Mar-22-21

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

March 22, 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

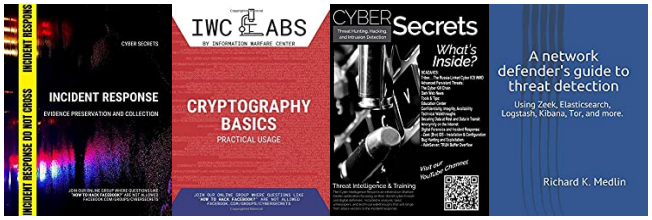
Internet Storm Center Infocon Status

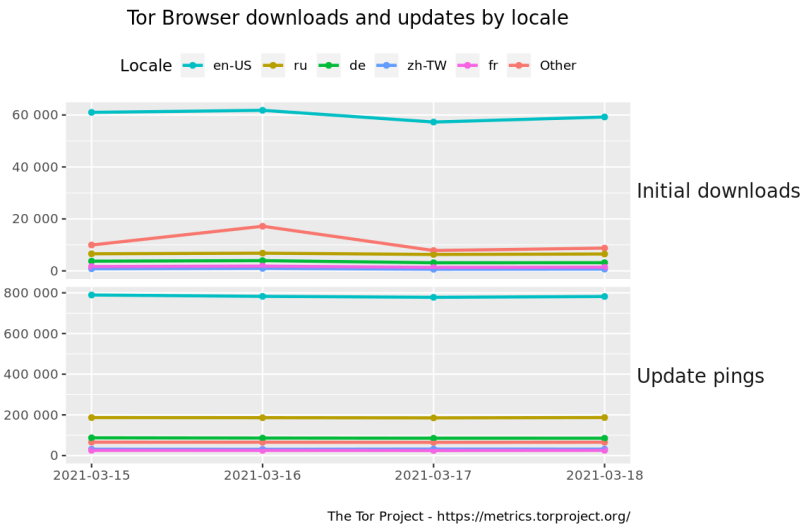
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* Netop Vision Pro Can Be Hacked To Attack Student PCs
* Russian Pleads Guilty To Tesla Ransomware Plot
* Trump Plans To Build His Own Social Media Platform
* U.S. Supreme Court Rebuffs Facebook Appeal In User Tracking Lawsuit
* Apple Devs Targeted By Malicious Xcode Project
* Zoom Screen Sharing Glitch Briefly Leaks Sensitive Data
* Swiss Hacker Indicted After Claiming Credit For Breaching Nissan, Intel
* Expert Hackers Used 11 Zero Days To Infect Windows, iOS, And Android Users
* State-Sponsored Threat Groups Target Telcos, Steal 5G Secrets
* Attackers Are Trying Hard To Backdoor iOS Developer's Macs
* Florida Mother, Daughter Charged With Hacking Homecoming Queen Election
* Google Cloud: Here Are The Six Best Vulnerabilities Security Researchers Found Last Year
* Mimecast Says SolarWinds Hackers Breached Its Network And Spied On Its Customers
* Teen Mastermind Pleads Guilty To Celeb Twitter Hack
* Exchange Cyberattacks Escalate As Microsoft Rolls One-Click Fix
* Adobe Forces Takedown Of Tweet Linking To 27-Year-Old Product
* Indian Government Is Planning Outright Ban On Cryptocurrency
* Google Warns Mac, Windows Users Of Chrome Zero-Day Flaw
* This Years-Old Microsoft Vulnerability Is Still Popular With Hackers, So Patch Now
* Encrypted Messaging App Signal Goes Down In China
* Google Faces $5 Billion Lawsuit Over Incognito Mode
* U.S. Indicts CEO Of Encrypted Phone Firm Sky
* Critical Security Hole Can Knock Smart Meters Offline
* Bitcoin Surges Past $60,000 For The First Time
* Microsoft Says Ransom Hackers Taking Advantage Of Server Flaws

Krebs on Security

* Fintech Giant Fiserv Used Unclaimed Domain
* Can We Stop Pretending SMS Is Secure Now?
* WeLeakInfo Leaked Customer Payment Info
* Microsoft Patch Tuesday, March 2021 Edition
* Warning the World of a Ticking Time Bomb
* A Basic Timeline of the Exchange Mass-Hack
* At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software
* Three Top Russian Cybercrime Forums Hacked
* Microsoft: Chinese Cyberspies Used 4 Exchange Server Flaws to Plunder Emails
* Payroll/HR Giant PrismHR Hit by Ransomware?

Dark Reading

* On the Road to Good Cloud Security: Are We There Yet?
* New Malware Hidden in Apple IDE Targets macOS Developers
* Verkada Attacker Charged With Wire Fraud, Conspiracy in US
* SolarWinds-Linked Attackers Target Microsoft 365 Mailboxes
* Russian Man Pleads Guilty in Thwarted Tesla Hack
* How Us Shady Geeks Put Others Off Security
* Tech Vendors' Lack of Security Transparency Worries Firms
* Facebook Expands Security Key Support to iOS & Android
* Women's History Month: Making Mentorship Meaningful
* New CopperStealer Malware Hijacks Social Media Accounts
* FBI: Business Email Compromise Cost $1.8B in 2020
* Beware the Package Typosquatting Supply Chain Attack
* What CISOs Can Learn From Big Breaches: Focus on the Root Causes
* Edge Poll: XDR Plans
* Ransom Payments Have Nearly Tripled
* Mimecast Says SolarWinds Attackers Accessed Its Source Code Repositories
* RDP Attacks Persist Near Record Levels in 2021
* CISA Issues Advisory on TrickBot Campaigns
* Teen Behind Twitter Hack Agrees to Three Years in Prison
* COVID, Healthcare Data & the Dark Web: A Toxic Stew

The Hacker News

* Popular Netop Remote Learning Software Found Vulnerable to Hacking
* Critical RCE Vulnerability Found in Apache OFBiz ERP Software-Patch Now
* Critical F5 BIG-IP Bug Under Active Attacks After PoC Exploit Posted Online
* Tesla Ransomware Hacker Pleads Guilty; Swiss Hacktivist Charged for Fraud
* Hackers Infecting Apple App Developers With Trojanized Xcode Projects
* New Zoom Screen-Sharing Bug Lets Other Users Access Restricted Apps
* Critical RCE Flaw Reported in MyBB Forum Software-Patch Your Sites
* How to Successfully Pursue a Career in Malware Analysis
* Why Cached Credentials Can Cause Account Lockouts and How to Stop it
* Google Reveals What Personal Data Chrome and Its Apps Collect On You
* Flaws in Two Popular WordPress Plugins Affect Over 7 Million Websites
* Mimecast Finds SolarWinds Hackers Stole Some of Its Source Code
* [Webinar] Oy Vey, We Hired a Large, Hairy Hacker…
* 18-Year-Old Hacker Gets 3 Years in Prison for Massive Twitter 'Bitcoin Scam' Hack
* Apple May Start Delivering Security Patches Separately From Other OS Updates

Security Week

* Adobe Patches Critical ColdFusion Security Flaw
* Electricity Distribution Systems at Increasing Risk of Cyberattacks, GAO Warns
* Researchers Raise Alarm for F5 BIG-IP Malware Attacks
* US Sentences Russian, North Macedonian in Cyber Fraud Case
* TikTok Pays Out $11,000 Bounty for High-Impact Exploit
* Cybersecurity M&A Roundup for Week of Mar. 15, 2021
* Cyber Attack Tied to China Boosts Development Bank's Chief
* China Slams US Plan to Expel Phone Carriers in Tech Clash
* Google: Sophisticated APT Group Burned 11 Zero-Days in Mass Spying Operation
* Russian Man Pleads Guilty to Role in Attempt to Plant Malware on Tesla Systems
* Microsoft Defender Antivirus Now Protects Users Against Ongoing Exchange Attacks
* Facebook Paid Out $50K for Vulnerabilities Allowing Access to Internal Systems
* Here's How Security Flaws in GE Relays Could Be Exploited in Real World Attacks
* US Charges Swiss 'Hacktivist' for Data Theft and Leaks
* Finland IDs Hackers Linked to Parliament Spying Attack
* New XcodeSpy Mac Malware Targets Software Developers
* How Your Security Approach Can Drive Resiliency in the Industrial Economy
* Five Months After Takedown Attempt, CISA and FBI Warn of Ongoing TrickBot Attacks
* Facebook Now Lets Mobile Users Secure Accounts with Security Keys
* Healthcare IoT Security Firm Cylera Closes $10 Million Series A Round

Infosecurity Magazine

* UK Heading for "Catastrophic" Digital Skills Shortage
* New Cybersecurity Programs to Protect US Energy
* UK Govt Department Loses 306 Mobiles and Laptops in Two Years
* Firms Urged to Patch as Attackers Exploit Critical F5 Bugs
* FBI: State and Local Governments Losing Millions to BEC
* Musk Denies Tesla Security Claims After Chinese Military Ban
* US Indicts Software Engineer
* APT31 Fingered for Cyber-Attack on Finnish Parliament
* Protective Intelligence Honors Launched
* ESET Exposes Malware Disguised as Clubhouse App
* Russian Man Pleads Guilty in Tesla Extortion Plot
* Website Builders Take Hands-Off Approach to Fake News

KnowBe4 Security Awareness Training Blog RSS Feed

* Not Your Father's Tech Support Scam
* Many Ways To Hack MFA
* FBI Warns that PYSA Ransomware is Targeting Schools
* [NEW FEATURE] Enhance Your Users' Learning Experience with Optional Learning
* Mom Charged in Deepfake Cheerleading Plot
* Another Tax Season, Another Opportunity for Scams
* Researchers Have Their Eye on Malicious Clones of Android Apps That Put Devices at Risk
* FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Losses Exceed $4.2
* [EYE-OPENER] USA CISA Advisory on Trickbot Campaigns: Phishing Training For Employees
* Ransomware Attacks Are Growing More Costly and Effective by the Day

ISC2.org Blog

* Healthcare Security - Security with Life and Death Consequences
* How Cloud Security Certification Can Give Your Career a Buzz
* Positive Interest in STEM: The latest side-effect of the pandemic
* Cybersecurity Predictions for 2021 from the (ISC)² Community of Security Professionals (Part 3)
* Latest CrowdStrike Global Threat Report Finds Healthcare Orgs in the Social Engineering Crosshairs

HackRead

* Russian hacker pleads guilty to planting malware in Tesla Gigafactory
* New malware "BlackRock" disguised as Android Clubhouse app
* US charges Swiss hacker behind massive Verkada security camera hack
* New macOS malware XcodeSpy found sneaking into spy on victims
* Mastermind of 2020's top celebrity Twitter hack sentenced to 3 years
* Sensitive data from US shipping management software firm exposed online
* Hacker dumps Guns.com database with customers, admin data

Koddos

* Russian hacker pleads guilty to planting malware in Tesla Gigafactory
* New malware "BlackRock" disguised as Android Clubhouse app
* US charges Swiss hacker behind massive Verkada security camera hack
* New macOS malware XcodeSpy found sneaking into spy on victims
* Mastermind of 2020's top celebrity Twitter hack sentenced to 3 years
* Sensitive data from US shipping management software firm exposed online
* Hacker dumps Guns.com database with customers, admin data

Naked Security

* Serious Security: Mac "XcodeSpy" backdoor takes aim at Xcode devs
* S3 Ep24: How not to get snooped, scammed or hoaxed [Podcast]
* Serious Security: The Linux kernel bugs that surfaced after 15 years
* Bitcoin scammer who hacked celeb Twitter accounts gets 3 years
* S3 Ep 23.5: An interview with cybersecurity expert John Noble CBE [Podcast]
* Naked Security Live - HAFNIUM explained in plain English
* How confidential are your calls? This iPhone app shared them with everyone
* S3 Ep23: Hafnium happenings, I see you, and Pythonic poison [Podcast]
* 150,000 security cameras allegedly breached in "too much fun" hack
* Serious Security: Webshells explained in the aftermath of HAFNIUM attacks

Threat Post

* Critical F5 BIG-IP Flaw Now Under Active Attack
* Office 365 Phishing Attack Targets Financial Execs
* Bogus Android Clubhouse App Drops Credential-Swiping Malware
* CopperStealer Malware Targets Facebook and Instagram Business Accounts
* Fiserv Forgets to Buy Domain It Used as System Default
* Trojanized Xcode Project Slips MacOS Malware to Apple Developers
* Zoom Screen-Sharing Glitch 'Briefly' Leaks Sensitive Data
* Security Researcher Hides ZIP, MP3 Files Inside PNG Files on Twitter
* Tutor LMS for WordPress Open to Info-Stealing Security Holes
* Cisco Plugs Security Hole in Small Business Routers

Null-Byte

* This Python Bundle Can Teach You Everything You Need to Know
* How to Use a Directional Antenna with ESP8266-Based Microcontroller
* Master the Internet of Things with This Certification Bundle
* There Are Hidden Wi-Fi Networks All Around You - These Attacks Will Find Them
* Rank Up in Google Searches with This SEO Couse Bundle
* How to Generate Crackable Wi-Fi Handshakes with an ESP8266-Based Test Network
* This Master Course Bundle on Coding Is Just $34.99
* How to Automate Remote SSH Control of Computers with Expect Scripts
* This VPN Will Give You a Lifetime of Security for Just $18
* How to Write Your Own Bash Scripts to Automate Tasks on Linux

IBM Security Intelligence

* The Next-Gen Cyber Range: Bringing Incident Response Exercises to the Cloud
* Loving the Algorithm: User Risk Management and Good Security Hygiene
* Reaching Strategic Outcomes With an MDR Service Provider: Part 5
* Retail Cybersecurity: How to Protect Your Customer Data
* Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts
* Top 10 Cybersecurity Vulnerabilities of 2020
* Why the Demand for Application Development Security Skills Is Exploding
* Innovation Through Diverse Thinking: Amplifying Gender Diversity and Shrinking the Skills Gap
* Cloud Native Tools Series Part 2: Understand Your Responsibilities
* Cloud Clarity: Adding Security and Control to the AWS Shared Responsibility Model

InfoWorld

* Why migrating to .Net 5 is worth the effort
* Authorization is the next big technical challenge
* 7 common cloud problems and how to fix them
* Move over Java, JavaScript is the new WORA. Or is it?
* How to pick cloud dev tools and infrastructure
* Apple proposes actor model for Swift concurrency
* Go programming gains in the workplace
* Knowledge management for agile and devops teams
* BlazingSQL review: Fast ETL for GPU-based data science
* PeachPie PHP to .NET project reaches 1.0 milestone

C4ISRNET - Media for the Intelligence Age Military

* L3Harris selected for F-16 electronic warfare protection system
* Pentagon, Intel partner to make more US microchips for military
* Israel starts research center for GPS-free navigation
* Air Force begins construction of new space environment lab
* Air Force curtails ABMS demos after budget slashed by Congress
* L3Harris sees opportunities in Pentagon's growing responsive space business
* Senators show support for increasing US Southern Command intelligence assets
* Army AI helper would suggest actions in multidomain fights
* Top Pentagon research arm combats 'aggressive' foreign investors
* Army participates in first-of-its-kind cyber exercise

The Hacker Corner

Conferences

* 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
* We've Moved!

Google Zero Day Project

* In-the-Wild Series: October 2020 0-day discovery
* Déjà vu-lnerability

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.

* UMassCTF 2021
* VolgaCTF 2021 Qualifier
* ALLES! CTF 2021 HW Edition
* ångstromCTF 2021
* Shakti CTF
* JUST CTF Finals 2021
* b01lers CTF
* RITSEC CTF 2021
* Midnight Sun CTF 2021 Quals
* HackPack CTF 2021

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

* Orasi: 1
* Crossroads: 1
* Grotesque: 1
* Gigachad: 1
* DriftingBlues: 3

Tools & Techniques

Packet Storm Security Tools Links

* TOR Virtual Network Tunneling Tool 0.4.5.7
* American Fuzzy Lop plus plus 3.11c
* Hydra Network Logon Cracker 9.2
* Wireshark Analyzer 3.4.4
* scanlogd 2.2.8
* Raptor WAF 0.62
* SQLMAP - Automatic SQL Injection Tool 1.5.3
* OpenSSH 8.5p1
* Zeek 4.0.0
* Suricata IDPE 6.0.2

Kali Linux Tutorials

* Diceware Password Generator : Generate High Entropy Passwords
* Darkdump : Search The Deep Web Straight From Your Terminal
* Rafel Rat : Android Rat Written In Java
* AnonX : An Encrypted File Transfer Via AES-256-CBC
* Strafer : A Tool To Detect Potential Infections In Elasticsearch Instances
* Turbo Intruder : A Burp Suite Extension For Sending Large Numbers
* Lazy-RDP : Script For AutomRDPatic Scanning And Brute-Force
* SnitchDNS : Database Driven DNS Server With A Web UI
* Genisys : Powerful Telegram Members Scraping and Adding Toolkit
* Confused : Tool To Check For Dependency Confusion Vulnerabilities

GBHackers Analysis

* MuddyWater Hacker Group Utilize Legitimate File-Sharing Service to Distribute Malware
* Netgear JGS516PE Ethernet Switch Flaws let Attackers Execute Remote Code
* Google Fixed yet Another Actively Exploited zero-day Vulnerability in the Chrome Browser
* Iranian Hackers Uses ScreenConnect Remote Access Tool to Target Government Agencies
* Linux Kernel Vulnerability that Allows Local Attackers to Escalate Privileges

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 187: When to Stop Looking for Evidence - Part 3
* Day 2 Wrap-Up Panel | SANS CTI Summit 2-21
* Will they Read my Reports? - Creating Value Driven Reports | Christopher Lopez | SANS CTI Summit
* Quantifying Intelligence: Increasing Executives IQ | Colin Conner | SANS CTI Summit 2021

Defcon Conference

* DEF CON 2020 NYE MISS JACKALOPE DJ Music Video
* DEF CON 2020 NYE ZEE DJ Music Video
* DEF CON 2020 NYE Yesterday & Tomorrow DJ Music Video
* DEF CON 2020 NYE Skittish & Bus DJ Music Video

Hak5

* Thousands of Enterprise Surveillance Cameras Hacked - ThreatWire
* Building DIY Lithium Battery Packs w/Glytch Pt1
* Microsoft Exchange Zero Days Actively Exploited - Update ASAP - ThreatWire

The PC Security Channel [TPSC]

* Ryuk Ransomware: Live Demo and Analysis
* Cyberpunk's Company Hacked by HelloKitty Ransomware: Live Demo

Eli the Computer Guy

* SMART SPEAKERS LISTENING - DETECT HEART RHYTHM
* YOUTUBE "CHECKS" - AI Screening of Video Uploads
* FUTURE CRIME PREVENTION (garbo)
* TWITTER CENSORING WORLD LEADERS

Security Now

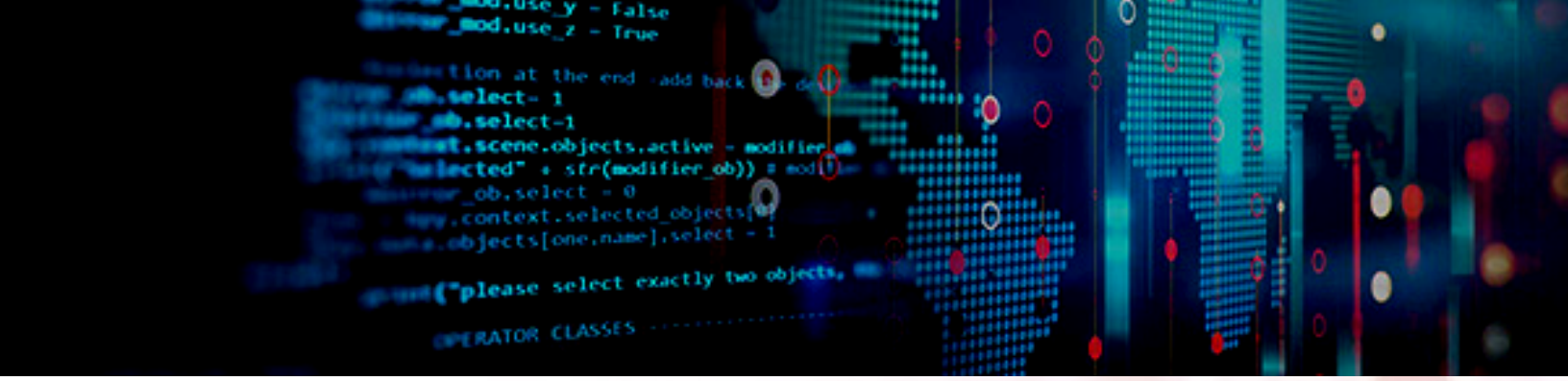
* ProxyLogon - New Chrome 0-Day, Patch Tuesday Redux, Spectre Comes to Chrome
* Hafnium - Dependency Confusion, Intel Side Channel Attacks, Crispy Subtitles From Lay's

Troy Hunt

* Weekly Update 235

Intel Techniques: The Privacy, Security, & OSINT Show

* 210-Lessons in Online Purchases & Domain Expiration
* 209-New OSINT Tactics



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

* 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
* Turkey Dog Continues to Target Turkish Speakers with RAT Trojans via COVID Lures
* Threat Hunting in a Post-WHOIS World
* The Business of LogoKit: The Actors and Marketing Behind a Popular Phishing Tool
* 2020 Mobile App Threat Landscape: New Threats Arise, But the Ecosystem Got Safer
* LogoKit: Simple, Effective, and Deceptive
* Attacks on the Capitol Showed the Pitfalls of Having a Narrow View of the Internet
* New Analysis Puts Magecart Interconnectivity into Focus

FireEye

* SOC Automation with InsightIDR and InsightConnect: Three Key Use Cases to Explore to Optimize Your Se
* Metasploit Wrap-Up
* Top Security Trends Driving Threat Detection and Response Priorities Today
* F5 Discloses Eight Vulnerabilities-Including Four Critical Ones-in BIG-IP Systems
* Rapid7 Announces Release of New tCell Amazon CloudFront Agent
* Metasploit Wrap-Up
* Introducing the 2020 Vulnerability Intelligence Report: 50 CVEs that Made Headlines in 2020
* InsightIDR's NTA Capabilities Expanded to AWS
* Patch Tuesday - March 2021
* What's New in DivvyCloud by Rapid7: February 2021 Feature Releases

Proof of Concept (PoC) & Exploits

Packet Storm Security

* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Insufficient Session Expiration
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Privilege Escalation
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Configuration Download
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Device Reboot
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Factory Reset
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Unauthenticated Log Disclosure
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Insecure Direct Object Reference
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Remote Code Execution
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Weak Default WiFi Password Algorithm
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Hard-Coded Credentails / Shell Access
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Authentication Bypass
* KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 Authenticated Command Injection
* Win32k ConsoleControl Offset Confusion
* VMware View Planner 4.6 Remote Code Execution
* SOYAL 701Client 9.0.1 Insecure Permissions
* SOYAL 701Server 9.0.1 Insecure Permissions
* SOYAL Biometric Access Control System 5.0 Cross Site Request Forgery
* SOYAL Biometric Access Control System 5.0 Weak Default Credentials
* SOYAL Biometric Access Control System 5.0 Master Code Disclosure
* VestaCP 0.9.8 Command Injection
* Eclipse Mosquitto MQTT Broker 2.0.9 Unquoted Service Path
* Profiling System For Human Resource Management 1.0 Remote Code Execution
* Boonex Dolphin 7.4.2 Cross Site Scripting
* LiveZilla Server 8.0.1.0 Cross Site Scripting
* Plone CMS 5.2.3 Cross Site Scripting

CXSecurity

* VMware View Planner 4.6 Remote Code Execution
* Win32k ConsoleControl Offset Confusion
* Profiling System For Human Resource Management 1.0 Remote Code Execution
* Microsoft Exchange 2019 SSRF / Arbitrary File Write
* FastStone Image Viewer 7.5 Buffer Overflow
* Windows Server 2012 SrClient DLL Hijacking
* SonLogger 4.2.3.3 Shell Upload

Proof of Concept (PoC) & Exploits

Exploit Database

* [local] OSAS Traverse Extension 11 - 'travextensionhostsvc' Unquoted Service Path
* [dos] ProFTPD 1.3.7a - Remote Denial of Service
* [webapps] MyBB 1.8.25 - Chained Remote Command Execution
* [remote] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Weak Default WiFi Password Algorithm
* [local] MacPaw Encrypto 1.0.1 - 'Encrypto Service' Unquoted Service Path
* [webapps] WordPress Plugin Delightful Downloads Jquery File Tree 1.6.6 - Path Traversal
* [local] Winpakpro 4.8 - 'WPCommandFileService' Unquoted Service Path
* [local] Winpakpro 4.8 - 'ScheduleService' Unquoted Service Path
* [local] Winpakpro 4.8 - 'GuardTourService' Unquoted Service Path
* [local] SAPSetup Automatic Workstation Update Service 750 - 'NWSAPAutoWorkstationUpdateSvc' Unquoted

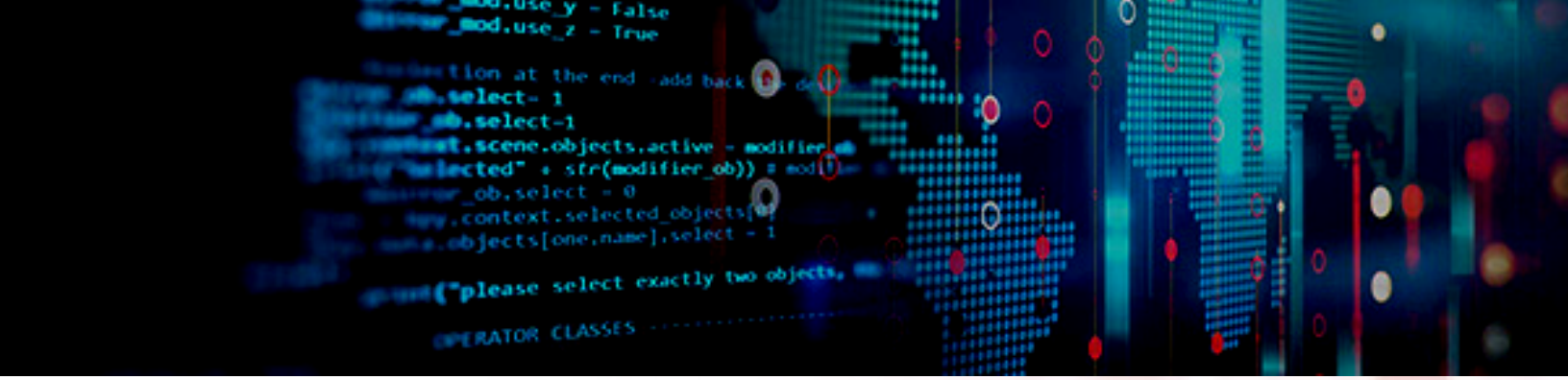
* [webapps] Online News Portal 1.0 - 'Multiple' Stored Cross-Site Scripting
* [webapps] Online News Portal 1.0 - 'name' SQL Injection
* [webapps] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Config Download (Unauthenticated)
* [dos] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Device Reboot (Unauthenticated)
* [webapps] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Factory Reset (Unauthenticated)
* [webapps] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Remote Code Execution
* [remote] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Hard coded Credentials Shell Access
* [webapps] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Authentication Bypass
* [webapps] KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Command Injection (Authenticated)
* [local] SOYAL 701 Client 9.0.1 - Insecure Permissions
* [local] SOYAL 701 Server 9.0.1 - Insecure Permissions
* [webapps] SOYAL Biometric Access Control System 5.0 - 'Change Admin Password' CSRF
* [webapps] SOYAL Biometric Access Control System 5.0 - Master Code Disclosure
* [webapps] VestaCP 0.9.8 - 'v_sftp_licence' Command Injection

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

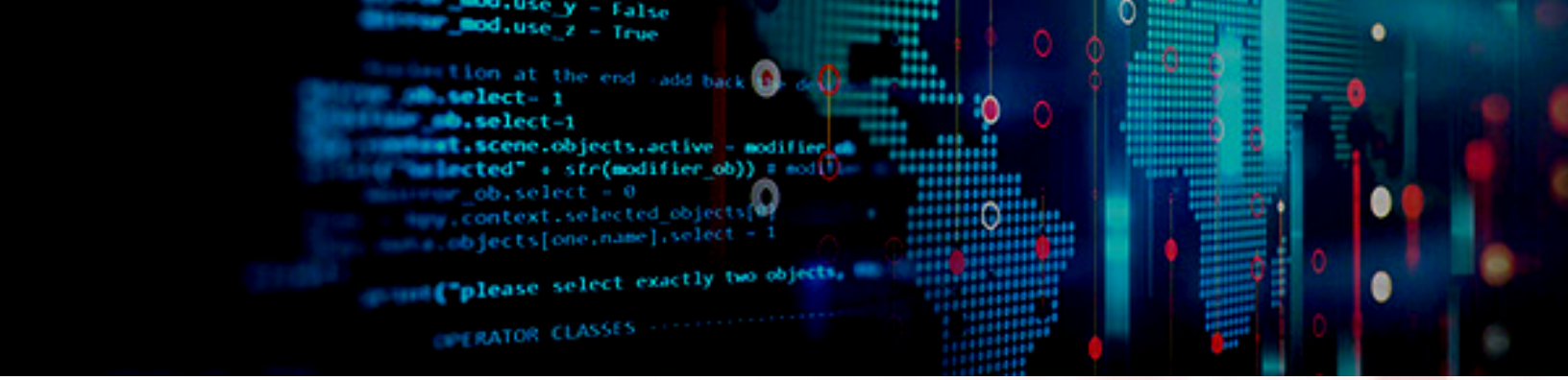
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.jdih.balangankab.go.id/read.txt
https://www.jdih.balangankab.go.id/read.txt notified by Mr.L3RB1
http://pariwisata.balangankab.go.id/read.txt
http://pariwisata.balangankab.go.id/read.txt notified by Mr.L3RB1
https://kesbangpol.balangankab.go.id/read.txt
https://kesbangpol.balangankab.go.id/read.txt notified by Mr.L3RB1
https://dishub.balangankab.go.id/read.txt
https://dishub.balangankab.go.id/read.txt notified by Mr.L3RB1
http://kelurahanpartim.balangankab.go.id/read.txt
http://kelurahanpartim.balangankab.go.id/read.txt notified by Mr.L3RB1
http://dinaskearsipan.balangankab.go.id/read.txt
http://dinaskearsipan.balangankab.go.id/read.txt notified by Mr.L3RB1
http://balangankab.go.id/read.txt
http://balangankab.go.id/read.txt notified by Mr.L3RB1
https://mediacenter.balangankab.go.id/read.txt
https://mediacenter.balangankab.go.id/read.txt notified by Mr.L3RB1
https://dpmptsp.balangankab.go.id/read.txt
https://dpmptsp.balangankab.go.id/read.txt notified by Mr.L3RB1
http://disdukcapil.balangankab.go.id/read.txt
http://disdukcapil.balangankab.go.id/read.txt notified by Mr.L3RB1
http://clusterqassim.gov.sa
http://clusterqassim.gov.sa notified by FzRaeL
http://www.wakf.go.tz/Hey.php
http://www.wakf.go.tz/Hey.php notified by Smmart_H4x0r
https://www.fbr.gov.pk/Moroccohack.html
https://www.fbr.gov.pk/Moroccohack.html notified by Moroccan Revolution
http://download1.fbr.gov.pk/Moroccohack.html
http://download1.fbr.gov.pk/Moroccohack.html notified by Moroccan Revolution
https://www.comunecalascibetta.gov.it/Moroccohack.html
https://www.comunecalascibetta.gov.it/Moroccohack.html notified by Moroccan Revolution
http://www.pa-bangkinang.go.id/idolsec.txt
http://www.pa-bangkinang.go.id/idolsec.txt notified by FRK48
http://pn-brebes.go.id/idolsec.txt
http://pn-brebes.go.id/idolsec.txt notified by FRK48



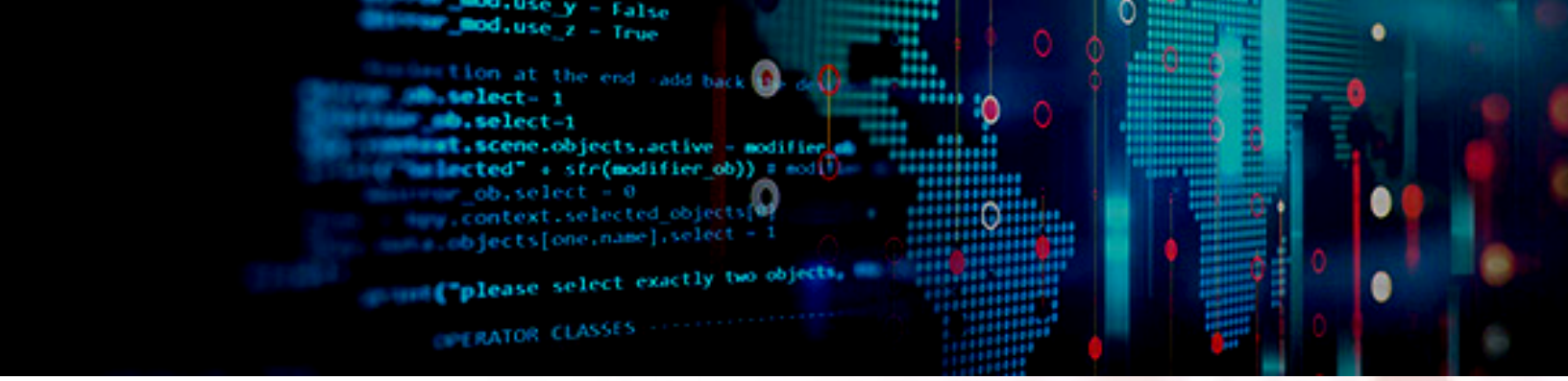
Dark Web News

Darknet Live

Man Bought MDMA on the Darkweb and Sold It to an Informant
A Bay Area man, while out on bond after buying MDMA on the darkweb, sold MDMA to a confidential informant. (via darknetlive.com)
Five Arrested for Ordering Marijuana on the Darkweb
Police in France arrested five people for allegedly ordering 500 grams of marijuana on the darkweb. (via darknetlive.com)
Encrypted Messaging App Signal Might Be Banned in China
Signal, the encrypted messaging application used by millions, appears to be the latest target of the "Great Firewall" in China. (via darknetlive.com)
Man Shipped 340 Grams of Fentanyl Pills Across the U.S.
A former resident of California admitted he had shipped a package of fentanyl pills from California to Pennsylvania. (via darknetlive.com)

Dark Web Link

What You Should Make Sure When Buying From Dark Web
Buying from dark web has been one of the central questions asked about operating the darknet as people around the world mostly use it to purchase illegal products. Since the darknet is deemed a place under the rock, people are sometimes nervous about conducting something unusual. This brings us to this article, where we carefully [...] The post What You Should Make Sure When Buying From Dark Web appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
World Market: An Alternative Darknet Marketplace For The World
In the era of continuous dark web market rush, finding an autonomous darknet marketplace that stays strong on its claims could be challenging. The challenges seemed to have toned down with the World Market's advent, deemed to be the ultimate alternative darknet market for the world. What Do World Market Boasts About? When it comes [...] The post World Market: An Alternative Darknet Marketplace For The World appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Signal: China Probably Blocked Access To The Encrypted Messaging Service
Mainland China may have blocked access to the renowned encrypted messaging service, Signal. The international social media service seems to have ceased in a country where the government rigidly controls the information flow. The Signal app users residing within China had to connect to a VPN or Virtual Private Network that permits them to get [...] The post Signal: China Probably Blocked Access To The Encrypted Messaging Service appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates
* Using CHIRP to Detect Post-Compromise Threat Activity in On-Premises Environments
* TTP Table for Detecting APT Activity Related to SolarWinds and Active Directory/M365 Compromise
* CISA-FBI Joint Advisory on TrickBot Malware
* Microsoft Releases Exchange On-premises Mitigation Tool
* Google Releases Security Updates for Chrome
* Updates on Microsoft Exchange Server Vulnerabilities
* FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server
* AA21-077A: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
* AA21-076A: TrickBot Malware
* Vulnerability Summary for the Week of March 15, 2021
* Vulnerability Summary for the Week of March 8, 2021

Zero Day Initiative Advisories

ZDI-CAN-12978: Delta Industrial Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-13028: Delta Industrial Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-13030: Delta Industrial Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-13036: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'peterjson of RedTeam@VNG Corporation' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-13196: 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 SecZone' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until

2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12959: 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 'garmin' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12956: 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 'garmin' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13199: Siemens

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12592: Schneider Electric

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13060: 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 SecZone' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13468: 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 'Brian Gorenc of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-18, 4 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13031: Delta Industrial Automation

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13033: Delta Industrial Automation

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13363: Trend Micro

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 'Simon Zuckerbraun - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13032: Delta Industrial Automation

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was

reported to the affected vendor on: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13456: Cisco

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: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13458: Cisco

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: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13104: Oracle

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 'Quynh Le of VNPT ISC' was reported to the affected vendor on: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13455: Cisco

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: 2021-03-17, 5 days ago. The vendor is given until 2021-07-15 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-13417: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-16, 6 days ago. The vendor is given until 2021-07-14 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-13414: Siemens

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-16, 6 days ago. The vendor is given until 2021-07-14 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-13413: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-16, 6 days ago. The vendor is given until 2021-07-14 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-13412: Siemens

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-16, 6 days ago. The vendor is given until 2021-07-14 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-13418: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-16, 6 days ago. The vendor is given until 2021-07-14 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

Red Hat Security Advisory 2021-0940-01

Red Hat Security Advisory 2021-0940-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-0933-01

Red Hat Security Advisory 2021-0933-01 - Django is a high-level Python Web framework that encourages rapid development and a clean, pragmatic design. It focuses on automating as much as possible and adhering to the DRY principle.

Red Hat Security Advisory 2021-0931-01

Red Hat Security Advisory 2021-0931-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. OVN, the Open Virtual Network, is a system to support virtual network abstraction. OVN complements the existing capabilities of OVS to add native support for virtual network abstractions, such as virtual L2 and L3 overlays and security groups. Issues addressed include buffer overflow and integer overflow vulnerabilities.

Red Hat Security Advisory 2021-0934-01

Red Hat Security Advisory 2021-0934-01 - KVM is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm-rhev packages provide the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4881-1

Ubuntu Security Notice 4881-1 - It was discovered that containerd incorrectly handled certain environment variables. Contrary to expectations, a container could receive environment variables defined for a different container, possibly containing sensitive information.

Red Hat Security Advisory 2021-0937-01

Red Hat Security Advisory 2021-0937-01 - An update for rubygem-em-http-request is now available for Red Hat OpenStack Platform 13 (Queens). Issues addressed include a man-in-the-middle vulnerability.

Red Hat Security Advisory 2021-0916-01

Red Hat Security Advisory 2021-0916-01 - A highly-available key value store for shared configuration. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0915-01

Red Hat Security Advisory 2021-0915-01 - Django is a high-level Python Web framework that encourages rapid development and a clean, pragmatic design. It focuses on automating as much as possible and adhering to the DRY principle.

Red Hat Security Advisory 2021-0922-01

Red Hat Security Advisory 2021-0922-01 - 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. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0882-01

Red Hat Security Advisory 2021-0882-01 - Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages technologies. Issues addressed include a HTTP request smuggling vulnerability.

Red Hat Security Advisory 2021-0883-01

Red Hat Security Advisory 2021-0883-01 - Perl is a high-level programming language that is commonly used for system administration utilities and web programming. Issues addressed include buffer overflow, denial of service, and integer overflow vulnerabilities.

Red Hat Security Advisory 2021-0876-01

Red Hat Security Advisory 2021-0876-01 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. Issues addressed include denial of

service, out of bounds read, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0877-01

Red Hat Security Advisory 2021-0877-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0881-01

Red Hat Security Advisory 2021-0881-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems.

Red Hat Security Advisory 2021-0878-01

Red Hat Security Advisory 2021-0878-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-0857-01

Red Hat Security Advisory 2021-0857-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include buffer overflow, denial of service, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0851-01

Red Hat Security Advisory 2021-0851-01 - The Public Key Infrastructure Core contains fundamental packages required by Red Hat Certificate System. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2021-0873-01

Red Hat Security Advisory 2021-0873-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include bypass and information leakage vulnerabilities.

Red Hat Security Advisory 2021-0860-01

Red Hat Security Advisory 2021-0860-01 - Red Hat Identity Management is a centralized authentication, identity management, and authorization solution for both traditional and cloud-based enterprise environments. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-0872-01

Red Hat Security Advisory 2021-0872-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include bypass and information leakage vulnerabilities.

Red Hat Security Advisory 2021-0856-01

Red Hat Security Advisory 2021-0856-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, denial of service, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0874-01

Red Hat Security Advisory 2021-0874-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include bypass and information leakage vulnerabilities.

Red Hat Security Advisory 2021-0862-01

Red Hat Security Advisory 2021-0862-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-0885-01

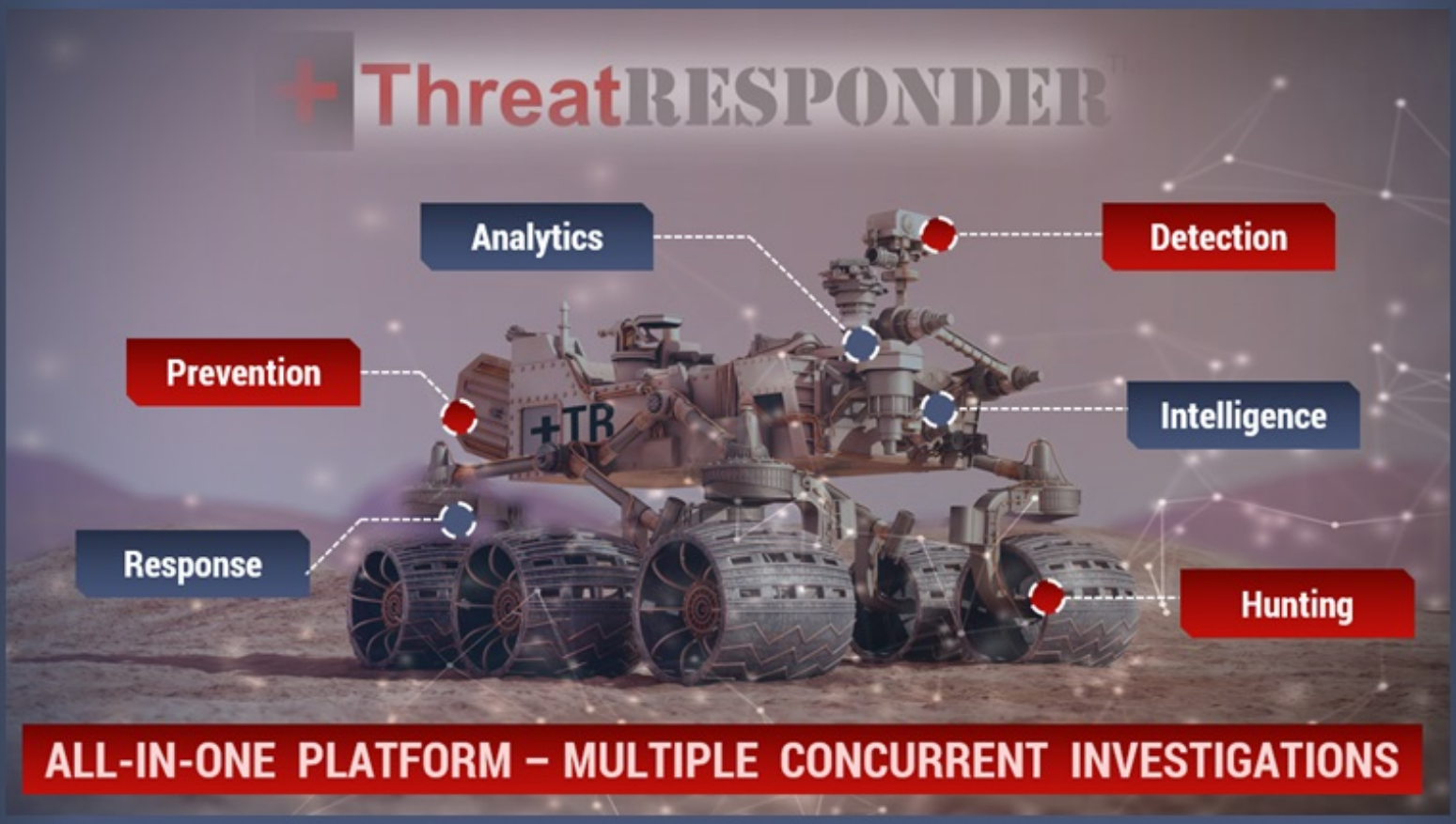
Red Hat Security Advisory 2021-0885-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.3.6 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.3.5, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.3.6 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include bypass and information leakage vulnerabilities.

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:

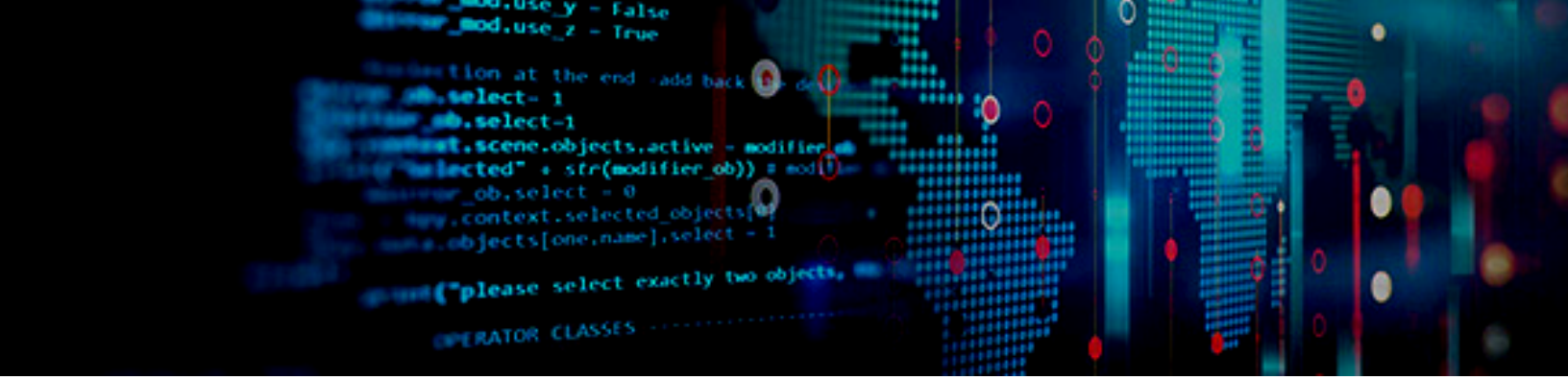
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

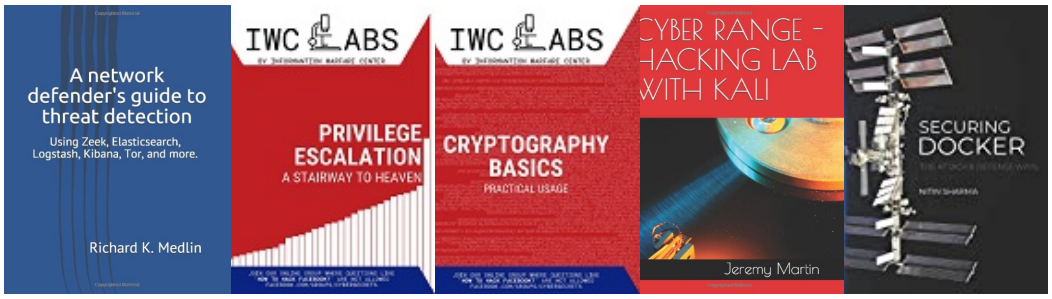


The Cyber Secrets publications on Amazon

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