Mar-18-21

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 18, 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

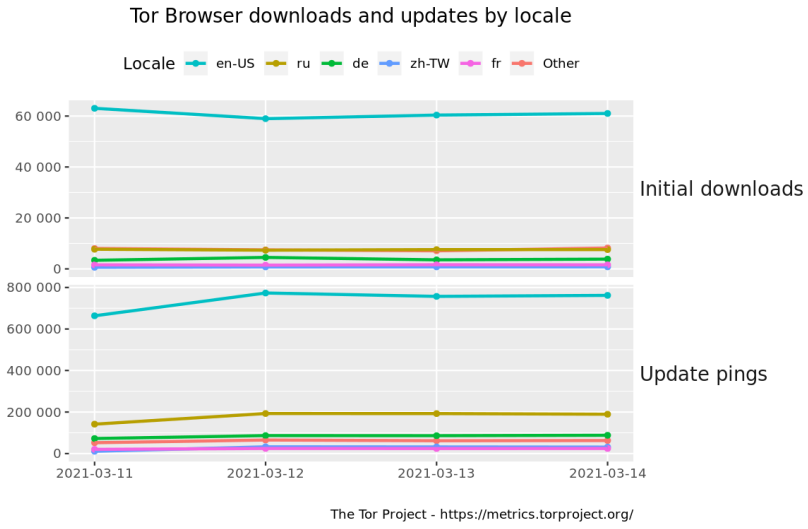
Internet Storm Center Infocon Status

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 in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

* CSI Linux has a tools update. You can update the tools in a terminal by typing
wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh

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

Index of Sections

Packet Storm Security

* 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
* Linux Systems Under Attack By New RedXOR Malware
* Legislators Work Towards Breach Law Requiring Notification
* Critics Fume After Github Removes Exploit Code For Exchange Vulnerabilities
* F5, CISA Warn Of Critical BIG-IP And BIG-IQ RCE Bugs
* This Trojan Malware Is Now Your Biggest Security Headache
* Vexing Mystery Surrounds 0-Day Attacks On Exchange Servers
* Bounty Hunter Hackers Earn $40m Thanks To Pandemic
* Linux Foundation Lauches Software Signing Service
* Microsoft Patch Tuesday Updates Fix 14 Critical Bugs
* OVHcloud Data Centers Engulfed In Flames
* Hack Of 150,000 Cameras Investigated By Verkada
* Chinese Hackers Targeted SolarWinds Customers In Parallel With Russian Op

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

* 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
* Enterprises Wrestle With Executive Social Media Risk Management
* 7 Tips to Secure the Enterprise Against Tax Scams
* Chinese APT Targets Telcos in 5G-Related Cyber-Espionage Campaign
* IronNet Cybersecurity to Go Public in Merger
* Microsoft Releases Mitigation Tool for On-Premises Exchange Servers
* Best Practices for Securing Service Accounts
* Software Development Security Firm Argon Announces Launch
* Metasploit Creator HD Moore's New Startup Raises $5M
* Combating Call Center Fraud in the Age of COVID
* DDoS's Evolution Doesn't Require a Security Evolution
* Buffalo Public Schools Cancel Classes Due to Ransomware
* CISA Updates Microsoft Exchange Advisory to Include China Chopper
* Lookout Acquires SASE Cloud Provider CipherCloud
* Name That Toon: Something Seems Afoul
* How to Choose the Right Cybersecurity Framework

The Hacker News

* 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
* New Mirai Variant and ZHtrap Botnet Malware Emerge in the Wild
* Use This One-Click Mitigation Tool from Microsoft to Prevent Exchange Attacks
* Rising Demand for DDoS Protection Software Market By 2020-2028
* CEO of Encrypted Chat Platform Indicted for Aiding Organised Criminals
* CompTIA Security Certification Prep - Lifetime Access for just $30
* Another Google Chrome 0-Day Bug Found Actively Exploited In-the-Wild
* Researchers Spotted Malware Written in Nim Programming Language
* Hackers Are Targeting Microsoft Exchange Servers With Ransomware

Security Week

* Ripoff Report Hacker Gets 12 Months in Prison
* Polish State Websites Hacked and Used to Spread False Info
* Chinese Cyberspies Target Telecom Companies in America, Asia, Europe
* Debunking the Top User Experience, Security, and Fraud Myths
* Vulnerability Management Firm Vulcan Cyber Raises $21 Million
* New Mirai Variant Leverages 10 Vulnerabilities to Hijack IoT Devices
* US Teen 'Mastermind' in Epic Twitter Hack Sentenced to Prison
* Mimecast Says SolarWinds Hackers Stole Source Code
* Cyber Insurance Company Coalition Raises $175 Million at $1.75 Billion Valuation
* FBI Warns of PYSA Ransomware Attacks on Education Institutions in US, UK
* HD Moore Banks $5M Funding for Rumble Asset Management Startup
* Russia Threatens to Block Twitter in a Month
* Recorded Future Buys Fraud Analytics Startup Gemini Advisory
* Twitter Users Can Now Secure Accounts With Multiple Security Keys
* Authentication Provider LoginID Raises $6 Million in Seed Funding
* Software Development Security Firm Argon Emerges From Stealth Mode
* Microsoft Ships One-Click Mitigation Tool for Exchange Attacks
* Over 80,000 Exchange Servers Still Affected by Actively Exploited Vulnerabilities
* Swiss Police Raid Over Hack on U.S. Security-Camera Company
* Google Chrome Zero-Day Under Attack, Again

Infosecurity Magazine

* Recorded Future Swoops for Gemini Advisory in $52m Deal
* FBI Alert: Pysa Ransomware Targeting Education Sector
* Average Ransom Payment Surged 171% in 2020
* CompTIA Launches Training Catalogue to Promote "Outstanding" IT Apprenticeships
* Infrastructure Security Specialist Optilan Appoints Adrian Bannister as CFO
* Dropbox to Make Password Manager Feature Free for All Users
* 50% of Incident Response Pros Want Better Work-Life Balance
* SEC Charges Man Over Cannabis Firm Pump-and-Dump
* Chinese Threat Actors Target Global 5G Operators
* More Than a Quarter of Threats Never Seen Before
* Fastway Couriers Confirms Security Breach
* Spanish Data Protection Agency Issues Highest Ever Fine

KnowBe4 Security Awareness Training Blog RSS Feed

* 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
* Cybercrime Officially Has Its Own Global Ecosystem
* Make No Mistake, This Changes Everything: Nation-State 2.0
* Give Me Â£1,000 to Stop Calling You
* [THIS IS UGLY] A Hacker Got All My Texts for $16
* 6 Advanced Email Phishing Attacks
* CyberheistNews Vol 11 #11 [AN IMPORTANT] NIST Update That You Should Be Aware Of
* FBI Warns Against Deepfakes' Potential for Social Engineering

ISC2.org Blog

* 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
* 6 Tips to Integrate Security into Agile Application Development

HackRead

* 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
* Google Facing Lawsuit Over Tracking Users in Incognito Mode
* COVID-19 testing service in US exposes patients' photos, passports
* "Hacker Games" launched to challenge and improve cybersecurity skills
* Windows-Only 7-Zip now Available for Linux

Koddos

* 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
* Google Facing Lawsuit Over Tracking Users in Incognito Mode
* COVID-19 testing service in US exposes patients' photos, passports
* "Hacker Games" launched to challenge and improve cybersecurity skills
* Windows-Only 7-Zip now Available for Linux

Naked Security

* 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
* 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
* Naked Security Live - ICU: How much do your home-working photos give away?
* Poison packages - "Supply Chain Risks" user hits Python community with 4000 fake modules

Threat Post

* Tutor LMS for WordPress Open to Info-Stealing Security Holes
* Cisco Plugs Security Hole in Small Business Routers
* Teen Behind Twitter Bit-Con Breach Cuts Plea Deal
* $4,000 COVID-19 'Relief Checks' Cloak Dridex Malware
* Mimecast: SolarWinds Attackers Stole Source Code
* State-sponsored Threat Groups Target Telcos, Steal 5G Secrets
* A New Paradigm in Data Security: Insider Risk Management
* PYSA Ransomware Pillages Education Sector, Feds Warn
* Mom & Daughter Duo Hack Homecoming Crown
* Latest Mirai Variant Targets SonicWall, D-Link and IoT Devices

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

* 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
* How Enterprise Design Thinking Can Improve Data Security Solutions

InfoWorld

* 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
* Spring Native turns Spring apps into native executables
* Getting started with winget, the Windows Package Manager
* Containers need standard operating environments too
* 8 great Python libraries for natural language processing
* JDK 16: The new features in Java 16
* Why loosely coupled state in public clouds is better

C4ISRNET - Media for the Intelligence Age Military

* 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
* New director takes over at Pentagon's top research office
* Jet packs are on their way to a battlefield near you
* In a cyberattack disaster, DoD needs backup squad to fix networks, restart critical systems
* Relativity Space wins responsive launch contract

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

* Déjà vu-lnerability
* A Look at iMessage in iOS 14

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.

* Codefest CTF 2020
* BlueHens CTF 2021
* LINE CTF 2021
* PoseidonCTF 2nd Edition **cancelled**
* Securinets CTF Quals 2021
* SPRUSH CTF Quals 2021
* UMassCTF 2021
* VolgaCTF 2021 Qualifier
* ALLES! CTF 2021 HW Edition
* ångstromCTF 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

* DLLHSC : DLL Hijack SCanner A Tool To Assist With The Discovery
* PowerSharpPack : Offensive CSharp Projects Wraped Into Powershell
* Girsh : Automatically Spawn A Reverse Shell Fully Interactive
* HTTP_Bridge : Send TCP Stream Packets Over Simple HTTP Request
* Gitls : Enumerate Git Repository URL From List Of URL / User / Org
* Go-RouterSocks : Router Sock. One Port Socks For All The Others
* HiddenEyeReborn : HiddenEye With Completely New Codebase & Better Features Set
* SUB 404 : A Fast Tool To Check Subdomain Takeover Vulnerability
* Procrustes : Script To Automates The Exfiltration Of Data Over DNS
* Chameleon : Customizable Honeypots For Monitoring Network Traffic

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

* Six CTI Challenges and Their Solutions - Reaching CTI's Full Potential | SANS CTI Summit 2021
* Getting started in DFIR: Testing 1,2,3 | Phill Moore
* Episode 185: When to Stop Looking for Evidence - Part 1
* VERISIZE your way into CTI | David Thejl-Clayton | 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]

* Cyberpunk's Company Hacked by HelloKitty Ransomware: Live Demo
* Windows Defender vs Ransomware in 2021

Eli the Computer Guy

* TINDER VIOLENCE BACKGOUND CHECKS (garbo)
* TWITTER HACKER SENTENCED to 3 YEARS in PRISON
* TWITTER BANS WORD - Memphis
* HOMEPOD is DEAD

Security Now

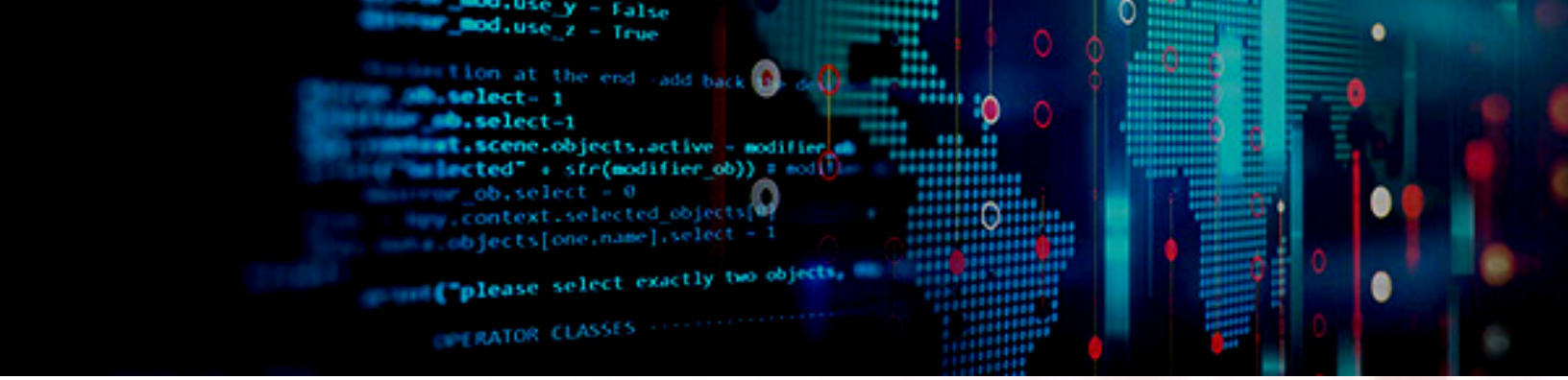
* ProxyLogon - New Chrome 0-Day, Patch Tuesday Redux, Spectre Comes to Chrome
* Hafnium - Dependency Confusion, Intel Side Channel Attacks, Crispy Subtitles From Lay's

Troy Hunt

* Weekly Update 234

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

* 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
* How to Keep Up With Vulnerability Management Challenges in Ephemeral Cloud Environments
* Metasploit Wrap-Up
* Mass Exploitation of Exchange Server Zero-Day CVEs: What You Need to Know
* IAM Never Gonna Give You Up, Never Gonna Breach Your Cloud

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Backdoor.Win32.Agent.mzn Buffer Overflow
* VestaCP 0.9.8 Cross Site Request Forgery
* CuteNews 2.1.2 Shell Upload
* Trojan-Dropper.Win32.Delf.p Buffer Overflow
* Trojan-Dropper.Win32.Delf.p Missing Authentication
* WoWonder Social Network Platform 3.1 SQL Injection
* GeoGebra Graphing Calculator 6.0.631.0 Denial Of Service
* Microsoft Windows Containers DP API Cryptography Flaw
* GeoGebra 3D Calculator 5.0.511.0 Denial Of Service
* GeoGebra CAS Calculator 6.0.631.0 Denial Of Service
* GeoGebra Classic 5.0.631.0-d Denial Of Service
* Alphaware E-Commerce System 1.0 Shell Upload / SQL Injection
* ExpressionEngine 6.0.2 PHP Code Injection
* VoIPmonitor 27.6 Buffer Overflow
* VoIPmonitor 27.5 Missing Memory Protections
* macOS CoreGraphics Integer Overflow / Out-Of-Bounds Write
* Online News Portal 1.0 Cross Site Scripting
* Online News Portal 1.0 SQL Injection
* Trojan.Win32.Siscos.bqe Insecure Permissions
* SonLogger 4.2.3.3 Shell Upload
* SonLogger 4.2.3.3 SuperAdmin Account Creation / Information Disclosure
* Windows Server 2012 SrClient DLL Hijacking
* VoIPmonitor WEB GUI 24.55 Cross Site Scripting
* Interactive Suite 3.6 Unquoted Service Path
* eBeam Education Suite 2.5.0.9 Unquoted Service Path

CXSecurity

* Windows Server 2012 SrClient DLL Hijacking
* SonLogger 4.2.3.3 Shell Upload
* GeoGebra 3D Calculator 5.0.511.0 Denial of Service (PoC)
* GeoGebra CAS Calculator 6.0.631.0 Denial Of Service
* GeoGebra Graphing Calculator 6.0.631.0 Denial Of Service
* GeoGebra Classic 5.0.631.0-d Denial Of Service
* Alphaware E-Commerce System 1.0 Shell Upload / SQL Injection

Proof of Concept (PoC) & Exploits

Exploit Database

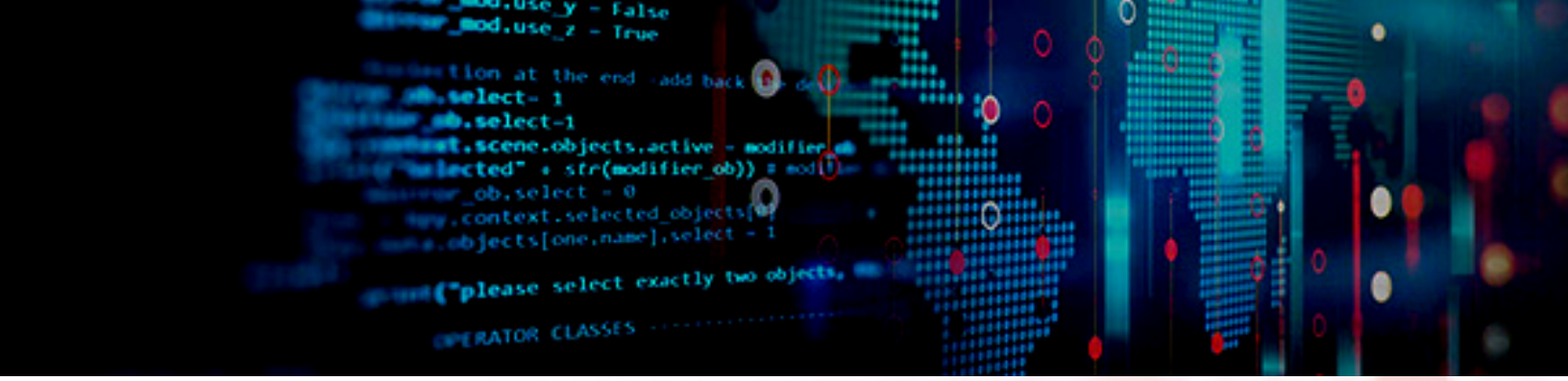
* [webapps] Hestia Control Panel 1.3.2 - Arbitrary File Write
* [webapps] SEO Panel 4.8.0 - 'order_col' Blind SQL Injection
* [webapps] rConfig 3.9.6 - Arbitrary File Upload to Remote Code Execution (Authenticated)
* [remote] Microsoft Exchange 2019 - SSRF to Arbitrary File Write (Proxylogon)
* [webapps] VestaCP 0.9.8 - 'v_interface' Add IP Stored XSS
* [local] VFS for Git 1.0.21014.1 - 'GVFS.Service' Unquoted Service Path
* [local] FastStone Image Viewer 7.5 - .cur BITMAPINFOHEADER 'BitCount' Stack Based Buffer Overflow (AS
* [webapps] VestaCP 0.9.8 - File Upload CSRF
* [webapps] WoWonder Social Network Platform 3.1 - 'event_id' SQL Injection
* [local] GeoGebra 3D Calculator 5.0.511.0 - Denial of Service (PoC)
* [local] GeoGebra CAS Calculato‪r‬ 6.0.631.0 - Denial of Service (PoC)
* [local] GeoGebra Classic 5.0.631.0-d - Denial of Service (PoC)
* [local] GeoGebra Graphing Calculato‪r‬ 6.0.631.0 - Denial Of Service (PoC)
* [webapps] Alphaware E-Commerce System 1.0 - Unauthenicated Remote Code Execution (File Upload + SQL i
* [webapps] SonLogger 4.2.3.3 - Unauthenticated Arbitrary File Upload (Metasploit)
* [webapps] Sonlogger 4.2.3.3 - SuperAdmin Account Creation / Information Disclosure
* [webapps] openMAINT openMAINT 2.1-3.3-b - 'Multiple' Persistent Cross-Site Scripting
* [local] Interactive Suite 3.6 - 'eBeam Stylus Driver' Unquoted Service Path
* [local] eBeam education suite 2.5.0.9 - 'eBeam Device Service' Unquoted Service Path
* [local] Realtek Wireless LAN Utility 700.1631 - 'Realtek11nSU' Unquoted Service Path
* [local] QNAP QVR Client 5.0.0.13230 - 'QVRService' Unquoted Service Path
* [webapps] rConfig 3.9.6 - 'path' Local File Inclusion (Authenticated)
* [webapps] MagpieRSS 0.72 - 'url' Command Injection and Server Side Request Forgery
* [webapps] Zenario CMS 8.8.53370 - 'id' Blind SQL Injection

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

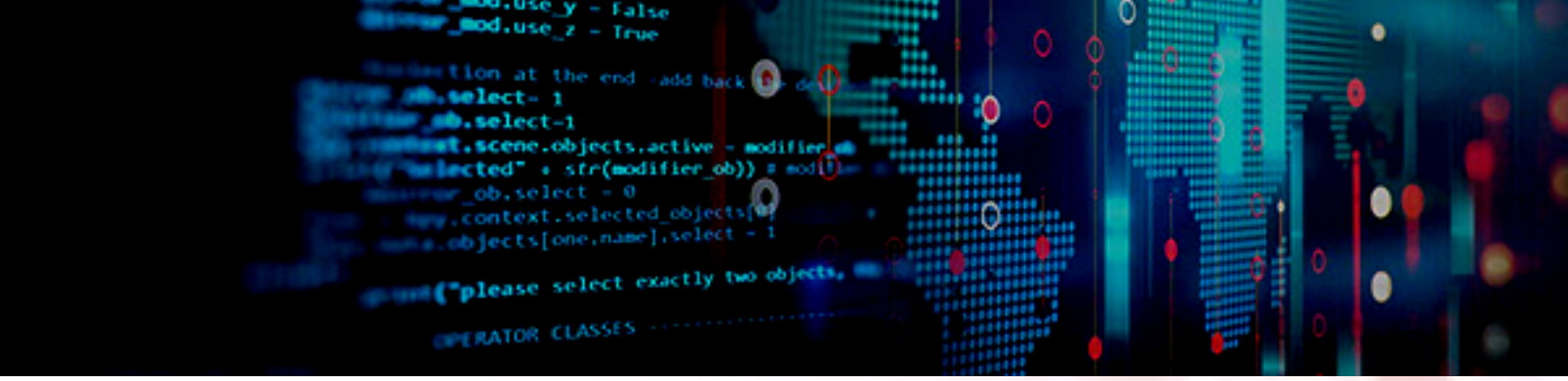
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://pmd.deliserdangkab.go.id/hell.php
https://pmd.deliserdangkab.go.id/hell.php notified by hell_c0de
https://perpustakaan.deliserdangkab.go.id/hell.php
https://perpustakaan.deliserdangkab.go.id/hell.php notified by hell_c0de
https://sikesa.deliserdangkab.go.id/hell.php
https://sikesa.deliserdangkab.go.id/hell.php notified by hell_c0de
https://dishub.deliserdangkab.go.id/hell.php
https://dishub.deliserdangkab.go.id/hell.php notified by hell_c0de
https://inspektorat.deliserdangkab.go.id/hell.php
https://inspektorat.deliserdangkab.go.id/hell.php notified by hell_c0de
http://www.ndi.ufpr.br
http://www.ndi.ufpr.br notified by Moroccan Revolution
http://www.midiacidada.ufpr.br/wp-css.php
http://www.midiacidada.ufpr.br/wp-css.php notified by Moroccan Revolution
http://www.gpla.gov.ly
http://www.gpla.gov.ly notified by cyber hacker-ly
http://army.gov.ly
http://army.gov.ly notified by cyber hacker-ly
http://punjabtourism.gov.in/rn.html
http://punjabtourism.gov.in/rn.html notified by Ren4Sploit
http://ipirti.gov.in/rn.html
http://ipirti.gov.in/rn.html notified by Ren4Sploit
http://biharbhawan.gov.in/rn.html
http://biharbhawan.gov.in/rn.html notified by Ren4Sploit
http://bijar.gov.ir/Morocco.html
http://bijar.gov.ir/Morocco.html notified by Moroccan Revolution
http://divandareh.gov.ir/index.html
http://divandareh.gov.ir/index.html notified by Moroccan Revolution
http://sarvabad.gov.ir
http://sarvabad.gov.ir notified by Moroccan Revolution
http://kamyaran.gov.ir
http://kamyaran.gov.ir notified by Moroccan Revolution
http://dehgolan.gov.ir
http://dehgolan.gov.ir notified by Moroccan Revolution



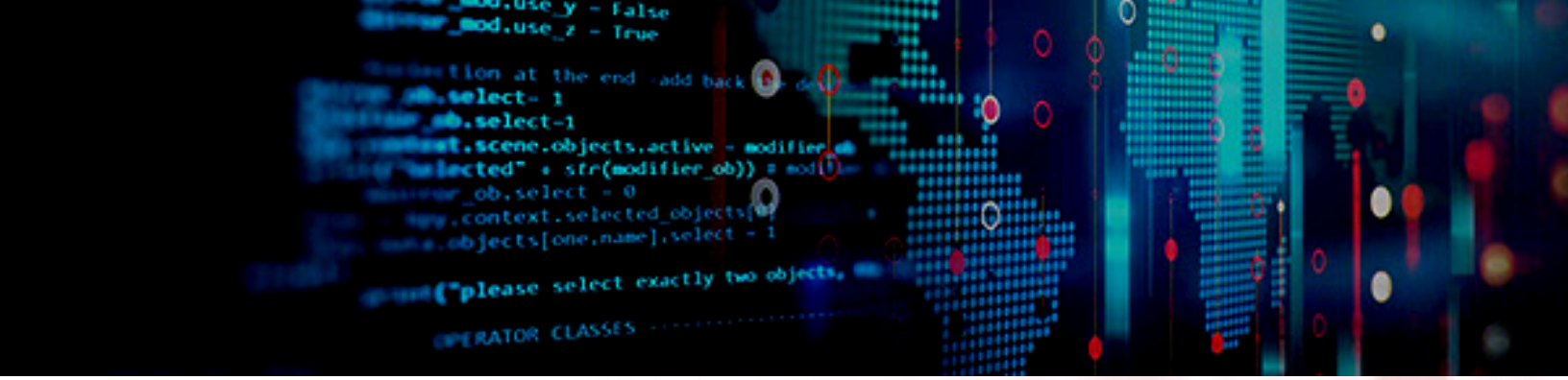
Dark Web News

Darknet Live

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)
Romanian Man Arrested for Alleged Drug Trafficking
Romanian authorities announced the arrest of a suspected drug trafficker who allegedly resold drugs purchased on darkweb markets. (via darknetlive.com)
New DEA Report Highlights the Darkweb and Bitcoin
The Drug Enforcement Administration released their 2020 National Drug Threat Assessment which outlined threats posed to the country through the various forms of drug trafficking. (via darknetlive.com)

Dark Web Link

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.
Fake Identity: IT Contractor Published Stolen Data On The Darknet
A Sydney based IT contractor who had allegedly published a stockpile of stolen personal data on the dark web had utilized the VPNs and onion routers and fake identity. He had set the fake accounts in the names of his colleagues for covering up his tracks, mentions the prosecutors. The accused had been identified as [...] The post Fake Identity: IT Contractor Published Stolen Data On The Darknet appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Child Pornography Violations: Longview Sex Offender Sentenced Prison
A sex offender from Longview, who has been identified as part of a joint global investigation, received a prison sentence for conducting child pornography violations in the Eastern District of Texas. The federal prison sentence was announced this week by the Acting U.S. Attorney, Nicholas J. Gangei. The accused was identified as Charles Orange, aged [...] The post Child Pornography Violations: Longview Sex Offender Sentenced Prison appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* 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
* F5 Security Advisory for RCE Vulnerabilities in BIG-IP, BIG-IQ
* Microsoft Releases March 2021 Security Updates
* AA21-076A: TrickBot Malware
* AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities
* Vulnerability Summary for the Week of March 8, 2021
* Vulnerability Summary for the Week of March 1, 2021

Zero Day Initiative Advisories

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, 1 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, 1 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, 1 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, 1 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, 1 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, 1 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, 1 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, 2 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, 2 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, 2 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, 2 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, 2 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-13421: 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, 2 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-13415: 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, 2 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-13424: 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, 2 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-13419: 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, 2 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-13402: 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, 2 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-13420: 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, 2 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-13430: 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, 2 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-13442: 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, 2 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-13407: 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, 2 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-13416: 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, 2 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-13023: 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: 2021-03-16, 2 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-13422: 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, 2 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 2021-0883-01
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.

Red Hat Security Advisory 2021-0871-01

Red Hat Security Advisory 2021-0871-01 - MongoDB is a higly-scalable document database. The Debezium MongoDB connector includes Java driver to access a MongoDB database.

Ubuntu Security Notice USN-4880-1

Ubuntu Security Notice 4880-1 - It was discovered that OpenJPEG incorrectly handled certain image data. An attacker could use this issue to cause OpenJPEG to crash, leading to a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-4879-1

Ubuntu Security Notice 4879-1 - It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad-hoc SSIDs. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Loris Reiff discovered that the BPF implementation in the Linux kernel did not properly validate attributes in the getsockopt BPF hook. A local attacker could possibly use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4878-1

Ubuntu Security Notice 4878-1 - It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad-hoc SSIDs. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Ryota Shiga discovered that the sockopt BPF hooks in the Linux kernel could allow a user space program to probe for valid kernel addresses. A local attacker could use this to ease exploitation of another kernel vulnerability. Various other issues were also addressed.

Red Hat Security Advisory 2021-0848-01

Red Hat Security Advisory 2021-0848-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4877-1

Ubuntu Security Notice 4877-1 - It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad-hoc SSIDs. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. 吴异 discovered that the NFS implementation in the Linux kernel did not properly prevent access outside of an NFS export that is a subdirectory of a file system. An attacker could possibly use this to bypass NFS access restrictions. Various other issues were also addressed.

Ubuntu Security Notice USN-4876-1

Ubuntu Security Notice 4876-1 - Olivier Benjamin and Pawel Wieczorkiewicz discovered a race condition the Xen paravirt block backend in the Linux kernel, leading to a use-after-free vulnerability. An attacker in a guest VM could use this to cause a denial of service in the host OS. It was discovered that the Marvell WiFi-Ex device driver in the Linux kernel did not properly validate ad-hoc SSIDs. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

SolarWinds TFTP Server 11.0.4.101 Remote Unauthenticated Reconfiguration

SolarWinds TFTP Server version 11.0.4.101 suffers from a remote unauthenticated reconfiguration vulnerability that could result in code execution.

Ubuntu Security Notice USN-4764-1

Ubuntu Security Notice 4764-1 - It was discovered that GLib incorrectly handled certain symlinks when replacing files. If a user or automated system were tricked into extracting a specially crafted file with File Roller, a remote attacker could possibly create files outside of the intended directory.

Red Hat Security Advisory 2021-0831-01

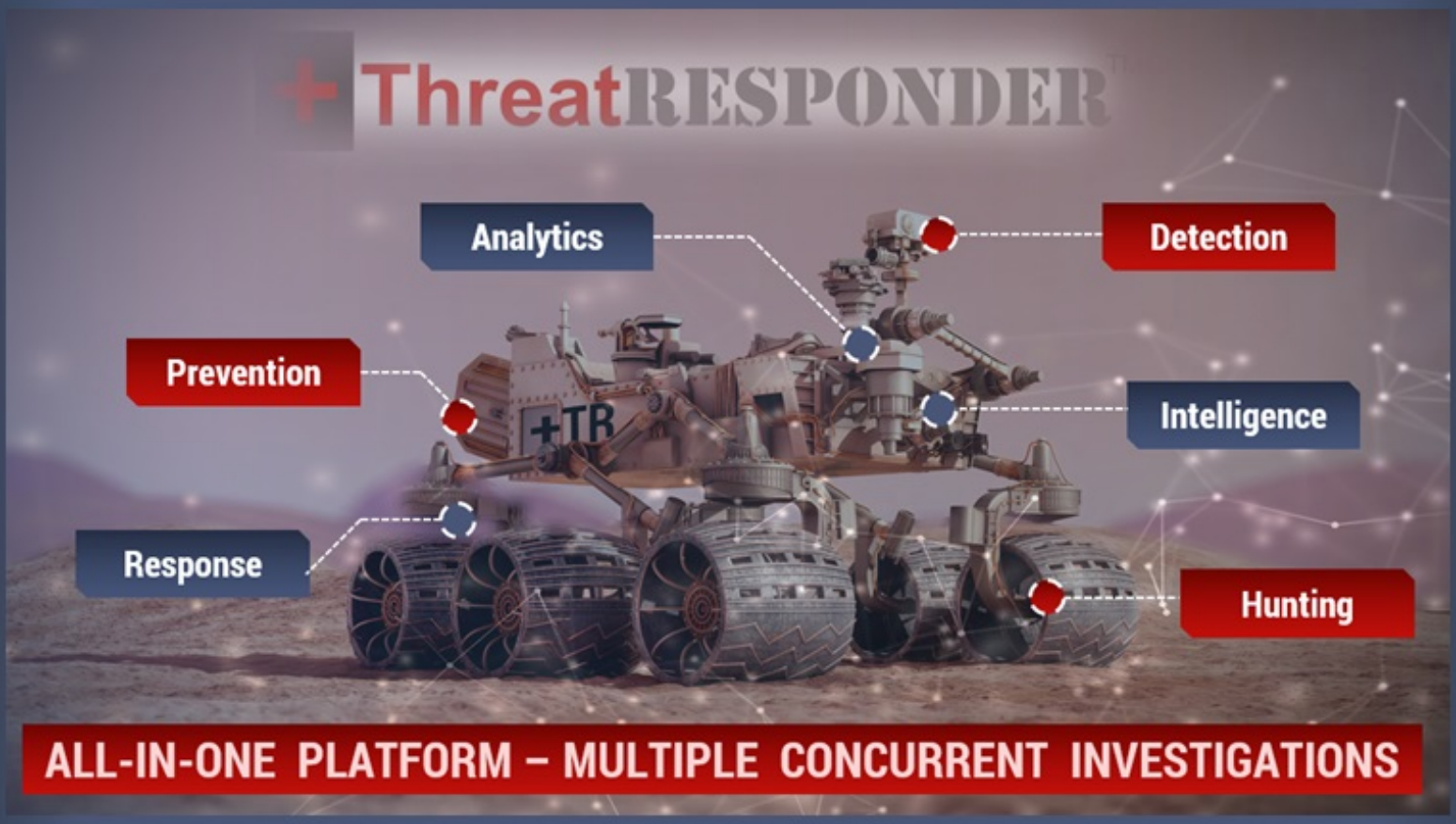
Red Hat Security Advisory 2021-0831-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

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:

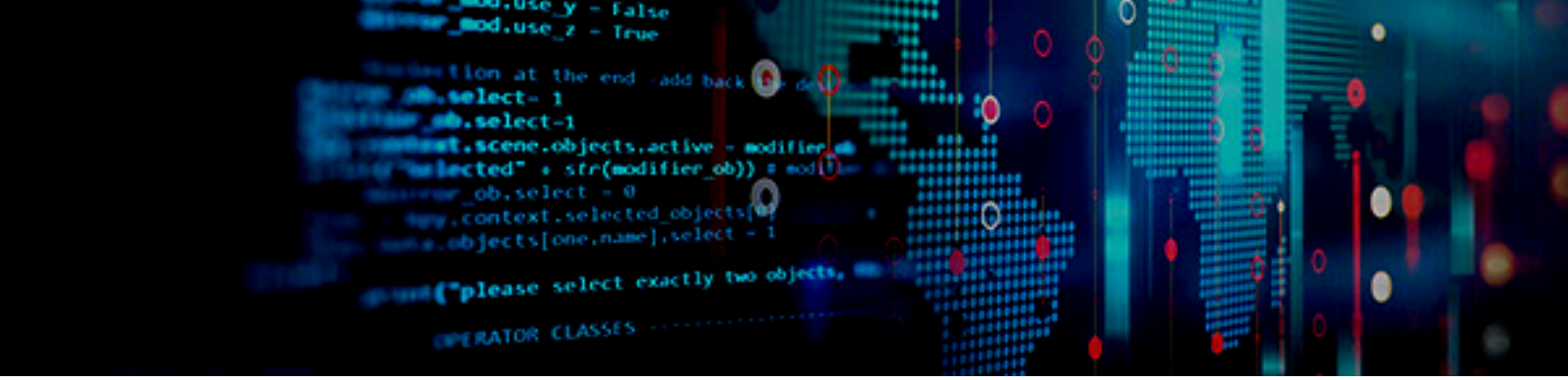
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

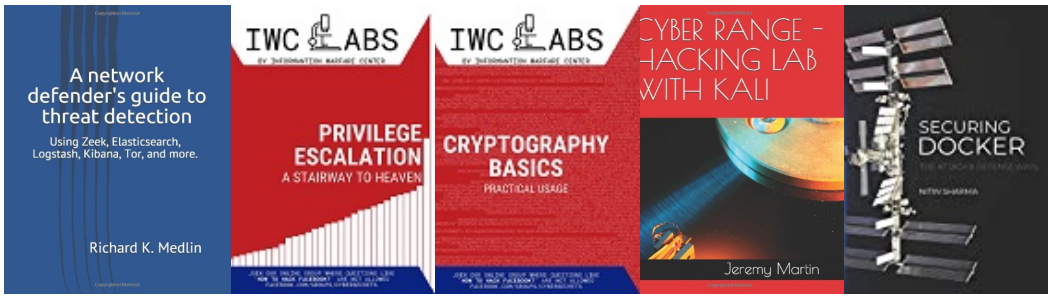


The Cyber Secrets publications on Amazon

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