Jun-14-21

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

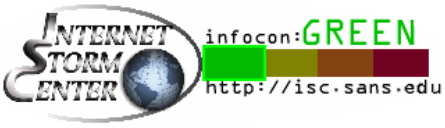
ARGOS
APPLIED INTELLIGENCE

June 14, 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

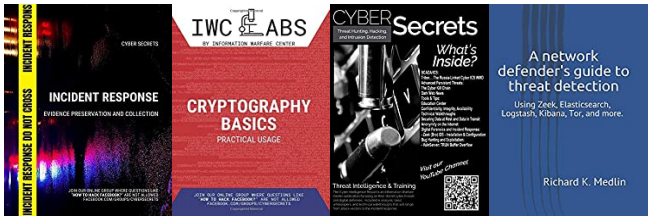


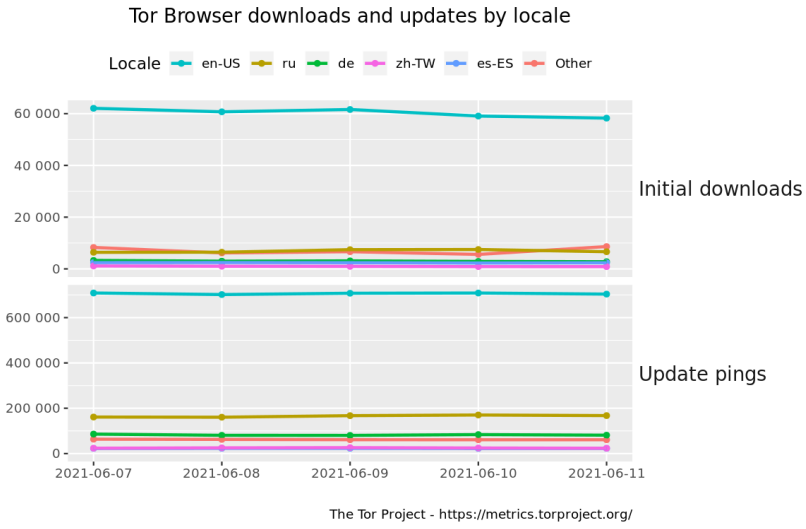
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

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

Index of Sections

Packet Storm Security

* How Hackers Used Slack To Break Into EA Games
* STEM Audio Table Rife With Business Threatening Bugs
* McDonald's Operations In South Korea And Taiwan Hit By Data Breach
* US Retailer Carter Leaks PII With URL Shortener
* Hackers Force Iowa College To Cancel Classes For Four Days
* Cops Are Using Facebook To Target Pipeline Protest Leaders
* Intel Plugs 29 Holes In CPUs, Bluetooth, Security
* Meat Giant JBS Pays $11 Million In Ransom To Resolve Attack
* Phil Zimmerman Looks Back On 30 Years Of PGP
* An0m Encrypted-Chat Sting Leads To Arrest Of 800
* DHS Chooses Companies To Run Civilian Agency Vulnerability Disclosure Programs
* One Fastly Customer Triggered Internet Meltdown
* Windows Container Malware Targets Kubernetes Clusters
* Apple Continues Privacy War With App Tracker Reports
* Majority Of Ransom Paid By Colonial Pipeline Seized By DOJ
* How The FBI And AFP Accessed Encrypted Messages In TrojanShield Investigation
* REvil Ransomware Gang Spill Details On US Attacks
* WhatsApp Hijack Scam Continues To Spread
* Apple Updates AirTags After Stalking Fears
* Patch Now: Attackers Are Hunting For This Critical VMware vCenter Flaw
* Hacker Lexicon: What Is A Supply Chain Attack?
* Chrome 91 Will Warn Users When Installing Untrusted Extensions
* Supreme Court Narrows Interpretation Of CFAA, To The Relief Of Ethical Hackers
* Google PPC Ads Used To Deliver Infostealers
* FBI Says It Is Investigating About 100 Types Of Ransomware

Krebs on Security

* Microsoft Patches Six Zero-Day Security Holes
* Justice Dept. Claws Back $2.3M Paid by Colonial Pipeline to Ransomware Gang
* Adventures in Contacting the Russian FSB
* Using Fake Reviews to Find Dangerous Extensions
* Boss of ATM Skimming Syndicate Arrested in Mexico
* How to Tell a Job Offer from an ID Theft Trap
* Recycle Your Phone, Sure, But Maybe Not Your Number
* Try This One Weird Trick Russian Hackers Hate
* DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized
* Microsoft Patch Tuesday, May 2021 Edition

Dark Reading

* Name That Toon: Sight Unseen
* Colonial Pipeline Cyberattack Proves a Single Password Isn't Enough
* Trickbot Investigation Shows Details of Massive Cybercrime Effort
* McDonald's Data Breach Exposed Business & Customer Data
* Details Emerge on How Gaming Giant EA Was Hacked
* Many Mobile Apps Intentionally Using Insecure Connections for Sending Data
* Secure Access Trade-offs for DevSecOps Teams
* New Ransomware Group Claiming Connection to REvil Gang Surfaces
* 'Fancy Lazarus' Criminal Group Launches DDoS Extortion Campaign
* Healthcare Device Security Firm COO Charged With Hacking Medical Center
* JBS CEO Says Company Paid $11M in Ransom
* 'Beware the Lady Named Katie'
* The Workforce Shortage in Cybersecurity Is a Myth
* Intl. Law Enforcement Operation Disrupts Slilpp Marketplace
* Deepfakes Are on the Rise, but Don't Panic Just Yet
* 11 Cybersecurity Vendors to Watch in 2021
* Cyber Is the New Cold War & AI Is the Arms Race
* Required MFA Is Not Sufficient for Strong Security: Report
* What to Know About Updates to the PCI Secure Software Standard
* RSA Spins Off Fraud & Risk Intelligence Unit

The Hacker News

* NoxPlayer Supply-Chain Attack is Likely the Work of Gelsemium Hackers
* Cybersecurity Executive Order 2021: What It Means for Cloud and SaaS Security
* Chinese Hackers Believed to be Behind Second Cyberattack on Air India
* Mozilla Says Google's New Ad Tech-FLoC-Doesn't Protect User Privacy
* Hackers Can Exploit Samsung Pre-Installed Apps to Spy On Users
* Live Cybersecurity Webinar - Deconstructing Cobalt Strike
* 7-Year-Old Polkit Flaw Lets Unprivileged Linux Users Gain Root Access
* New Cyber Espionage Group Targeting Ministries of Foreign Affairs
* U.S. Authorities Shut Down Slilpp-Largest Marketplace for Stolen Logins
* Emerging Ransomware Targets Dozens of Businesses Worldwide
* Using Breached Password Detection Services to Prevent Cyberattack
* Beef Supplier JBS Paid Hackers $11 Million Ransom After Cyberattack
* New Chrome 0-Day Bug Under Active Attacks - Update Your Browser ASAP!
* New TLS Attack Lets Attackers Launch Cross-Protocol Attacks Against Secure Sites
* Crypto-Mining Attacks Targeting Kubernetes Clusters via Kubeflow Instances

Security Week

* G7 Tells Russia to Crack Down on Ransomware, Other Cybercrime
* Cybersecurity Training Company Immersive Labs Raises $75 Million
* Google Offers UK Watchdog Role in Browser Cookie Phase-Out
* Cybersecurity M&A Roundup for June 7-13, 2021
* Apple Reaffirms Privacy Stance Amid Trump Probe Revelations
* Volkswagen America Discloses Data Breach Impacting 3.3 Million
* Wray: FBI Frowns on Ransomware Payments Despite Recent Trend
* Recorded Future Unveils $20M Threat-Intel Investment Fund
* COO of Security Company Charged for Cyberattack on Medical Center
* RSA Spins Out Fraud and Risk Intelligence Unit as Standalone Company Outseer
* McDonald's Says Hackers Breached Data in Taiwan, South Korea
* GitHub Discloses Details of Easy-to-Exploit Linux Vulnerability
* Canada Privacy Watchdog Slams Police Use of Facial Recognition Tool
* Alibaba's Lazada Launches Public Bug Bounty Program
* Gaming Giant EA Confirms Breach, Theft of Source Code
* Italy Sets Up Cybersecurity Agency After Russia Warnings
* Authorities Take Down Stolen Login Credentials Marketplace Slilpp
* Attackers Leverage SonicWall VPN Flaw to Compromise SRA Appliances
* Flaws in Rockwell Software Impact Products From Schneider Electric, GE and Others
* GitHub Starts Scanning for Exposed Package Registry Credentials
* Honeywell Launches OT Cybersecurity Monitoring and Response Service
* US Drops Trump Order Targeting TikTok, Plans Its Own Review
* Webinar Today: CISO Guide to Preventing Vendor Email Compromise
* ALPACA: New TLS Attack Allows User Data Extraction, Code Execution

Infosecurity Magazine

* Government Wants Startups to Build a More Secure Nation
* G7 Turns Up the Heat on Putin Over Ransomware Attacks
* Global Police Close Record Number of Fake Pharma Sites
* COO Charged in Georgia Hospital Cyber-attack
* US Launches National AI Task Force
* McDonald's Suffers Data Breach
* Gaming Giant EA Suffers Major Data Breach
* #G7UK: UK and US Strike New Agreements on Cybersecurity
* Unknown Attacker Chains Chrome and Windows Zero-Days
* China's New "Anti-Sanctions" Law Means Headache for Foreign Firms
* Quantum Breakthrough in Britain Creates 600km Secure Link
* IT Administrator Sentenced for Sabotaging Employer

KnowBe4 Security Awareness Training Blog RSS Feed

* KnowBe4 Earns 2021 Top Rated Award from TrustRadius
* Deal or No Deal: The Double-edged Sword of the IT Security Bundle
* Insights Into Credential Phishing
* FINRA Warns U.S. Brokerage Firms of New Phishing Campaign Threatening Penalties for Non-Compliance
* Ransomware Tops IBMs List of Most Observed Attack Types with Sodinokibi Maintaining the Lead
* 78% of CISOs Say Attacks Have Increased as a Result of More Employees Working from Home
* Chinese Hacker Group Debuts After 3 Years of Testing with a Previously Unseen Backdoor Exploit
* The Future Of Ransomware
* CyberheistNews Vol 11 #22 [Heads Up] New Email Attack Takes a Phishing-Turned-Vishing Angle To S
* Phishing Trends Show X-Rated Themes Have Skyrocketed 974%

ISC2.org Blog

* Best Practices and Techniques for Pseudonymization
* Help Shape the ISSMP Exam
* An Inside Look at Cloud Security from Industry Experts
* Make New Connections with (ISC)² Community
* Software Security Testing - Hidden Thoughts Can Cost You

HackRead

* Game giant Electronic Arts is the latest victim of massive data breach
* What You Need to Know About SOX Compliance
* 800+ criminals arrested after FBI turned Anom app into honeypot
* How gamers should secure their accounts from cyber attacks
* FBI recovers millions in ransom from DarkSide ransomware gang
* Kubernetes Clusters Targeted by Siloscape Malware
* 4 Ways For Employees To Distinguish Phishing Attacks

Koddos

* Game giant Electronic Arts is the latest victim of massive data breach
* What You Need to Know About SOX Compliance
* 800+ criminals arrested after FBI turned Anom app into honeypot
* How gamers should secure their accounts from cyber attacks
* FBI recovers millions in ransom from DarkSide ransomware gang
* Kubernetes Clusters Targeted by Siloscape Malware
* 4 Ways For Employees To Distinguish Phishing Attacks

Naked Security

* ALPACA - the wacky TLS security vulnerability with a funky name
* S3 Ep36: Trickbot coder busted, passwords cracked, and breaches judged [Podcast]
* Chrome zero-day, hot on the heels of Microsoft's IE zero-day. Patch now!
* How could the FBI recover BTC from Colonial's ransomware payment?
* Latvian woman charged with writing malware for the Trickbot Group
* How to hack into 5500 accounts… just using "credential stuffing"
* S3 Ep35: Apple chip flaw, Have I Been Pwned, and Covid tracker trouble [Podcast]
* "Have I Been Pwned" breach site partners with… the FBI!
* "Unpatchable" vuln in Apple's new Mac chip - what you need to know
* S3 Ep34: Apple bugs, scammers busted, and how crooks bypass 2FA [Podcast]

Threat Post

* Unpatched Bugs Found Lurking in Provisioning Platform Used with Cisco UC
* Baby Clothes Giant Carter's Leaks 410K Customer Records
* REvil Hits US Nuclear Weapons Contractor: Report
* Cyberpunk 2077 Hacked Data Circulating Online
* Monumental Supply-Chain Attack on Airlines Traced to State Actor
* Police Grab Slilpp, Biggest Stolen-Logins Market
* Hackers Steal FIFA 21 Source Code, Tools in EA Breach
* 'Fancy Lazarus' Cyberattackers Ramp up Ransom DDoS Efforts
* Chrome Browser Bug Under Active Attack
* STEM Audio Table Rife with Business-Threatening Bugs

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

IBM Security Intelligence

* Educating the Educators: Protecting Student Data
* Everyone Wants to Build a Cyber Range: Should You? Part 2
* Cybersecurity Tips for Business Travelers: Best Practices for 2021
* What is Network Detection and Response and Why is it So Important?
* Confidential Computing: The Future of Cloud Computing Security
* How Good Transaction Security Can Make Customer Visits Easier
* 5 Global Supply Chain Security Threats (and How to Handle Them)
* Thoughts From a Data Security Expert: 3 Things That Keep Me Up at Night
* Cyber Gangs: Who Are They in 2021 and What Do They Want?
* Learning the Building Blocks You Need for Consumer Identity and Access Management Part 2: Engage

InfoWorld

* The great cloud computing surge
* Go 1.17 moves to beta, with language and compiler enhancements
* From legacy to the cloud: The 3 stages of enterprise modernization
* Excel, Python, and the future of data science
* Visual Studio Code adds Workplace Trust for code editing safety
* Oracle offers Java management service
* Complexity is the biggest threat to cloud success and security
* JDK 17: The new features in Java 17
* Snowflake pushes back at… whom?
* "Do More with R" video tutorials

C4ISRNET - Media for the Intelligence Age Military

* Founder of Army tactical network team reflects on tenure, future of joint war fighting
* NATO surveillance drones dial up flying hours, maritime sensing
* Space Command asks Congress for $67 million to achieve full operational capability
* Marine Corps names new top information officer
* 'Drone Wars': New book wonders who will be the next drone superpower
* 2 combatant command budgets left out funding for JADC2 international collaboration tool
* NORAD, NORTHCOM want $80 million to test SpaceX and OneWeb in the Arctic
* DoD wish list seeks more funds to boost Pacific missile defense, weapons cybersecurity
* US Cyber Command wants more money for network defense
* Army says 2025 tactical network will make JADC2 a reality

The Hacker Corner

Conferences

* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)
* How To Sponsor Cybersecurity Conferences
* How To Secure Earned Cybersecurity Speaking Engagements
* World RPA & AI Summit | Interview with Ashley Pena

Google Zero Day Project

* Fuzzing iOS code on macOS at native speed
* Designing sockfuzzer, a network syscall fuzzer for XNU

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.

* The Threat Interceptors Challenge
* CTF InterIUT 2021
* WeCTF 2021
* CTFZone 2021
* Hack-A-Sat 2 Qualifiers
* Hacky Holidays - Space Race
* CyberThreatForce CTF | 2021
* 0CTF/TCTF 2021 Quals
* redpwnCTF 2021
* ENOWARS 5

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

* hacksudo: L.P.E.
* hacksudo: FOG
* Prime (2021): 2
* DriftingBlues: 9 (final)
* AdmX: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

* tcpdump 4.99.1
* nfstream 6.3.2
* GNU Privacy Guard 2.2.28
* Petalus 1.0.0
* SQLMAP - Automatic SQL Injection Tool 1.5.6
* Flawfinder 2.0.17
* Wireshark Analyzer 3.4.6
* Zeek 4.0.2
* American Fuzzy Lop plus plus 3.13c
* Flawfinder 2.0.16

Kali Linux Tutorials

* Onelinepy : Python Obfuscator To Generate One-Liners And FUD Payloads
* Arkhota : A Web Brute Forcer For Android
* Dent : A Framework For Creating COM-based Bypasses Utilizing Vulnerabilities In Microsoft's WDAPT Sen
* Bucky : An Automatic S3 Bucket Discovery Tool
* DNS-Black-Cat(DBC) : Multi Platform Toolkit For An Interactive DNS Shell Commands Exfiltration, By Us
* Php_Code_Analysis : Scan your PHP code for vulnerabilities
* Solr-GRAB : Steal Apache Solr Instance Queries With Or Without A Username And Password
* CiLocks : Android LockScreen Bypass
* MurMurHash : Tool To Calculate A MurmurHash Value Of A Favicon To Hunt Phishing Websites On The Shoda
* AMSITrigger : The Hunt For Malicious Strings

GBHackers Analysis

* EA Sports Hacked - Hackers Stolen Source Code With 780 GB of Data
* Russian Hacker Jailed for Running a Darkweb Market Place that Sells Stolen Credit card Details
* Russian Hacker Group Nobelium Attack U.S Gov Agencies By Targeting 3,000 Email Accounts
* Hackers Exploited Fortinet Vulnerabilities to Gain Access of a U.S. Municipal Government Webserver
* 13 Vulnerabilities in Nagios Server Let Hackers Compromises The IT Infrastructure

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Mobile Validation - Working together for the Common Good
* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course

Defcon Conference

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

Hak5

* Hacked by an Evil Neighbor w/ Retia
* Amazon Sidewalk is LIVE - Opt Out Now! - ThreatWire
* Hacking Hardware with @_MG_

The PC Security Channel [TPSC]

* Windows Defender vs Malware in 2021
* Darkside Ransomware: The threat behind the state of emergency in the US

Eli the Computer Guy

* DNS for Cybersecurity
* Apply to Jobs You are UNDER QUALIFIED for - Tech Career Advice
* ELI THE COMPUTER GUY is DEAD (third community strike)
* Arduino - Raspberry Pi Web Fan Control with MySQL

Security Now

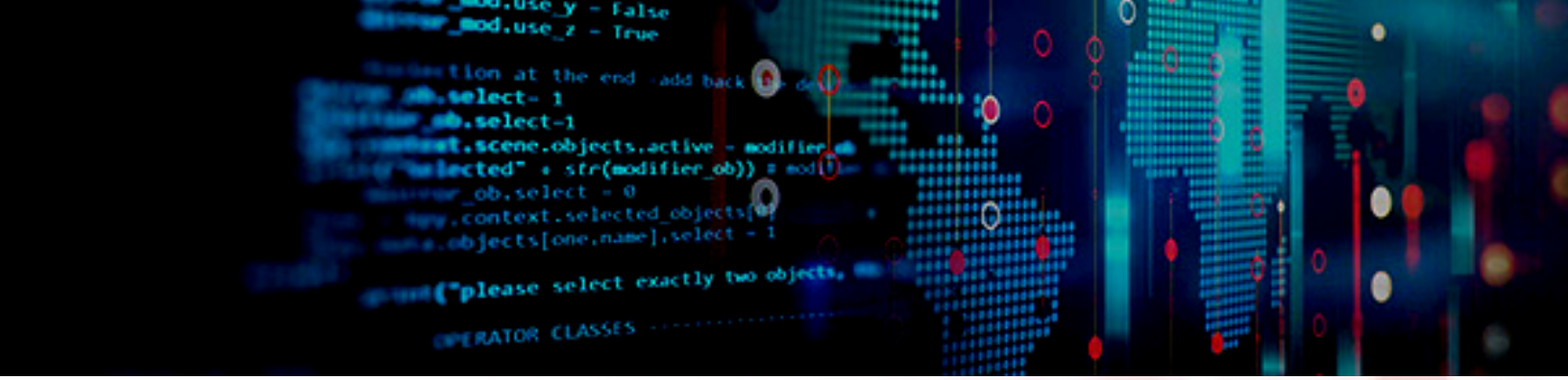
* Extrinsic Password Managers - Great CyberSecurity Awakening of 2021, NAT vs IPv6, Tavis Ormandy
* Epsilon Red - Chrome 91, Emsisoft's Ransomware Decryption Tool, Revisiting Amazon Sidewalk

Troy Hunt

* Weekly Update 247

Intel Techniques: The Privacy, Security, & OSINT Show

* 220-Privacy, Security, & OSINT Potluck
* 219-Tracking (Or Getting Tracked) with AirTags



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

* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think
* MobileInter: A Popular Magecart Skimmer Redesigned For Your Phone
* DarkSide is Standing Down, But Its Affiliates Live On
* Next-Gen Threat Intelligence: Adding Profound Value to Security and Risk Functions
* TrickBot: Get to Know the Malware That Refuses to Be Killed
* SolarWinds: Illuminating the Hidden Patterns That Advance the Story
* For Threat Actors, Shadow Z118 is the Kit That Keeps on Giving
* RiskIQ is Illuminating the Global Attack Surface With Next-Gen Security Intelligence

FireEye

* Metasploit Wrap-Up
* Attack Surface Analysis Part 1: Vulnerability Scanning
* [Security Nation] Jeff Man on Mapping the MITRE ATT&CK Framework Against PCI
* Akkadian Provisioning Manager Multiple Vulnerabilities Disclosure
* Patch Tuesday - June 2021
* Action! Start putting automation into practice.
* Kill chains: Part 2→Strategic and tactical use cases
* Metasploit Wrap-Up
* All about the boundaries: The cloud IAM lifecycle approach
* Proposed security researcher protection under CFAA

Proof of Concept (PoC) & Exploits

Packet Storm Security

* NetSetManPro 4.7.2 Privilege Escalation
* Accela Civic Platorm 21.1 Cross Site Scripting
* Backdoor.Win32.Zombam.gen Buffer Overflow
* WordPress Database Backups 1.2.2.6 Cross Site Request Forgery
* Grocery Crud 1.6.4 SQL Injection
* OpenEMR 5.0.0 Remote Shell Upload
* Backdoor.Win32.Zombam.gen Code Execution
* Backdoor.Win32.Zombam.gen Cross Site Scripting
* WoWonder Social Network Platform 3.1 Authentication Bypass
* Zenario CMS 8.8.52729 SQL Injection
* Cerberus FTP Web Service 11 Cross Site Scripting
* Microsoft SharePoint Server 16.0.10372.20060 Server-Side Request Forgery
* Ability FTP Server 2.34 Denial Of Service
* Solar-Log 500 2.8.2 Password Disclosure
* Solar-Log 500 2.8.2 Incorrect Access Control
* NSClient++ 0.5.2.35 Remote Code Execution
* GravCMS 1.10.7 Arbitrary YAML Write / Update
* Student Result Management System 1.0 SQL Injection
* TextPattern CMS 4.8.7 Cross Site Scripting
* memono Notepad 4.2 Denial Of Service
* EasyFTP Server 1.7.0.11 Denial Of Service
* Sticky Notes Widget 3.0.6 Denial Of Service
* n+otes 1.6.2 Denial Of Service
* Internet Explorer jscript9.dll Memory Corruption
* WordPress Visitors-App 0.3 Cross Site Scripting

CXSecurity

* Sticky Notes Widget 3.0.6 Denial Of Service
* Microsoft SharePoint Server 16.0.10372.20060 Server-Side Request Forgery
* Ability FTP Server 2.34 Denial Of Service
* FreeFloat FTP Server 1.0 Denial Of Service
* Rocket.Chat 3.12.1 NoSQL Injection / Code Execution
* IcoFX 2.6 Buffer Overflow
* SAMI FTP Server 2.0.2 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

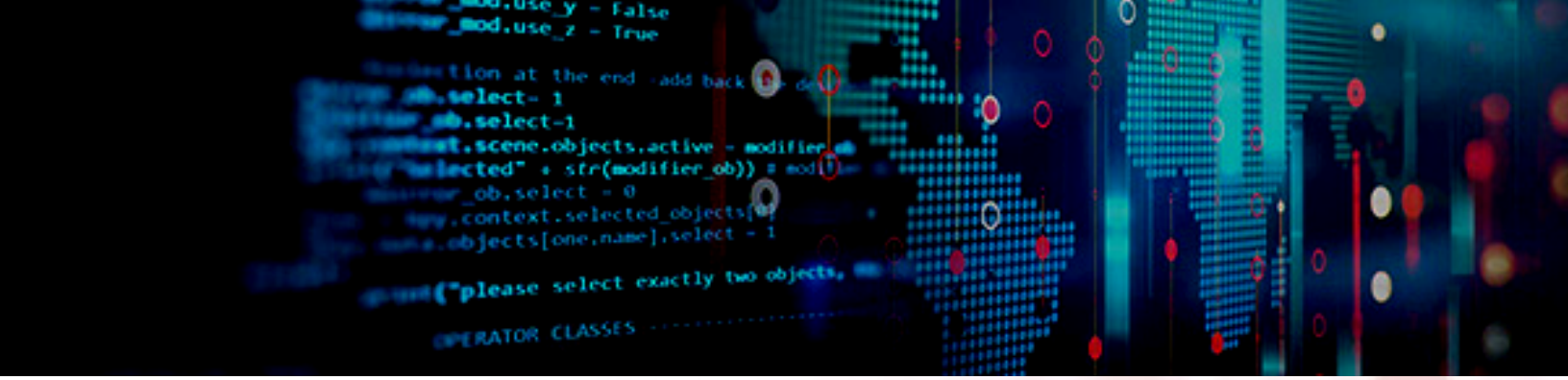
* [dos] Notex the best notes 6.4 - Denial of Service (PoC)
* [dos] Post-it 5.0.1 - Denial of Service (PoC)
* [dos] Secure Notepad Private Notes 3.0.3 - Denial of Service (PoC)
* [local] WibuKey Runtime 6.51 - 'WkSvW32.exe' Unquoted Service Path
* [webapps] OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution (Authenticated)
* [local] Spy Emergency 25.0.650 - 'Multiple' Unquoted Service Path
* [webapps] TextPattern CMS 4.8.7 - Remote Command Execution (Authenticated)
* [webapps] Small CRM 3.0 - 'Authentication Bypass' SQL Injection
* [webapps] Stock Management System 1.0 - 'user_id' Blind SQL injection (Authenticated)
* [webapps] COVID19 Testing Management System 1.0 - 'State' Stored Cross-Site-Scripting (XSS)
* [webapps] GLPI 9.4.5 - Remote Code Execution (RCE)
* [webapps] Accela Civic Platform 21.1 - 'contactSeqNumber' Insecure Direct Object References (IDOR)
* [webapps] Accela Civic Platform 21.1 - 'successURL' Cross-Site-Scripting (XSS)
* [webapps] WoWonder Social Network Platform 3.1 - Authentication Bypass
* [webapps] Zenario CMS 8.8.52729 - 'cID' Blind & Error based SQL injection (Authenticated)
* [webapps] Solar-Log 500 2.8.2 - Unprotected Storage of Credentials
* [webapps] Solar-Log 500 2.8.2 - Incorrect Access Control
* [webapps] Grocery crud 1.6.4 - 'order_by' SQL Injection
* [webapps] WordPress Plugin Database Backups 1.2.2.6 - 'Database Backup Download' CSRF
* [webapps] OpenEMR 5.0.0 - Remote Code Execution (Authenticated)
* [webapps] Microsoft SharePoint Server 16.0.10372.20060 - 'GetXmlDataFromDataSource' Server-Side Reque
* [webapps] Cerberus FTP Web Service 11 - 'svg' Stored Cross-Site Scripting (XSS)
* [webapps] Accela Civic Platform 21.1 - 'servProvCode' Cross-Site-Scripting (XSS)
* [dos] n+otes 1.6.2 - Denial of Service (PoC)

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*

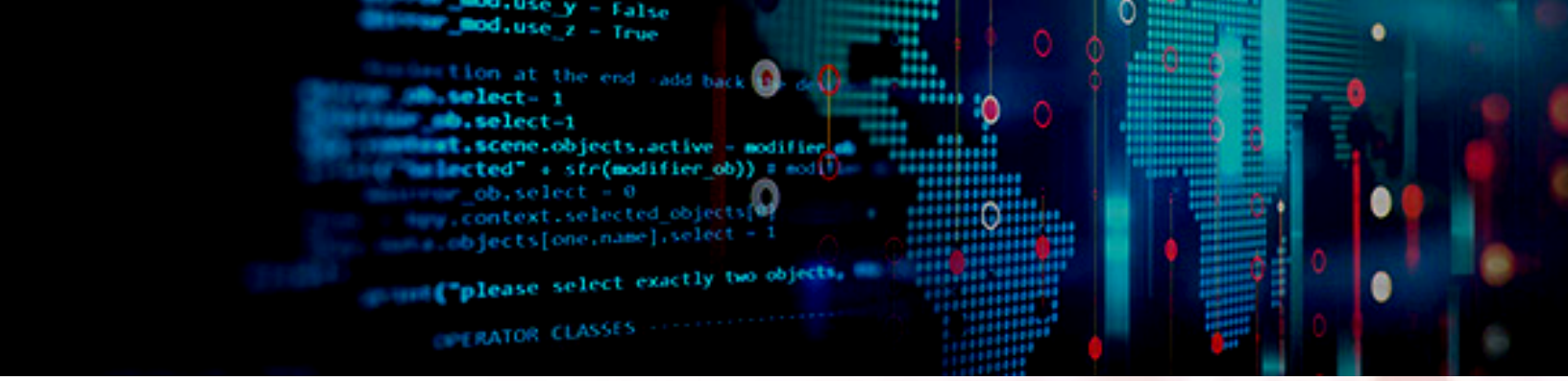
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.inspilip.gob.ec/OJS/public/site/images/krz/kz.gif
https://www.inspilip.gob.ec/OJS/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://chronos.samu.fortaleza.ce.gov.br/public/site/images/krz/kz.gif
https://chronos.samu.fortaleza.ce.gov.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://ejournal3.kemsos.go.id/public/site/images/krz/kz.gif
https://ejournal3.kemsos.go.id/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://makassar.lan.go.id/jap/public/site/images/krz/kz.gif
http://makassar.lan.go.id/jap/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://jurnalsetjen.kemendagri.go.id/public/site/images/krz/kz.gif
https://jurnalsetjen.kemendagri.go.id/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://ejournal.bappeda.jatengprov.go.id/public/site/images/krz/kz.gif
http://ejournal.bappeda.jatengprov.go.id/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://reunir.revistas.ufcg.edu.br/public/site/images/krz/kz.gif
https://reunir.revistas.ufcg.edu.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://raizes.revistas.ufcg.edu.br/public/site/images/krz/kz.gif
http://raizes.revistas.ufcg.edu.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://revistas.ufcg.edu.br/ActaBra/public/site/images/krz/kz.gif
http://revistas.ufcg.edu.br/ActaBra/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://etech.sc.senai.br/public/site/images/krz/kz.gif
https://etech.sc.senai.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://periodicos.ufsm.br/public/site/images/krz/kz.gif
https://periodicos.ufsm.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
https://siddhayatra.kemdikbud.go.id/public/site/images/krz/kz1.gif
https://siddhayatra.kemdikbud.go.id/public/site/images/krz/kz1.gif notified by Mr.Kro0oz.305
https://rsc.revistas.ufcg.edu.br/public/site/images/krzz/kz.gif
https://rsc.revistas.ufcg.edu.br/public/site/images/krzz/kz.gif notified by Mr.Kro0oz.305
https://journal.kpu.go.id/public/site/images/krz11/kz.gif
https://journal.kpu.go.id/public/site/images/krz11/kz.gif notified by Mr.Kro0oz.305
https://periodicos.ufsc.br/public/site/images/krz/kz.gif
https://periodicos.ufsc.br/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://multilingual.kemdikbud.go.id/public/site/images/krz/kz.gif
http://multilingual.kemdikbud.go.id/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305
http://www.bbkkp.go.id/ojs/prosiding/public/site/images/krz/kz.gif
http://www.bbkkp.go.id/ojs/prosiding/public/site/images/krz/kz.gif notified by Mr.Kro0oz.305



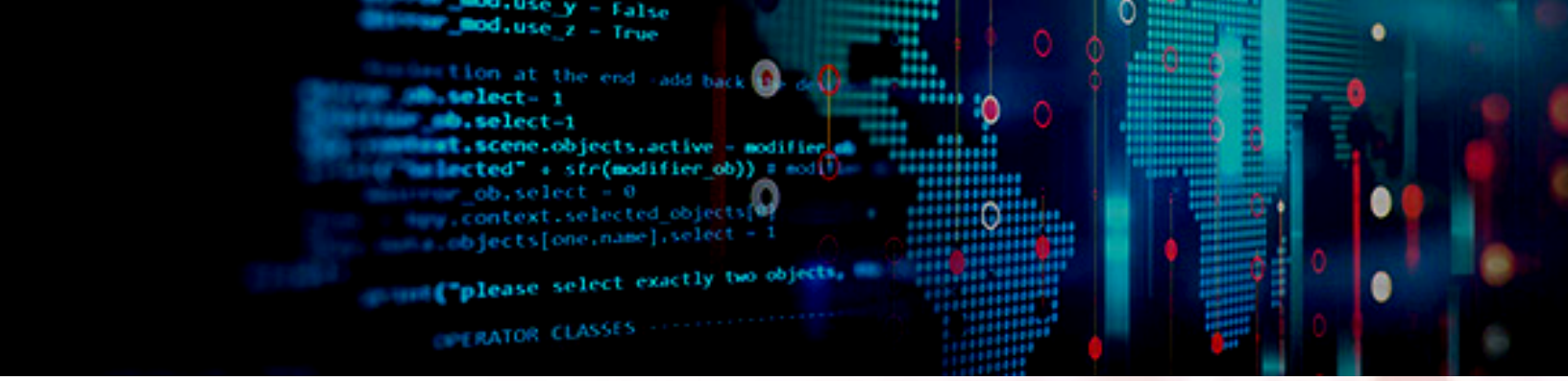
Dark Web News

Darknet Live

[Canadian Man Bought a Glock from an Undercover U.S. Fed]
A Canadian man was sentenced to prison for purchasing a Glock 19 from an undercover fed on the darkweb. (via darknetlive.com)
[The FBI Secretly Ran an Encrypted Messaging Platform]
The Federal Bureau of Investigation created its own encrypted device company and distributed thousands of devices to alleged criminals worldwide. (via darknetlive.com)
[PayPal Closed Someone's Account for Running Tor Relays]
PayPal apparently shut down a Tor supporter's account in response to activities supporting Tor, according to the EFF. (via darknetlive.com)
[SK Police Arrest 500 for Alleged Darkweb Drug Transactions]
The Seoul Metropolitan Police Agency apprehended more than 500 people suspected of buying or selling drugs on the darkweb. (via darknetlive.com)

Dark Web Link

[Encrypted Messaging System From FBI To Challenge The Criminals?]
The FBI had secretly launched an encrypted messaging system named Anom back in 2018. Anom had been very helpful in assisting in the yearlong sting operations. However, to date, everything about the secret messaging system had been under the veil. Lately, the law enforcement agencies across the U.S., Europe and Oceania had revealed the origins of [...] The post Encrypted Messaging System From FBI To Challenge The Criminals? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Insurance Ransom Payment: Azusa Officials Hid 2018 Cyber Attack]
The disclosure of the sensitive records of the Azusa Police Department being hacked by the hackers revealed something big about the insurance ransom payment. The city officials have lately acknowledged that they had experienced another hefty ransomware attack. They have also mentioned that they hid the information from the public for about two years. The [...] The post Insurance Ransom Payment: Azusa Officials Hid 2018 Cyber Attack appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[CP Possession Leads Nescopeck Man Face 100 Counts & Jail]
A man from Nescopeck pleaded guilty in February to 100 counts of CP possession and he has been sentenced to complete up to two years in jail after his sentencing. The accused had been identified as Eric S. Williams of aged 41 years. He had appeared before Joseph F. Sklarosky Jr, Luzerne County Judge, for sentencing on [...] The post CP Possession Leads Nescopeck Man Face 100 Counts & Jail appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* CISA Addresses the Rise in Ransomware Targeting Operational Technology Assets
* SAP Releases June 2021 Security Updates
* Adobe Releases Security Updates for Multiple Products
* Microsoft Releases June 2021 Security Updates
* Unpatched VMware vCenter Software
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Best Practices for Mapping to MITRE ATT&CKÂ®
* AA21-148A: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* Vulnerability Summary for the Week of May 31, 2021
* Vulnerability Summary for the Week of May 24, 2021

Zero Day Initiative Advisories

ZDI-CAN-13791: Fatek Automation
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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-06-11, 3 days ago. The vendor is given until 2021-10-09 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-13999: Fuji Electric
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-06-11, 3 days ago. The vendor is given until 2021-10-09 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-13802: SolarWinds
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-06-11, 3 days ago. The vendor is given until 2021-10-09 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-13925: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13965: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13923: 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 'Anonymous' was

reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13926: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13986: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13966: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13964: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13922: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13963: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-13924: 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 'Anonymous' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14022: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14033: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14034: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14024: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14020: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14014: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14021: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14016: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14018: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14015: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 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-14017: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 5 days ago. The vendor is given until 2021-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-4986-3

Ubuntu Security Notice 4986-3 - USN-4986-1 fixed a vulnerability in rpcbind. The update caused a regression resulting in rpcbind crashing in certain environments. This update fixes the problem. It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind to consume resources, leading to a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-2380-01

Red Hat Security Advisory 2021-2380-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation.

Ubuntu Security Notice USN-4971-2

Ubuntu Security Notice 4971-2 - USN-4971-1 fixed several vulnerabilities in libwebp. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that libwebp incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause libwebp to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2375-01

Red Hat Security Advisory 2021-2375-01 - PostgreSQL is an advanced object-relational database management system. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2372-01

Red Hat Security Advisory 2021-2372-01 - PostgreSQL is an advanced object-relational database management system. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2370-01

Red Hat Security Advisory 2021-2370-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Red Hat Security Advisory 2021-2371-01

Red Hat Security Advisory 2021-2371-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Ubuntu Security Notice USN-4986-2

Ubuntu Security Notice 4986-2 - USN-4986-1 fixed a vulnerability in rpcbind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind to consume resources, leading to a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-2150-01

Red Hat Security Advisory 2021-2150-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 3.11.452.

Red Hat Security Advisory 2021-2363-01

Red Hat Security Advisory 2021-2363-01 - GUPnP is an object-oriented open source framework for creating UPnP devices and control points, written in C using GObject and libsoup. The GUPnP API is intended to be easy to use, efficient and flexible.

Red Hat Security Advisory 2021-2364-01

Red Hat Security Advisory 2021-2364-01 - The libwebp packages provide a library and tools for the WebP graphics format. WebP is an image format with a lossy compression of digital photographic images. WebP consists of a codec based on the VP8 format, and a container based on the Resource Interchange File Format. Webmasters, web developers and browser developers can use WebP to compress, archive, and distribute digital images more efficiently. Issues addressed include buffer overflow and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2365-01

Red Hat Security Advisory 2021-2365-01 - The libwebp packages provide a library and tools for the WebP graphics format. WebP is an image format with a lossy compression of digital photographic images. WebP consists of a codec

based on the VP8 format, and a container based on the Resource Interchange File Format. Webmasters, web developers and browser developers can use WebP to compress, archive, and distribute digital images more efficiently. Issues addressed include buffer overflow and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2361-01

Red Hat Security Advisory 2021-2361-01 - PostgreSQL is an advanced object-relational database management system. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2360-01

Red Hat Security Advisory 2021-2360-01 - PostgreSQL is an advanced object-relational database management system. Issues addressed include an integer overflow vulnerability.

Ubuntu Security Notice USN-4986-1

Ubuntu Security Notice 4986-1 - It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind to consume resources, leading to a denial of service.

Red Hat Security Advisory 2021-2359-01

Red Hat Security Advisory 2021-2359-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2357-01

Red Hat Security Advisory 2021-2357-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2355-01

Red Hat Security Advisory 2021-2355-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, integer overflow, and out of bounds write vulnerabilities.

Red Hat Security Advisory 2021-2356-01

Red Hat Security Advisory 2021-2356-01 - Nettle is a cryptographic library that is designed to fit easily in almost any context: In crypto toolkits for object-oriented languages, such as C++, Python, or Pike, in applications like LSH or GNUPG, or even in kernel space.

Ubuntu Security Notice USN-4985-1

Ubuntu Security Notice 4985-1 - It was discovered that some Intel processors may not properly invalidate cache entries used by Intel Virtualization Technology for Directed I/O. This may allow a local user to perform a privilege escalation attack. Joseph Nuzman discovered that some Intel processors may not properly apply EIBRS mitigations and hence may allow unauthorized memory reads via sidechannel attacks. A local attacker could use this to expose sensitive information, including kernel memory. Various other issues were also addressed.

Red Hat Security Advisory 2021-2303-01

Red Hat Security Advisory 2021-2303-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2305-01

Red Hat Security Advisory 2021-2305-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2304-01

Red Hat Security Advisory 2021-2304-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2301-01

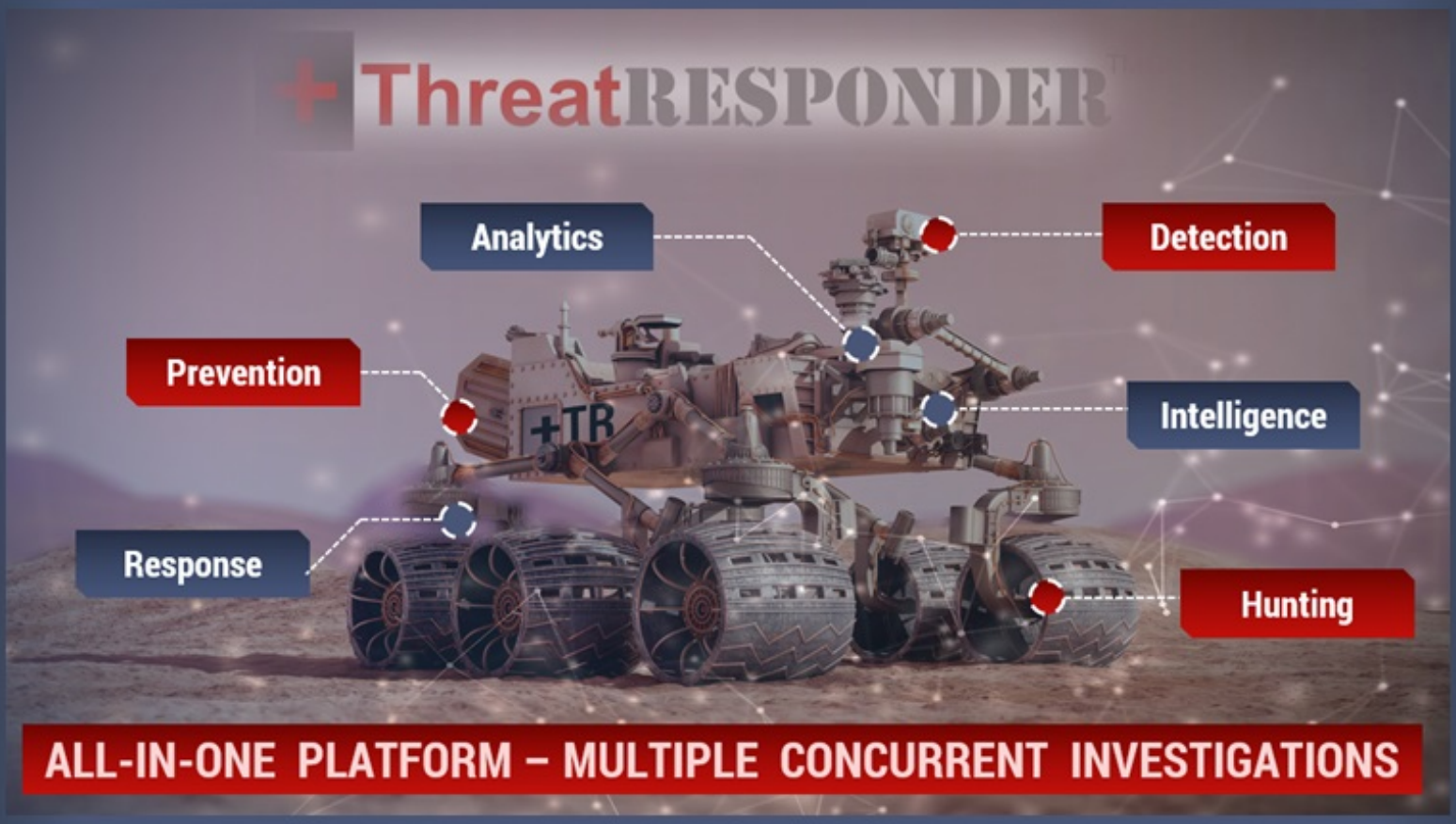
Red Hat Security Advisory 2021-2301-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

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:

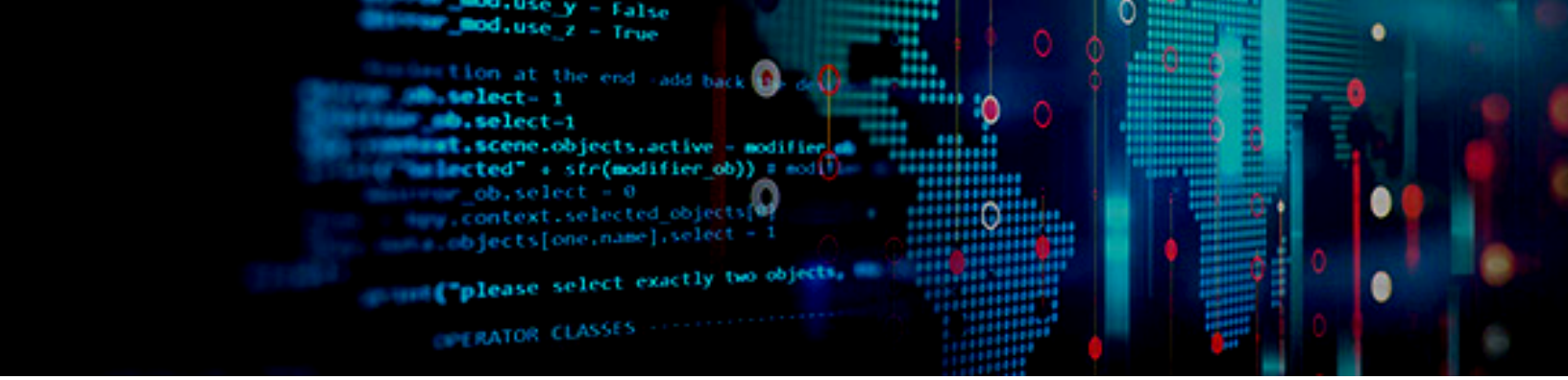
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

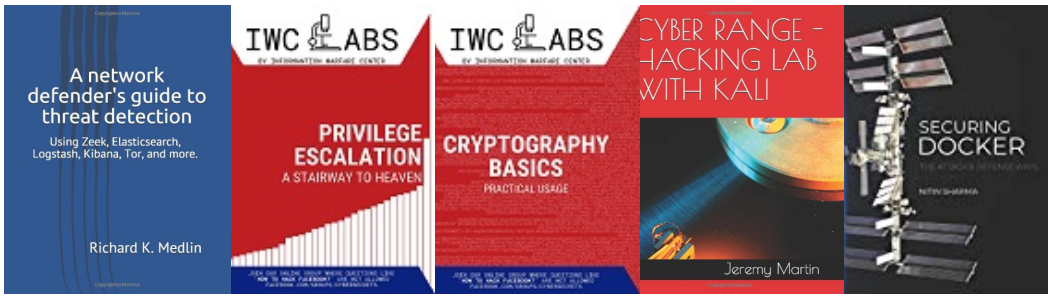


The Cyber Secrets publications on Amazon

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