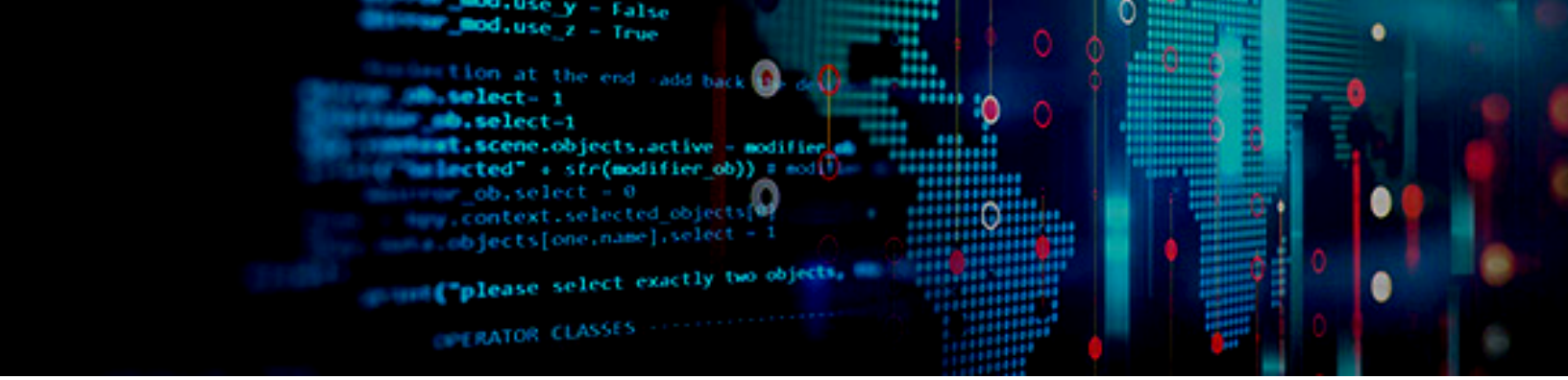
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

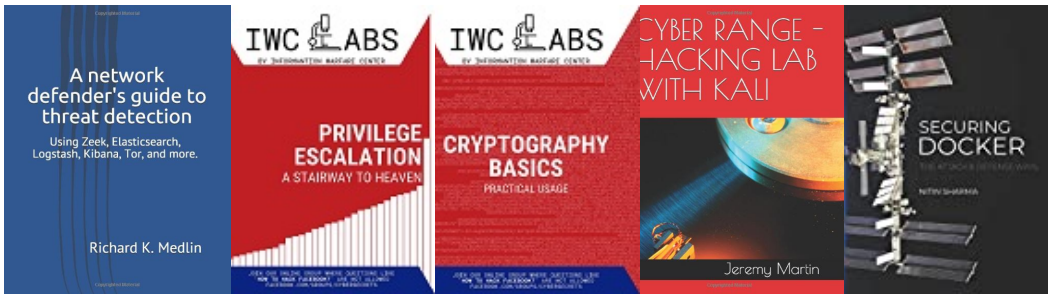


The Cyber Secrets publications on Amazon

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.

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