Mar-01-21

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

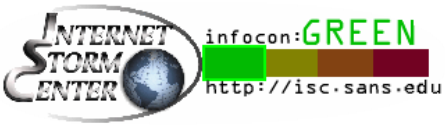
LINUX

ARGOS
APPLIED INTELLIGENCE

March 1, 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



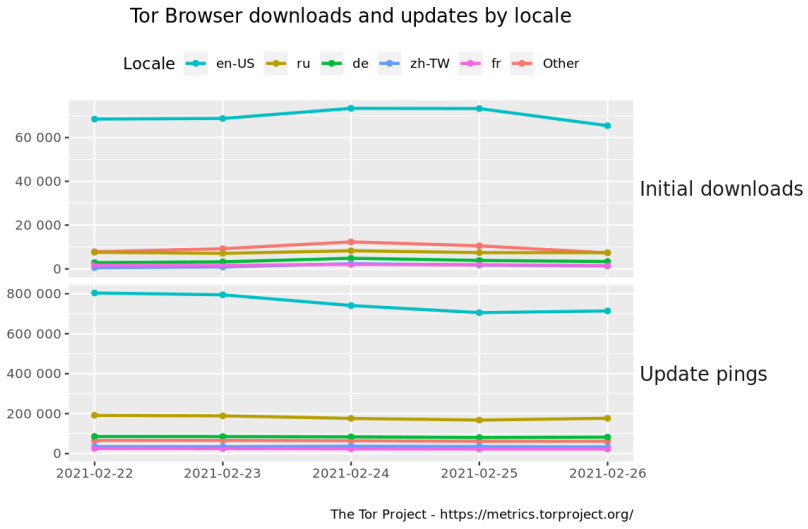
Internet Storm Center Infocon Status

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.

* The newest issue in the Cyber Secrets series (#6) - Incident Response: Evidence Preservation and Collection is now availible on Amazon!! This issue Incident Responce and Threat Hunting topics. Great for any security team.

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

Index of Sections

Packet Storm Security

* Hackers Improve SEO Before Deploying Malware
* Spyware Fan MBS Accused By US Intel Of Khashoggi Death
* Clubhouse's Security And Privacy Lag Behind Its Quick Growth
* Judge Approves $650 Million Settlement Of Privacy Lawsuit Against Facebook
* Go Malware Is Now Common, Having Been Adopted By Both APT And E-Crime Groups
* Old Foe Or New Enemy? Here's How Researchers Handle APT Attribution
* Oxford Lab With COVID-19 Research Links Targeted By Hackers
* Round Two Coming In Congressional Grilling Over SolarWinds
* Npower App Attack Exposed Customers' Bank Details
* Chart Shows Connections Between Cybercrime Groups
* Ukraine Says Russia Planted Malware In Its Document Portal
* Cisco Warns Of Critical Auth Bypass Security Flaw
* McDonald's Has An Intel Team Spying On Workers
* Four New Hacking Groups Are Targeting Critical Infrastructure
* VMware Warns Of Critical Remote Code Execution Flaw
* SolarWinds Hack Was The Work Of At Least 1,000 Engineers, Tech Execs Tell Senate
* Bombardier Data Posted On Ransomware Site Following FTA Hack
* SolarWinds Hackers Also Went After NASA And The FAA
* SolarWinds Hearing Announced By House Committees
* Hackers Are Selling Network Logins To The Highest Bidder
* Bitcoin Blockchain Helps Botnet From Being Taken Down
* 10K Microsoft Email Users Hit In FedEx Phishing Attack
* Hunting For Bugs In Telegram's Animated Stickers Remote Attack Surface
* Chinese Spyware Code Was Copied From America's NSA
* Parents Alerted To NurseryCam Security Breach

Krebs on Security

* Is Your Browser Extension a Botnet Backdoor?
* How $100M in Jobless Claims Went to Inmates
* Checkout Skimmers Powered by Chip Cards
* Mexican Politician Removed Over Alleged Ties to Romanian ATM Skimmer Gang
* U.S. Indicts North Korean Hackers in Theft of $200 Million
* Bluetooth Overlay Skimmer That Blocks Chip
* What's most interesting about the Florida water system hack? That we heard about it at all.
* Microsoft Patch Tuesday, February 2021 Edition
* Arrest, Raids Tied to 'U-Admin' Phishing Kit
* Facebook, Instagram, TikTok and Twitter Target Resellers of Hacked Accounts

Dark Reading

* New Jailbreak Tool Works on Most iPhones
* Universal Health Services Suffered $67 Million Loss Due to Ransomware Attack
* MSP Provider Builds Red Team as Attackers Target Industry
* Cybercrime 'Help Wanted': Job Hunting on the Dark Web
* Building a Next-Generation SOC Starts With Holistic Operations
* NSA Releases Guidance on Zero-Trust Architecture
* 'Nerd' Humor
* The Edge Pro Tip: Fasten Your Seatbelts
* Securing Super Bowl LV
* Attackers Turn Struggling Software Projects Into Trojan Horses
* After a Year of Quantum Advances, the Time to Protect Is Now
* Inside Strata's Plans to Solve the Cloud Identity Puzzle
* Microsoft Releases Free Tool for Hunting SolarWinds Malware
* North Korea's Lazarus Group Expands to Stealing Defense Secrets
* Ransomware, Phishing Will Remain Primary Risks in 2021
* Thousands of VMware Servers Exposed to Critical RCE Bug
* 5 Key Steps Schools Can Take to Defend Against Cyber Threats
* How to Avoid Falling Victim to a SolarWinds-Style Attack
* Cybercriminals Target QuickBooks Databases
* New APT Group Targets Airline Industry & Immigration

The Hacker News

* Gootkit RAT Using SEO to Distribute Malware Through Compromised Sites
* Why do companies fail to stop breaches despite soaring IT security investment?
* Chinese Hackers Targeted India's Power Grid Amid Geopolitical Tensions
* SolarWinds Blames Intern for Weak Password That Led to Biggest Attack in 2020
* North Korean Hackers Targeting Defense Firms with ThreatNeedle Malware
* ALERT: Malicious Amazon Alexa Skills Can Easily Bypass Vetting Process
* Cisco Releases Security Patches for Critical Flaws Affecting its Products
* Chinese Hackers Using Firefox Extension to Spy On Tibetan Organizations
* The Top Free Tools for Sysadmins in 2021
* Russian Hackers Targeted Ukraine Authorities With Supply-Chain Malware Attack
* Online Trackers Increasingly Switching to Invasive CNAME Cloaking Technique
* Experts Warns of Notable Increase in QuickBooks Data Files Theft Attacks
* Everything You Need to Know About Evolving Threat of Ransomware
* Critical RCE Flaws Affect VMware ESXi and vSphere Client - Patch Now
* Experts Find a Way to Learn What You're Typing During Video Calls

Security Week

* US Right-Wing Platform Gab Acknowledges it Was Hacked
* Suspected Chinese APT Group Targets Power Plants in India
* Asian Food Distribution Giant JFC International Hit by Ransomware
* Inside the Ransomware Economy
* Auth0 Names Jameeka Green Aaron as Chief Information Security Officer
* Data Privacy Startup TripleBlind Raises $8.2 Million in Seed Funding
* Boat Building Giant Beneteau Says Cyberattack Disrupted Production
* NSA Publishes Guidance on Adoption of Zero Trust Security
* US Shifts State Grant Focus to Extremism, Cyberthreats
* Cybersecurity M&A Round-Up for February 2021
* Vendor Quickly Patches Serious Vulnerability in NATO-Approved Firewall
* IT Asset Management Firm Axonius Raises $100 Million
* Judge Approves $650M Facebook Privacy Lawsuit Settlement
* HYAS Raises $16 Million to Hunt Adversary Infrastructure
* Meet the Vaccine Appointment Bots, and Their Foes
* Chinese Threat Actor Uses Browser Extension to Hack Gmail Accounts
* Security, Privacy Issues Found in Tens of COVID-19 Contact Tracing Apps
* Microsoft Releases Open Source Resources for Solorigate Threat Hunting
* Unprotected Private Key Allows Remote Hacking of Rockwell Controllers
* TikTok owner ByteDance to pay $92M in US privacy Settlement

Infosecurity Magazine

* United Airlines to Pay $49m to Settle False Data Claim
* Florida Police Arrest 12 Alleged Online Predators
* Facebook Photo-tagging Lawsuit Settled for $650m
* Half of Orgs Concerned Remote Working Puts Them at Greater Risk of Cyber-Attacks
* 70% of Orgs Facing New Security Challenges Due to #COVID19 Pandemic
* Go Malware Detections Increase 2000%
* Self-Assessment Tool Aims to Enhance Small Biz Security
* Berlin Resident Jailed for NHS Bomb Threats
* USA Third Most Affected by Stalkerware
* Atos Acquires Two Cybersecurity Companies
* FBI Investigating Michigan School District Hack
* Winners of Inaugural SBRC Cyber Community Awards Announced

KnowBe4 Security Awareness Training Blog RSS Feed

* [HEADS UP] New Dutch Data Breach Report Warns of Explosive Increase in Cyber Attacks and Stolen Perso
* New York State Education Department Warns of Phishing Campaign
* Phishing Attacks Double in 2020 While Carrying the Highest Month of Attacks on Record
* UK Police Arrest SIM-Swapping Gang Responsible for the Theft of Over $100 Million in Cryptocurrency
* Microsoft Dominates as the Most Impersonated Brand in Phishing Attacks
* [Heads Up] New Ryuk Ransomware Strain Now Worms Itself To All Your Windows LAN Devices
* New scary good deepfake videos of Tom Cruise show the threat to society is very real
* [Heads Up] Ransomware and Phishing Attacks Are Not Going Away in 2021
* Phishing Catch of the Day: Your Inbox Will be Deactivated
* The Dilemma: Best-of-Breed Stand-Alone or a Bundled Suite of tools?

ISC2.org Blog

* THE HEALTHCARE INTERNET OF THINGS - FOR BETTER OR WORSE
* Survey Says: CISSP and CCSP Among the Most In Demand IT Certifications of 2021
* Challenges and Misconceptions of Certificate Revocation in PKI
* The Future of Cybersecurity in Higher Education: Four Possible Scenarios
* Global Achievement Awards - What's new in 2021?

HackRead

* Crypto firm Tether claims hackers have demanded $24m in ransom
* Gab hacked - DDoSecrets leak profiles, posts, DMs, passwords online
* Microsoft release open-source CodeQL queries to hunt SolarWinds hacks
* Hackers using malicious Firefox extension to phish Gmail credentials
* Apple Glass may feature 3D Audio and Self-Cleaning in new patent
* Cryptocurrency exchange in liquidation due to hack, hacked again
* 5G Promises to Increase Adoption of Cryptocurrency Investing

Koddos

* Crypto firm Tether claims hackers have demanded $24m in ransom
* Gab hacked - DDoSecrets leak profiles, posts, DMs, passwords online
* Microsoft release open-source CodeQL queries to hunt SolarWinds hacks
* Hackers using malicious Firefox extension to phish Gmail credentials
* Apple Glass may feature 3D Audio and Self-Cleaning in new patent
* Cryptocurrency exchange in liquidation due to hack, hacked again
* 5G Promises to Increase Adoption of Cryptocurrency Investing

Naked Security

* Naked Security Live - Beware copyright scams
* S3 Ep21: Cryptomining clampdown, the 100-ton man, and ScamClub ads [Podcast]
* Keybase secure messaging fixes photo-leaking bug - patch now!
* Nvidia announces official "anti-cryptomining" software drivers
* Naked Security Live - How to calculate important things using a computer
* The massive coronavirus IT blunder with a funny side
* S3 Ep20: Corporate megahacking, true love gone bad, and tax grabs [Podcast]
* US names three North Koreans in laundry list of cybercrime charges
* "ScamClub" gang outed for exploiting iPhone browser bug to spew ads
* Romance scams at all-time high: here's what you need to know

Threat Post

* Malware Loader Abuses Google SEO to Expand Payload Delivery
* Passwords, Private Posts Exposed in Hack of Gab Social Network
* Firewall Vendor Patches Critical Auth Bypass Flaw
* Amazon Dismisses Claims Alexa 'Skills' Can Bypass Security Vetting Process
* Stalkerware Volumes Remain Concerningly High, Despite Bans
* Lazarus Targets Defense Companies with ThreatNeedle Malware
* Yeezy Fans Face Sneaker-Bot Armies for Boost 'Sun' Release
* Malware Gangs Partner Up in Double-Punch Security Threat
* Podcast: Ransomware Attacks Exploded in Q4 2020
* Protecting Sensitive Cardholder Data in Today's Hyper-Connected World

Null-Byte

* 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
* Start Learning How to Code in Just a Week
* Create a USB Mouse Jiggler to Keep a Target Computer from Falling Asleep (& Prank Friends Too)
* Boost Your Security with a VPN & Private Email Service
* How to Use RedRabbit for Pen-Testing & Post-Exploitation of Windows Machines

IBM Security Intelligence

* Offboarding: A Checklist for Safely Closing an Employee's Digital Doors
* Developers vs. Security: Who is Responsible for Application Security?
* Security Automation: The Future of Enterprise Defense
* 2021 X-Force Threat Intelligence Index Reveals Peril From Linux Malware, Spoofed Brands and COVID-19
* How a CISO's Executive Role Has Changed
* Manufacturing Cybersecurity Threats and How To Face Them
* Cyber Resilience Strategy Changes You Should Know in the EU's Digital Decade
* Braced for Impact: Fostering Good Cloud Security Posture Management
* The Uncertainty of Cybersecurity Hiring
* Firewall Services and More: What's Next for IT?

InfoWorld

* How to work with static anonymous functions in C# 9
* 15 ways to leave your cloud provider
* Nominate yourself for the 2021 Enterprise Architecture Awards
* 9 fine libraries for C++ programming
* Google Jetpack Compose Android UI toolkit now in beta
* IT Salary Survey 2021: The results are in
* Does AI-driven cloud computing need ethics guidelines?
* NumPy 1.20 introduces type annotations
* JDK 17: What's in store for Java 17
* IT Salary Survey 2021: Security and cloud computing certifications on the up

C4ISRNET - Media for the Intelligence Age Military

* 'Wakeup call': Report calls for massive AI investments to counter China
* Turkey's Baykar begins designing AI-powered combat drone
* NORAD is using artificial intelligence to see the threats it used to miss
* Who will lead the world in artificial intelligence?
* Unmanned systems, artificial intelligence dominate the IDEX showroom
* Report broadens conversation on space militarization and Space Force satellite defense
* 3 years later, DISA director reflects on how agency fought off elimination
* Securing data in a telework environment: modern defense solutions
* Space Force chief sees larger role for commercial industry in its missions
* Semiconductors, minerals: Supply chain review to cover key military tech

The Hacker Corner

Conferences

* 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!
* Best Web Application Conferences 2021 - 2022

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.

* zer0pts CTF 2021
* Winja CTF
* NahamCon CTF 2021
* UTCTF 2021
* vishwaCTF 2021
* BCA CTF 2021
* BCA CTF 2021
* LINE CTF 2021
* PoseidonCTF 2nd Edition **cancelled**
* SPRUSH CTF Quals 2021

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

* y0usef: 1
* BlueSky: 1
* Chill Hack: 1
* Jetty: 1
* DevGuru: 1

Tools & Techniques

Packet Storm Security Tools Links

* American Fuzzy Lop plus plus 3.10c
* Faraday 3.14.2
* Global Socket 1.4.25
* jSQL Injection 0.84
* Zeek 3.2.4
* OpenDNSSEC 2.1.8
* Global Socket 1.4.24
* Wapiti Web Application Vulnerability Scanner 3.0.4
* I2P 0.9.49
* Faraday 3.14.1

Kali Linux Tutorials

* GitLab Watchman : Monitoring GitLab For Sensitive Data Shared Publicly
* Understanding the Desktop as a Service Model
* OSV : Open Source Vulnerabilities
* UDdup : Urls De-Duplication Tool For Better Recon
* 7 Mac Tips that a New User Should Know
* Damn Vulnerable GraphQL Application
* BaphoDashBoard : Dashboard For Manage & Generate The Baphomet Ransomware
* C++ Assignment Help: Everything You Need to Know
* XSSTRON : Electron JS Browser To Find XSS Vulnerabilities
* 10 Best Linux Educational Software for Students

GBHackers Analysis

* Researchers Find a Way to Learn What Users Type in Video Calling
* New PDF Vulnerability Let Attackers Bypass the Signature Validation in PDF and Replace Content
* Unpatched SHAREit Flaw Let Attackers Execute Remote Code
* Microsoft will Enable Domain Controller Enforcement Mode to Address Zerologon Flaw
* Hackers Using 4 Zero-day Vulnerabilities to Attack Windows and Android Devices Remotely

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 178: Tools & Techniques: Opening an iPad
* Hack Your Stakeholder: Eliciting Intelligence Requirements with Design Thinking | SANS CTI Summit
* Riding the WAVE to Better Collaboration and Security | SANS CTI Summit 2021
* Episode 177: Tools & Techniques: Opening an iPhone

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

* Apple M1 Malware Found, Brave Browser Leaked DNS Queries - ThreatWire
* Phishing Using Morse Code, Signal Responds to Iran Ban, Chrome Zero Day News - ThreatWire
* Unlimited LTE Hotspot on PC via Phone or USB modem! -GlytchTips

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* GOLD PLAY BUTTON - REJECTED
* CALIFORNIA COVID VARIANT SUCKS
* ATT SELLING DIRECTV - cancel your subscription NOW
* YOUTUBE SPACES are DEAD

Security Now

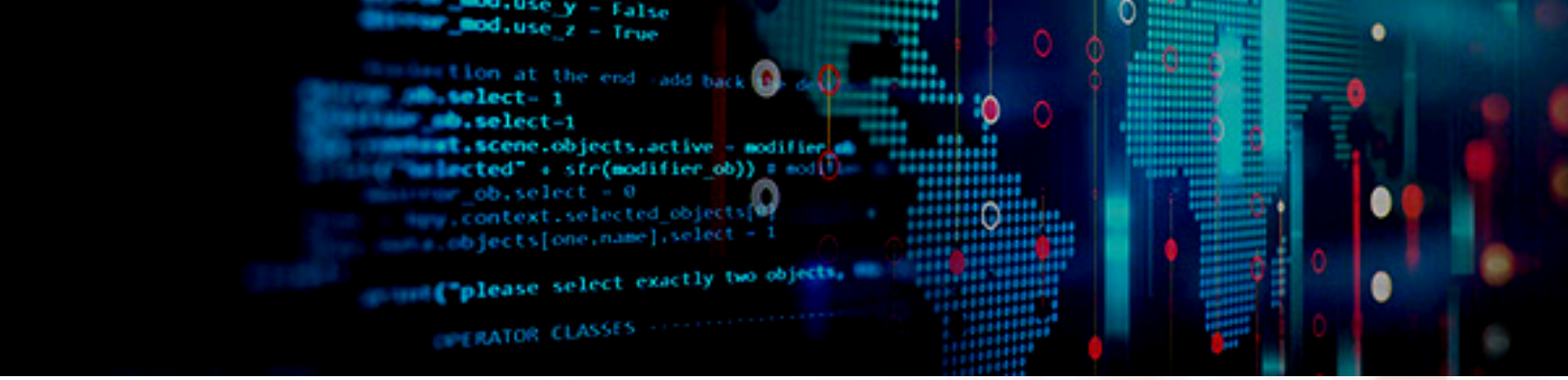
* Dependency Confusion - SHAREit's Security Update, Solorigate, Brave's "Private Window With Tor"
* C.O.M.B. - Florida Water Supply Hack Update, Major Patch Tuesday, Android SHAREit Vulnerability

Troy Hunt

* Weekly Update 232

Intel Techniques: The Privacy, Security, & OSINT Show

* 208-Amazon Privacy & VOIP Updates
* 207-VPN Routers Revisited



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

Unfortunately, at the time of this report, the RiskIQ resource was not availible.

FireEye

* How to Achieve and Maintain Continuous Cloud Compliance
* Metasploit Wrap-Up
* Celebrating Black History Today and Every Day
* Building a Holistic VRM Strategy That Includes the Web Application Layer
* Multiple Unauthenticated Remote Code Control and Execution Vulnerabilities in Multiple Cisco Products
* VMware vCenter Server CVE-2021-21972 Remote Code Execution Vulnerability: What You Need to Know
* Software Engineering, Vulnerability and Risk Management: Revolutionizing the Security Landscape at Ra
* How to Combat Alert Fatigue With Cloud-Based SIEM Tools
* Metasploit Wrap-Up
* Take the Full-Stack Approach to Securing Your Modern Attack Surface

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For February, 2021
* FortiLogger 4.4.2.2 Arbitrary File Upload
* Concrete5 8.5.4 Cross Site Scripting
* Trojan-Spy.Win32.Stealer.osh Insecure Permissions
* Online Catering Reservation System 1.0 Code Execution
* Covid-19 Contact Tracing System 1.0 Code Execution
* VMware vCenter Server 7.0 Arbitrary File Upload
* Backdoor.Win32.RemoteManipulator.fdo Insecure Permissions
* WiFi Mouse 1.7.8.5 Remote Code Execution
* Package Control Arbitrary File Write
* Microsoft DirectWrite fsg_ExecuteGlyph Buffer Overflow
* Chrome DataElement Out-Of-Bounds Read
* Trojan-Proxy.Win32.Delf.ai Buffer Overflow
* Doctor Appointment System 1.0 Cross Site Scripting
* Trojan-Dropper.Win32.Daws.etlm Unauthenticated Reboot
* Online Catering Reservation System 1.0 SQL Injection
* VisualWare MyConnection Server 11.x Remote Code Execution
* Triconsole 3.75 Cross Site Scripting
* Zenphoto CMS 1.5.7 Shell Upload
* Remote Desktop Web Access Authentication Timing Attack
* Trojan.Win32.Hotkeychick.am Insecure Permissions
* Backdoor.Win32.Azbreg.amw Insecure Permissions
* Trojan-Spy.Win32.SpyEyes.elr Insecure Permissions
* Trojan-Dropper.Win32.Daws.etlm Unauthenticated Reboot
* Squid 4.14 / 5.0.5 Code Execution / Double Free

CXSecurity

* Covid-19 Contact Tracing System 1.0 Code Execution
* VMware vCenter Server 7.0 Unauthenticated File Upload
* Unified Remote 3.9.0.2463 Remote Code Execution
* SLMail 5.1.0.4420 Remote Code Execution
* SpotAuditor 5.3.5 Denial Of Service
* ASUS Remote Link 1.1.2.13 Remote Code Execution
* HFS (HTTP File Server) 2.3.x Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

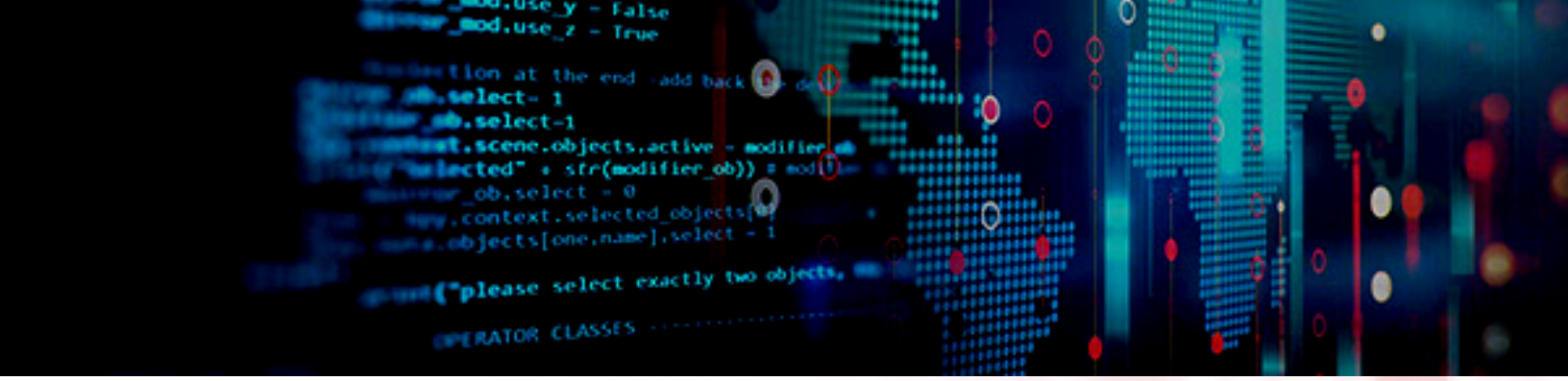
* [webapps] Covid-19 Contact Tracing System 1.0 - Remote Code Execution (Unauthenticated)
* [webapps] Online Catering Reservation System 1.0 - Remote Code Execution (Unauthenticated)
* [webapps] VMware vCenter Server 7.0 - Unauthenticated File Upload
* [remote] WiFi Mouse 1.7.8.5 - Remote Code Execution
* [webapps] FortiLogger 4.4.2.2 - Unauthenticated Arbitrary File Upload (Metasploit)
* [remote] Remote Desktop Web Access - Authentication Timing Attack (Metasploit Module)
* [webapps] LightCMS 1.3.4 - 'exclusive' Stored XSS
* [webapps] Triconsole 3.75 - Reflected XSS
* [webapps] Simple Employee Records System 1.0 - File Upload RCE (Unauthenticated)
* [webapps] Vehicle Parking Management System 1.0 - 'catename' Persistent Cross-Site Scripting (XSS)
* [remote] ASUS Remote Link 1.1.2.13 - Remote Code Execution
* [webapps] LayerBB 1.1.4 - 'search_query' SQL Injection
* [dos] Product Key Explorer 4.2.7 - 'multiple' Denial of Service (PoC)
* [dos] SpotAuditor 5.3.5 - 'multiple' Denial Of Service (PoC)
* [local] Softros LAN Messenger 9.6.4 - 'SoftrosSpellChecker' Unquoted Service Path
* [remote] Unified Remote 3.9.0.2463 - Remote Code Execution
* [local] LogonExpert 8.1 - 'LogonExpertSvc' Unquoted Service Path
* [remote] python jsonpickle 2.0.0 - Remote Code Execution
* [remote] HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
* [webapps] Batflat CMS 1.3.6 - 'multiple' Stored XSS
* [webapps] Monica 2.19.1 - 'last_name' Stored XSS
* [webapps] Beauty Parlour Management System 1.0 - 'sername' SQL Injection
* [webapps] OpenText Content Server 20.3 - 'multiple' Stored Cross-Site Scripting
* [local] dataSIMS Avionics ARINC 664-1 - Local Buffer Overflow (PoC)
* [webapps] Online Exam System With Timer 1.0 - 'email' SQL injection Auth Bypass

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*

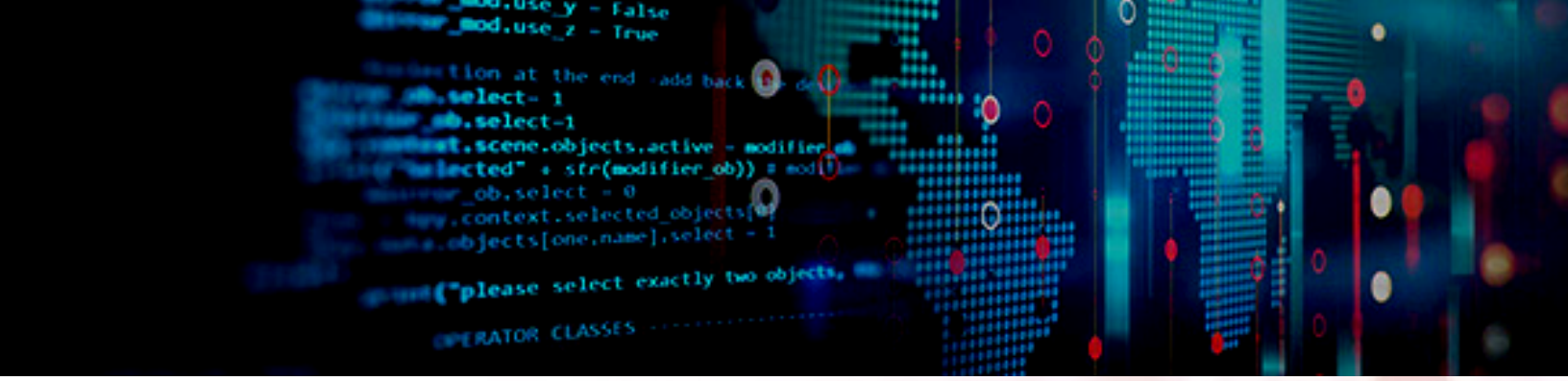
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://transparencia.escuinapa.gob.mx
https://transparencia.escuinapa.gob.mx notified by HighTech
https://informame.escuinapa.gob.mx
https://informame.escuinapa.gob.mx notified by HighTech
https://www.umv.gov.co/tmp/index.html
https://www.umv.gov.co/tmp/index.html notified by org0n
http://dpmd.bonebolangokab.go.id/34.htm
http://dpmd.bonebolangokab.go.id/34.htm notified by Anonymous09
http://dinastph.sumutprov.go.id/34.htm
http://dinastph.sumutprov.go.id/34.htm notified by prizeHdru
http://lms.icta.go.ke
http://lms.icta.go.ke notified by Ayyıldız Tim
http://asdsp.kilimo.go.ke
http://asdsp.kilimo.go.ke notified by Ayyıldız Tim
https://sitara.pta-babel.go.id
https://sitara.pta-babel.go.id notified by ONE HAT CYBER TEAM
https://monpeg.pta-babel.go.id
https://monpeg.pta-babel.go.id notified by ONE HAT CYBER TEAM
https://aco.pta-babel.go.id
https://aco.pta-babel.go.id notified by ONE HAT CYBER TEAM
http://systems.laguna.gov.ph/pwnd.html
http://systems.laguna.gov.ph/pwnd.html notified by Mr.GonzX
http://sipp.pn-simpangtigaredelong.go.id/r0t.txt
http://sipp.pn-simpangtigaredelong.go.id/r0t.txt notified by r#0t_p4c$m4n
http://sipp.pa-sragen.go.id/r0t.txt
http://sipp.pa-sragen.go.id/r0t.txt notified by r#0t_p4c$m4n
https://muninuevochimbote.gob.pe
https://muninuevochimbote.gob.pe notified by bandz.in
http://perpustakaan.pn-kuningan.go.id/miris.html
http://perpustakaan.pn-kuningan.go.id/miris.html notified by Mr.Rm19
http://latihan.pn-kuningan.go.id/miris.html
http://latihan.pn-kuningan.go.id/miris.html notified by Mr.Rm19
http://aula.pn-kuningan.go.id/miris.html
http://aula.pn-kuningan.go.id/miris.html notified by Mr.Rm19



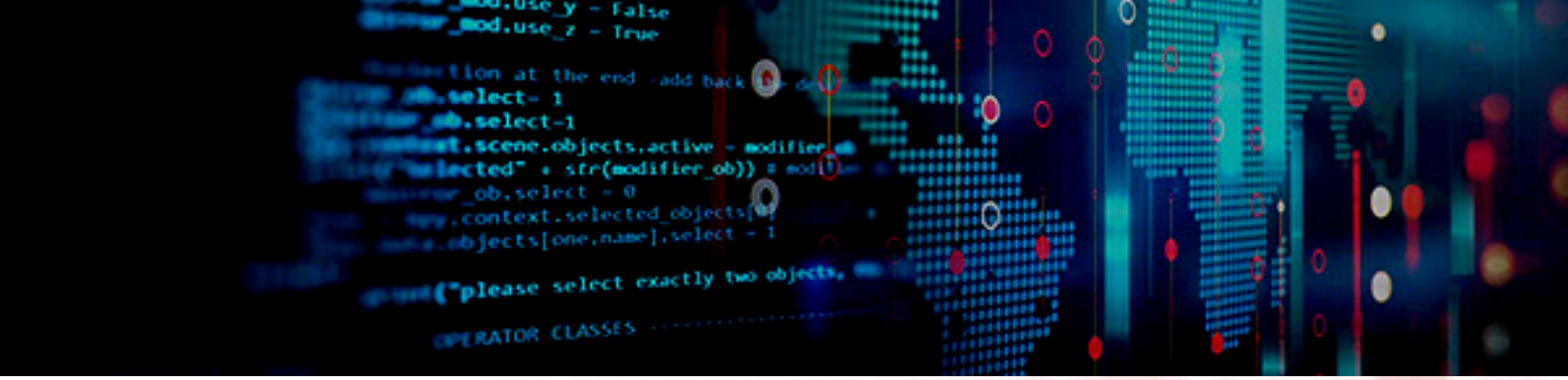
Dark Web News

Darknet Live

Three Arrested for Selling Opioids on Darkweb Markets
The FBI relied on a Bitcoin trader during an investigation into the suspected operators of two darkweb vendor accounts. (via darknetlive.com)
Four Arrested in Germany for Selling Drugs on the Darkweb
German Customs arrested four men suspected of selling prescription medication and other drugs on the darkweb. (via darknetlive.com)
Australian Man Sentenced for Selling Ecstasy on the Darkweb
An Australian man was sentenced to prison after pleading guilty to distributing MDMA on the darkweb. (via darknetlive.com)
Brave Browser Leaked DNS Queries for Onion Services
Brave, a browser that allows users to access onion services, had a bug that sent queries for onion addresses to public DNS resolvers. (via darknetlive.com)

Dark Web Link

Twitter Scam: Fraudsters Earned $145K+ in Bitcoin, Ethereum And Dogecoin
The cryptocurrency scammers had earned a minimum of $145,000 this week through promoting fake giveaways using hacked verified Twitter accounts, causing massive Twitter scam. Last month it had been reported that an increasing trend had been spotted where verified Twitter accounts had been hacked for promoting the fake cryptocurrency giveaways. During that time, the series [...] The post Twitter Scam: Fraudsters Earned $145K+ in Bitcoin, Ethereum And Dogecoin appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Cryptophone: A New Way To Keep Your Cryptocurrency Safe
Cryptocurrencies or digital currencies seem to be the new currency that the majority of people rely on. Being digital assets, it is vulnerable to getting hacked, and people owing them can get so-called "wallet-rupt” if they do not care about its security. This thought has given rise to what we will discuss here, Cryptophone. Additionally, [...] The post Cryptophone: A New Way To Keep Your Cryptocurrency Safe appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Facebook Illegal Trade: Experts Call To Address Issue
The experts who had been tracking the online crime had urged the United States prosecutors to address the Facebook illegal trade of drugs and other goods through its pages. It has been seen that the social media giant had allegedly facilitated the illicit trade amid the ongoing opioid crisis in the U.S. The Facebook illegal trade is not solely [...] The post Facebook Illegal Trade: Experts Call To Address Issue appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* NSA Releases Guidance on Zero Trust Security Model
* Cisco Releases Security Updates
* Mozilla Releases Security Updates for Thunderbird, Firefox ESR, and Firefox
* VMware Releases Multiple Security Updates
* CISA Releases Joint Cybersecurity Advisory on Exploitation of Accellion File Transfer Appliance
* SonicWall Releases Additional Patches
* Cisco Releases Security Updates for AnyConnect Secure Mobility Client
* Google Releases Security Updates for Chrome
* AA21-055A: Exploitation of Accellion File Transfer Appliance
* AA21-048A: AppleJeus: Analysis of North Korea's Cryptocurrency Malware
* Vulnerability Summary for the Week of February 22, 2021
* Vulnerability Summary for the Week of February 15, 2021

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-0672-01

Red Hat Security Advisory 2021-0672-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. Issues addressed include a buffer overflow vulnerability.

Genua GenuGate High Resistance Firewall Authentication Bypass

Genua GenuGate High Resistance Firewall versions prior to 10.1 p4, 9.6 p7, and 9.0 Z p19 suffer from an authentication bypass vulnerability.

Red Hat Security Advisory 2021-0681-01

Red Hat Security Advisory 2021-0681-01 - The podman tool manages pods, container images, and containers. It is part of the libpod library, which is for applications that use container pods. Container pods is a concept in Kubernetes.

Red Hat Security Advisory 2021-0670-01

Red Hat Security Advisory 2021-0670-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0663-01

Red Hat Security Advisory 2021-0663-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Red Hat Security Advisory 2021-0669-01

Red Hat Security Advisory 2021-0669-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-4754-2

Ubuntu Security Notice 4754-2 - USN-4754-1 fixed a vulnerability in Python. The fix for CVE-2021-3177 introduced a regression in Python 2.7. This update reverts the security fix pending further investigation. It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service.

Ubuntu Security Notice USN-4754-1

Ubuntu Security Notice 4754-1 - It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service.

Ubuntu Security Notice USN-4755-1

Ubuntu Security Notice 4755-1 - It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Ubuntu Security Notice USN-4752-1

Ubuntu Security Notice 4752-1 - Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen discovered that legacy pairing and secure-connections pairing authentication in the Bluetooth protocol could allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. A physically proximate attacker could use this to impersonate a previously paired Bluetooth device. Jay Shin discovered that the ext4 file system implementation in the Linux kernel did not properly handle directory access with broken indexing, leading to an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4751-1

Ubuntu Security Notice 4751-1 - It was discovered that the console keyboard driver in the Linux kernel contained a race condition. A local attacker could use this to expose sensitive information. Minh Yuan discovered that the tty driver in the Linux kernel contained race conditions when handling fonts. A local attacker

could possibly use this to expose sensitive information. Bodong Zhao discovered a use-after-free in the Sun keyboard driver implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4753-1

Ubuntu Security Notice 4753-1 - It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

Ubuntu Security Notice USN-4750-1

Ubuntu Security Notice 4750-1 - Bodong Zhao discovered a use-after-free in the Sun keyboard driver implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4749-1

Ubuntu Security Notice 4749-1 - Bodong Zhao discovered a use-after-free in the Sun keyboard driver implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4748-1

Ubuntu Security Notice 4748-1 - It was discovered that the jfs file system implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to possibly cause a denial of service. It was discovered that the memory management subsystem in the Linux kernel did not properly handle copy-on-write operations in some situations. A local attacker could possibly use this to gain unintended write access to read-only memory pages. Various other issues were also addressed.

Ubuntu Security Notice USN-4747-2

Ubuntu Security Notice 4747-2 - USN-4747-1 fixed a vulnerability in screen. This update provides the corresponding update for Ubuntu 14.04 ESM. Felix Weinmann discovered that GNU Screen incorrectly handled certain character sequences. A remote attacker could use this issue to cause GNU Screen to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-0100-01

Red Hat Security Advisory 2021-0100-01 - The file-integrity-operator image update is now available for OpenShift Container Platform 4.7. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2020-5364-01

Red Hat Security Advisory 2020-5364-01 - 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 extra low-latency container images for Red Hat OpenShift Container Platform 4.7. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2021-0664-01

Red Hat Security Advisory 2021-0664-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Red Hat Security Advisory 2020-5633-01

Red Hat Security Advisory 2020-5633-01 - 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 container images for Red Hat OpenShift Container Platform 4.7.0. Issues addressed include bypass, denial of service, integer overflow, man-in-the-middle, and memory leak vulnerabilities.

Red Hat Security Advisory 2021-0661-01

Red Hat Security Advisory 2021-0661-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.8.0.

Red Hat Security Advisory 2021-0659-01

Red Hat Security Advisory 2021-0659-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.8.0 ESR.

Red Hat Security Advisory 2020-5634-01

Red Hat Security Advisory 2020-5634-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.0.

Red Hat Security Advisory 2021-0662-01

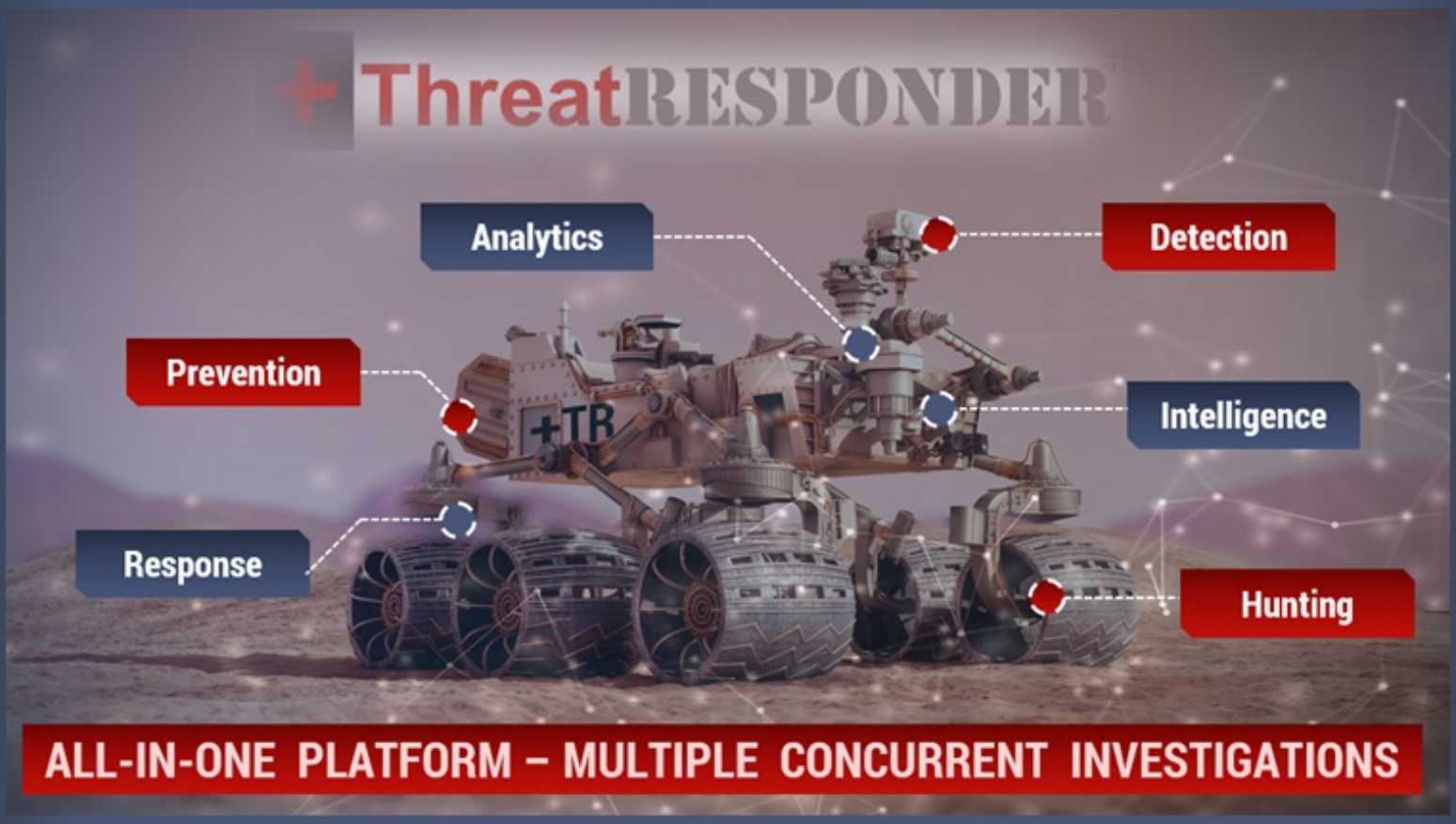
Red Hat Security Advisory 2021-0662-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.8.0.

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:

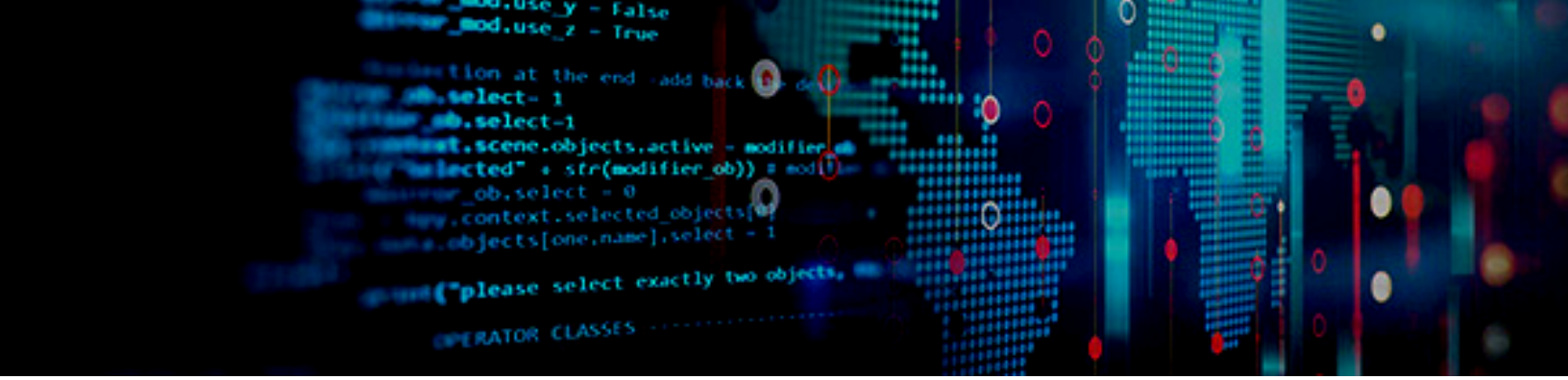
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

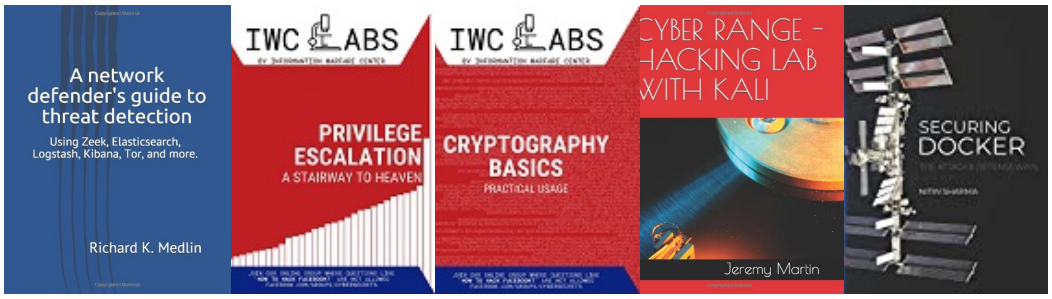


The Cyber Secrets publications on Amazon

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