
Oct-04-21
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

October 4, 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

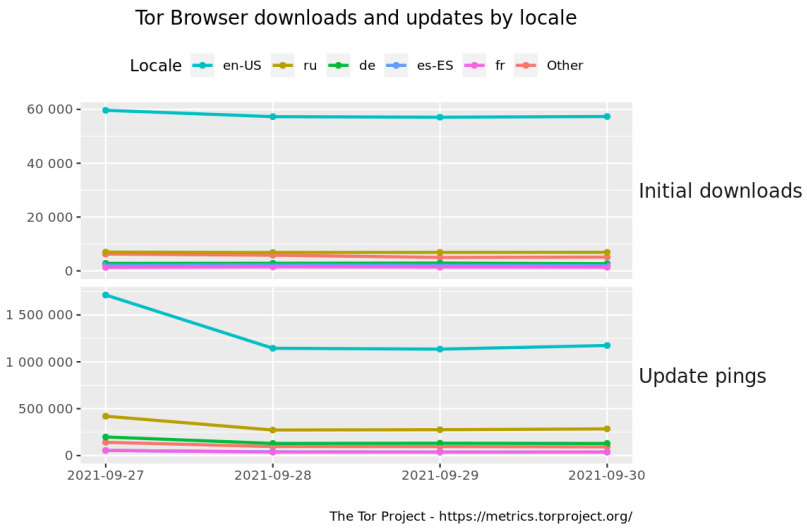
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

Just released!!! Web App Hacking: Carnage & Pwnage



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.

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

Index of Sections

Packet Storm Security

* Facebook, Instagram, WhatsApp Go Down
* Fraudster Jailed For Stealing Military Records, Benefits
* Ukrainian Cops Cuff Two Over $150m Ransomware Gang Allegations, Seize $1.3m In Cryptocurrency
* Researcher Refuses Telegram's Bounty Award, Discloses Bug
* MFA Glitch Leads To 6K+ Coinbase Customers Getting Robbed
* Neiman Marcus Data Breach Impacts 4.6 Million Customers
* FCC Aggressively Moves To Block Spam Calls
* IKEA Put Cameras In Employee Warehouse Bathrooms
* Apple Pay With Visa Hacked To Make Payments With Locked iPhones
* Conti Ransomware Expands Ability To Blow Up Backups
* Anonymous Has Leaked Disk Images From Epik
* Apple AirTags Can Be Weaponized For XSS Attacks
* Fears Surrounding Pegasus Spyware Prompt New Trojan Campaign
* Google Launches Rewards Program For Tsunami
* Cryptocurrency Expert Admits Aiding North Korea
* Weaponized Telegram Bots Compromise PayPal Accounts
* German IT Security Watchdog Examines Xiaomi Phone
* CIA Officials Under Trump Discussed Assassinating Julian Assange
* Credential Spear-Phishing Uses Spoofed Zix Encrypted Email
* UK Umbrella Payroll Firm GiantPay Confirms Attack
* Microsoft Warns Of Malware With Persistent Backdoor For Hackers
* Old Coal Plant Is Now Mining Bitcoin For A Utility Company
* Frustrated Dev Drops Three Zero Day Vulns Affecting Apple iOS 15 After Six Month Wait
* How To Find And Remove Spyware From Your Phone
* Mr Goxx, The Crypto Trading Hamster Beat Human Investors

Krebs on Security

* What Happened to Facebook, Instagram, & WhatsApp?
* FCC Proposal Targets SIM Swapping, Port-Out Fraud
* The Rise of One-Time Password Interception Bots
* Apple AirTag Bug Enables 'Good Samaritan' Attack
* Indictment, Lawsuits Revive Trump-Alfa Bank Story
* Does Your Organization Have a Security.txt File?
* Trial Ends in Guilty Verdict for DDoS-for-Hire Boss
* Customer Care Giant TTEC Hit By Ransomware
* Microsoft Patch Tuesday, September 2021 Edition
* KrebsOnSecurity Hit By Huge New IoT Botnet "Meris"

Dark Reading

* One Identity Acquires OneLogin to Boost Identity Security Portfolio
* New Atom Silo Ransomware Group Targets Confluence Servers
* Law Enforcement Agencies Seize $375K in Ukraine Ransomware Bust
* CISA Kicks Off Cybersecurity Awareness Month
* Mandiant Confirms Name Change from FireEye, Inc. to Mandiant, Inc.
* Name That Edge Toon: Mobile Monoliths
* Top 5 Skills Modern SOC Teams Need to Succeed
* Companies Face Issues as Let's Encrypt Root Certificate Expires
* Why Windows Print Spooler Remains a Big Attack Target
* 4.6M Neiman Marcus Online Customers Alerted to Data Breach
* CISA and Girls Who Code Partner to Create Career Pathways for Young Women
* It's Time to Rethink Identity and Authentication
* Enterprises Planning SecOps Technology Deployments
* More Than 90% of Q2 Malware Was Hidden in Encrypted Traffic
* Akamai Acquires Guardicore in $600M Deal
* 10 Recent Examples of How Insider Threats Can Cause Big Breaches and Damage
* FireEye Products & McAfee Enterprise Merge to Create $2B Entity
* You're Going to Be the Victim of a Ransomware Attack
* The New Security Basics: 10 Most Common Defensive Actions
* 5 Ways to Become a Better Cyber-Threat Exterminator
* SecZetta Announces $20.5M Series B Funding
* Shades of SolarWinds Attack Malware Found in New 'Tomiris' Backdoor
* Startup Beyond Identity Now Offers Passwordless Multifactor Authentication for Consumers
* 50% of Servers Have Weak Security Long After Patches Are Released
* Salt Security Finds Widespread Elastic Stack API Security Vulnerability that Exposes Customer and Sys

The Hacker News

* Creating Wireless Signals with Ethernet Cable to Steal Data from Air-Gapped Systems
* Poorly Configured Apache Airflow Instances Leak Credentials for Popular Services
* A New APT Hacking Group Targeting Fuel, Energy, and Aviation Industries
* The Shortfalls of Mean Time Metrics in Cybersecurity
* Apple Pay Can be Abused to Make Contactless Payments From Locked iPhones
* Chinese Hackers Used a New Rootkit to Spy on Targeted Windows 10 Users
* Beware of Fake Amnesty International Antivirus for Pegasus that Hacks PCs with Malware
* Update Google Chrome ASAP to Patch 2 New Actively Exploited Zero-Day Flaws
* New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught
* Incentivizing Developers is the Key to Better Security Practices
* Here's a New Free Tool to Discover Unprotected Cloud Storage Instances

* New Tomiris Backdoor Found Linked to Hackers Behind SolarWinds Cyberattack
* Cybersecurity Firm Group-IB's CEO Arrested Over Treason Charges in Russia
* Facebook Releases New Tool That Finds Security and Privacy Bugs in Android Apps
* Beware! This Android Trojan Stole Millions of Dollars from Over 10 Million Users

Security Week

* Two 'Prolific' Ransomware Operators Arrested in Ukraine
* Hackers Stole Cryptocurrency From Thousands of Coinbase Accounts
* Expired Let's Encrypt Root Certificate Causes Problems for Many Companies
* Pottawatomie County Fixing Systems After Ransomware Attack
* Cybersecurity M&A Roundup: 43 Deals Announced in September 2021
* PoC Exploit Released for macOS Gatekeeper Bypass
* Google Pledges $1 Million to Secure Open Source Program
* Suit Blames Baby's Death on Cyberattack at Alabama Hospital
* McAfee Enterprise, FireEye Products Merged Into $2B Entity
* ChamelGang Hackers Target Energy, Aviation, and Government Sectors
* Third-Party Identity Risk Provider SecZetta Raises $20.5 Million
* Proposed Bill Would Require Organizations to Report Ransomware Payments
* Neiman Marcus Confirms Payment Cards Compromised in Data Breach
* Google Patches Two More Exploited Zero-Day Vulnerabilities in Chrome
* Google Patches Vulnerability in Cloud Endpoints Proxy
* Threat Actor Promises Pegasus Spyware Protection, Serves Trojan Instead
* Hackers Can Exploit Apple AirTag Vulnerability to Lure Users to Malicious Sites
* Xage Lands DOE Contract to Bring Zero Trust Principles to Emergency Responders
* Telemetry Report Shows Patch Status of High-Profile Vulnerabilities
* GriftHorse Android Trojan Infects Over 10 Million Devices Worldwide
* New CISA Tool Helps Organizations Assess Insider Threat Risks
* Contactless Payment Card Hack Affects Apple Pay, Visa
* Turkish National Charged for DDoS Attack on U.S. Company
* Optimizing Monitoring Services For Intelligence Teams

Infosecurity Magazine

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

KnowBe4 Security Awareness Training Blog RSS Feed

* New James Bond Movie is Cybercriminals Shiniest Phishbait
* Hackers rob thousands of Coinbase customers using phishing attacks and an MFA flaw
* Phishing Attacks Maintain "New Normal" Elevated Levels into the Middle of 2021
* 90% of All Cyber Attacks on Organizations Involve Social Engineering
* Phishing Campaign Impersonates Zix Messages
* Happy Cybersecurity Awareness Month 2021 from KnowBe4!
* Europol: Italian Mafia Tied to Cybercriminals Responsible for â‚¬10 Million in Cyberattacks
* 5th Circuit Court Finds Cyber Insurer Must Pay for $1 Million Social Engineering Attack
* Phishing Kits and Phishing-as-a-Service Responsible for Over 300,000 URLs Used in Phishing Attacks
* Someone's Impersonating the California DMV in Texts

ISC2.org Blog

* (ISC)² Celebrates Cybersecurity Awareness Month With Treasure Trove of Knowledge Building Resour
* House Delays U.S. Infrastructure Bill Vote - Cybersecurity Funding in Jeopardy? And What Security Pra
* Younger Workers: Security Is a 'Hindrance'
* How Will $1.9 Billion for Cybersecurity Protect American Infrastructure?
* How Continuous Monitoring is a Driver of Effective Risk Management

HackRead

* Facebook down with Messenger, Instagram, WhatsApp service disruption
* Ex-army admin jailed for 12 years over US military health data theft
* Android flubot malware installs itself by faking security update
* Hackers exploit 2FA flaw to steal crypto from 6,000 Coinbase users
* Anonymous leaks more EPIK host data; 'larger than previous leak'
* Apple AirTags can be used as trojan for credential hacking
* GriftHorse Android malware hit 10 million devices in 70 countries

Koddos

* Facebook down with Messenger, Instagram, WhatsApp service disruption
* Ex-army admin jailed for 12 years over US military health data theft
* Android flubot malware installs itself by faking security update
* Hackers exploit 2FA flaw to steal crypto from 6,000 Coinbase users
* Anonymous leaks more EPIK host data; 'larger than previous leak'
* Apple AirTags can be used as trojan for credential hacking
* GriftHorse Android malware hit 10 million devices in 70 countries

Naked Security

* Cybersecurity Awareness Month: #BeCyberSmart
* Gift card fraud: four suspects hit with money laundering charges
* S3 Ep52: Let's Encrypt, Outlook leak, and VMware exploit [Podcast]
* How to steal money via Apple Pay using the "Express Transit" feature
* Serious Security: Let's Encrypt gets ready to go it alone (in a good way!)
* S3 Ep51: OMIGOD a gaping hole, waybill scams, and Face ID hacked [Podcast]
* STILL ALIVE! iOS 12 gets 3 zero-day security patches - update now
* How Outlook "autodiscover" could leak your passwords - and how to stop it
* VMware patch bulletin warns: "This needs your immediate attention."
* iOS 15 launches with 22 documented security patches - including a Face ID bypass using a "3D model"

Threat Post

* Facebook Outage Drags Down Instagram, WhatsApp, Messenger, Oculus VR
* Encrypted & Fileless Malware Sees Big Growth
* Transnational Fraud Ring Bilks U.S. Military Service Members Out of Millions
* MFA Glitch Leads to 6K+ Coinbase Customers Getting Robbed
* 3.1M Neiman Marcus Customer Card Details Breached
* Flubot Malware Targets Androids With Fake Security Updates
* New APT ChamelGang Targets Russian Energy, Aviation Orgs
* Google Emergency Update Fixes Two Chrome Zero Days
* Military's RFID Tracking of Guns May Endanger Troops
* Tips & Tricks for Unmasking Ghoulish API Behavior

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

* A Journey in Organizational Resilience: Crisis Management
* Cybersecurity Awareness: The Basics Are the Foundation
* Deploying Proven Data Security Tools to Combat the Rising Cost of a Data Breach
* Cybersecurity Awareness Month: It's Time to Ditch the Fear
* What Is Zero Trust? A Complete Guide for Security Professionals
* Using Vendor Management to Defend Against Supply Chain Attacks
* Roundup: Health Care Data Breaches and Defenses in the News
* Enterprise Management Associates: A Survey on Modern Data Security in a Multicloud World
* Know the Four Pillars of Cloud Security That Reduce Data Breach Risk
* What Video Doorbells Have to Teach Us About the Difficulties of IoT Security

InfoWorld

* What's new in Python 3.10
* BrandPost: How CIS and ATO on AWS Can Ease the Compliance Process
* BrandPost: Four Reasons to Use Hardened VMs for Your Cloud Migration
* BrandPost: CIS Hardened VMs on AWS Graviton2: Enhancing EC2 Security
* BrandPost: 5 Cloud Computing Benefits: Why You Should Work in the Cloud
* BrandPost: 3 Ways to Use CIS Cloud Security Resources on the AWS Cloud
* The way we AI now
* How cloud-native apps and microservices impact the development process
* Review: Google Cloud Vertex AI irons out ML platform wrinkles
* Sumo Logic enhances observability suite for app, infrastructure performance

C4ISRNET - Media for the Intelligence Age Military

* Swarm grammar: DARPA to test whether single user can control 200 drones
* Air Force squeezes new cyber defense teams out of its communications squadrons
* In first, Turkmenistan shows off Bayraktar TB2 drone
* Morocco and Israel to sign kamikaze drone deal
* HawkEye 360 wins radiofrequency mapping contract with intelligence agency
* West Point researchers explore a virtual future for training
* US Army trains forces across military on tools to fight drones
* An autonomous robot may have already killed people - here's how the weapons could be more destabilizi
* What you should know about 'Bitskrieg: The New Challenge of Cyberwarfare'
* Ukraine is set to buy 24 Turkish drones. So why hasn't Russia pushed back?

The Hacker Corner

Conferences

* Marketing Cybersecurity In 2021
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* 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)

Google Zero Day Project

* Fuzzing Closed-Source JavaScript Engines with Coverage Feedback
* Understanding Network Access in Windows AppContainers

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.

* pbctf 2021
* DamCTF 2021
* Digital Overdose 2021 Autumn CTF
* SPbCTF's Student CTF 2021 Quals
* DEADFACE CTF
* iCTF
* Reply Cyber Security Challenge 2021
* Collegiate SECTF
* ASIS CTF Quals 2021
* BuckeyeCTF 2021

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

* doubletrouble: 1
* Beelzebub: 1
* Vikings: 1
* DarkHole: 2
* Deathnote: 1

Tools & Techniques

Packet Storm Security Tools Links

* Bing.com Hostname / IP Enumerator 1.0.5
* TestSSL 3.0.6
* PyRDP RDP Man-In-The-Middle Tool
* Seth RDP Man-In-The-Middle Tool
* MedSec Network Utility Tool
* Falco 0.30.0
* SQLMAP - Automatic SQL Injection Tool 1.5.10
* Haveged 1.9.15
* Google Tsunami Security Scanner Pre-Alpha
* OpenSSH 8.8p1

Kali Linux Tutorials

* QueenoSno : Golang Binary For Data Exfiltration With ICMP Protocol
* PoW-Shield : Project Dedicated To Fight DDoS And Spam With Proof Of Work, Featuring An Additional WA
* Haklistgen : Turns Any Junk Text Into A Usable Wordlist For Brute-Forcing
* Reconky : A Great Content Discovery Bash Script For Bug Bounty Hunters Which Automate Lot Of Task And
* Wordlistgen : Quickly Generate Context-Specific Wordlists For Content Discovery From Lists Of URLs Or
* AES256_Passwd_Store : Secure Open-Source Password Manager
* DirSearch : A Go Implementation Of Dirsearch
* PyHook : An Offensive API Hooking Tool Written In Python Designed To Catch Various Credentials Within
* Weakpass : Rule-Based Online Generator To Create A Wordlist Based On A Set Of Words
* MailRipV2 : Improved SMTP Checker / SMTP Cracker With Proxy-Support, Inbox Test And Many More Feature

GBHackers Analysis

* Critical RCE Flaw in the core Netgear Firmware Let Remote Attackers to Take Control of an Affected Sy
* Apple Fixes iMessage Zero-Click Bug That Used to Deploy NSO Pegasus Spyware
* U.S. Cyber Command Warns of Active Mass Exploitation Attempts Targeting Confluence Flaws
* Conti Ransomware Gang Hacking Microsoft Exchange Servers Using ProxyShell Exploits
* WhatsApp Image Filter Bug Let Hackers Steal Sensitive Data

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown | September 2021
* 2021 SANS DFIR Summit Day 2 Wrap Up
* SANS Law Enforcement Appreciation Programs
* 2021 SANS DFIR Summit Day 1 Wrap Up Panel

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelgänger Your Häx Dollars at Work
* DEF CON 29 Red Team Village - CTF Day 2
* DEF CON 29 Recon Village - Ben S - Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

Hak5

* Detect WiFi Attacks on the WiFi Nugget (ESP8266 Monitor Mode)
* 3 Apple Zero Days Publicly Released; FBI Withholds Ransomware Decryptor Key - ThreatWire
* HakByte: Set Up a Headless Raspberry Pi Wardriving Rig

The PC Security Channel [TPSC]

* Linux Malware Calls Home: Vermilion Strike
* Linux Ransomware

Eli the Computer Guy

* Office Hours - Tech Question and Answers PLACEHOLDER
* Office Hours with Tomer Shvueli (Digital Nomad) - PLACEHOLDER
* Office Hours - Tech Question and Answers (Sep 30, 2021)
* Patch Management Introduction (Cyber Security Part 6)

Security Now

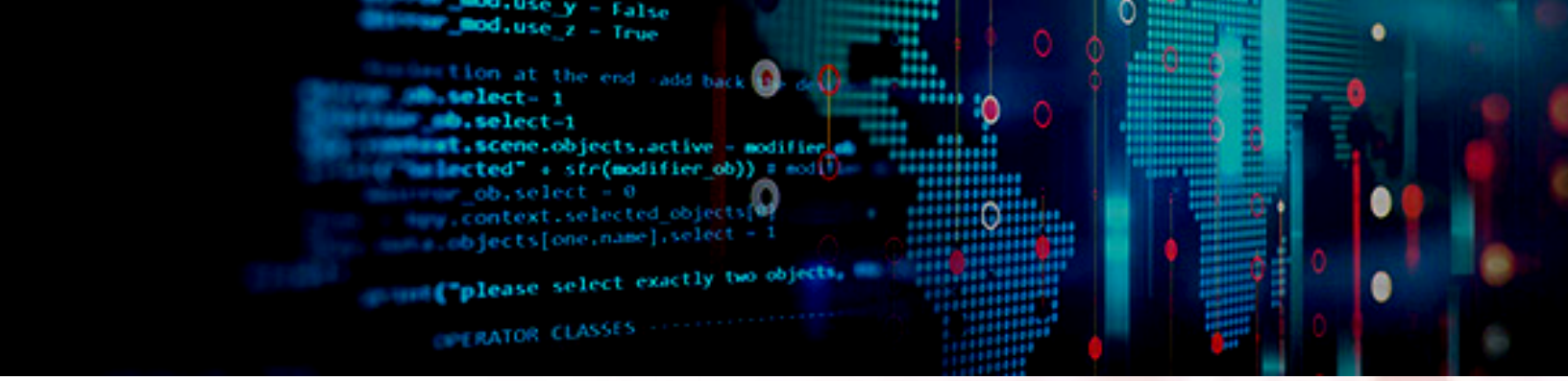
* autodiscover.fiasco - Epik Confirms Hack, Apple Annoys Bug Reporters, Chrome's 12th 0-Day in 2021
* Cobalt Strike - Android Auto-Revokes Permissions, DDoS on VoIP.ms, Patch Tuesday, Was GRC Pwned?

Troy Hunt

* Weekly Update 263

Intel Techniques: The Privacy, Security, & OSINT Show

* 236-Three Topics in 14 Minutes
* 235-iOS 15 Privacy Guide



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

* "Bom" Skimmer is Magecart Group 7's Latest Model
* Untangling the Spider Web
* Flowspec Bulletproof Services Enable Cybercrime Worldwide
* RiskIQ Analysis Links EITest and Gootloader Campaigns, Once Thought to Be Disparate
* Introducing Next-Gen Vulnerability Intelligence to Identify and Prioritize CVEs in Real-time
* Magecart Group 8: Patterns in Hosting Reveal Sustained Attacks on E-Commerce
* Your Growing Digital Attack Surface And How To Protect It
* Bear Tracks: Infrastructure Patterns Lead to More Than 30 Active APT29 C2 Servers
* New Analysis Shows XAMPP Serving Agent Tesla and Formbook Malware
* Taking a Closer Look at a Malicious Infrastructure Mogul

FireEye

* [The Lost Bots] Episode 6: D&R + VM = WINNING!
* Metasploit Wrap-Up
* National Cybersecurity Awareness Month: How Security Pros Can Get Involved
* The 2021 OWASP Top 10 Have Evolved: Here's What You Should Know
* [Security Nation] Rob Graham on Mike Lindell's Cyber Symposium
* To the Left: Your Guide to Infrastructure as Code for Shifting Left
* Metasploit Wrap-Up
* Ransomware: Is Critical Infrastructure in the Clear?
* Easier URI Targeting With Metasploit Framework
* Rapid7 Technical Support: Building a Career Path With Endless Possibilities

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Company's Recruitment Management System SQL Injection
* Local Offices Contact Directory Site SQL Injection
* College Management System 1.0 Insecure Direct Object Reference
* College Management System 1.0 Cross Site Scripting
* College Management System 1.0 SQL Injection
* Gatekeeper Bypass Proof Of Concept
* Lifestyle Store 1.0 Cross Site Scripting
* Young Entrepreneur E-Negosyo System 1.0 Cross Site Scripting
* Young Entrepreneur E-Negosyo System 1.0 SQL Injection
* Vehicle Service Managment System 1.0 Shell Upload
* Vehicle Service Management System 1.0 SQL Injection
* Open Game Panel Remote Code Execution
* Pet Shop Management System 1.0 Privilege Escalation / Shell Upload
* College Management System 1.0 Arbitrary File Upload
* Lodging Reservation Management System 1.0 SQL Injection
* Payara Micro Community 5.2021.6 Directory Traversal
* Packet Storm New Exploits For September, 2021
* WhatsUpGold 21.0.3 Cross Site Scripting
* Blood Bank System 1.0 SQL Injection
* Phpwcms 1.9.30 Cross Site Scripting
* Drupal MiniorangeSAML 8.x-2.22 Privilege Escalation
* Exam Form Submission System 1.0 SQL Injection
* Vehicle Service Management System 1.0 Shell Upload
* CMSimple_XH 1.7.4 Remote Command Execution
* PlaceOS 1.2109.1 Open Redirection

CXSecurity

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

Proof of Concept (PoC) & Exploits

Exploit Database

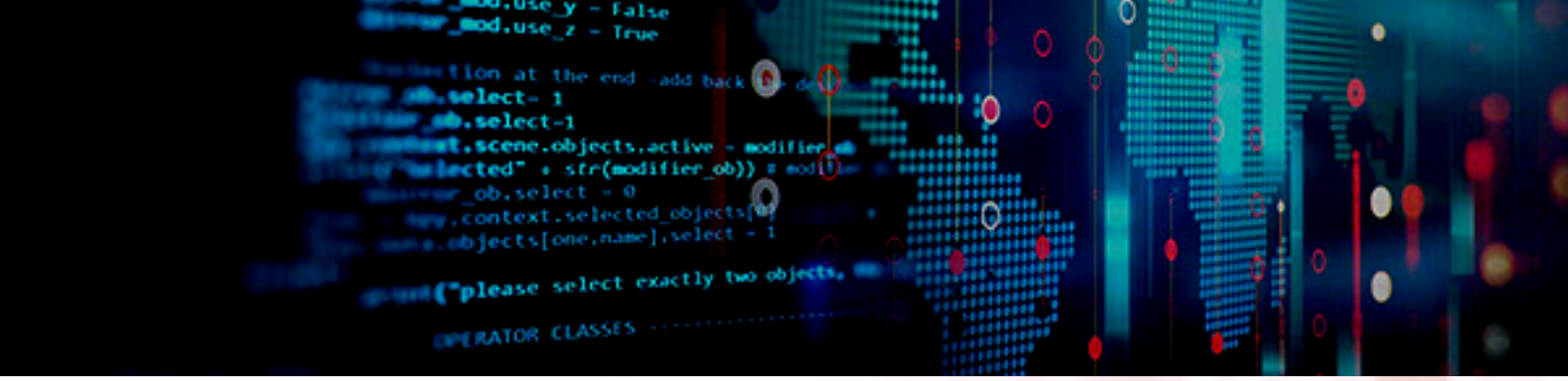
* [webapps] Young Entrepreneur E-Negosyo System 1.0 - 'PRODESC' Stored Cross-Site Scripting (XSS)
* [webapps] Young Entrepreneur E-Negosyo System 1.0 - SQL Injection Authentication Bypass
* [webapps] Open Game Panel - Remote Code Execution (RCE) (Authenticated)
* [webapps] Lodging Reservation Management System 1.0 - SQL Injection / Authentication Bypass
* [webapps] Payara Micro Community 5.2021.6 - Directory Traversal
* [webapps] Directory Management System 1.0 - SQL Injection Authentication Bypass
* [webapps] CMSimple_XH 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] WhatsUpGold 21.0.3 - Stored Cross-Site Scripting (XSS)
* [webapps] Dairy Farm Shop Management System 1.0 - SQL Injection Authentication Bypass
* [webapps] Vehicle Service Management System 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Phpwcms 1.9.30 - File Upload to XSS
* [webapps] Blood Bank System 1.0 - SQL Injection / Authentication Bypass
* [webapps] Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation via XML Signature Wrapping
* [webapps] Exam Form Submission System 1.0 - SQL Injection Authentication Bypass
* [webapps] PlaceOS 1.2109.1 - Open Redirection
* [webapps] Pharmacy Point of Sale System 1.0 - 'Multiple' SQL Injection (SQLi)
* [webapps] Cmsimple 5.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Cyber Cafe Management System Project (CCMS) 1.0 - SQL Injection Authentication Bypass
* [webapps] Wordpress Plugin JS Jobs Manager 1.1.7 - Unauthenticated Plugin Install/Activation
* [webapps] Pet Shop Management System 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] OpenSIS 8.0 - 'cp_id_miss_attn' Reflected Cross-Site Scripting (XSS)
* [remote] Mitrastar GPT-2541GNAC-N1 - Privilege escalation
* [webapps] WordPress Plugin Redirect 404 to Parent 1.3.0 - Reflected Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Select All Categories and Taxonomies 1.3.1 - Reflected Cross-Site Scriptin

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*

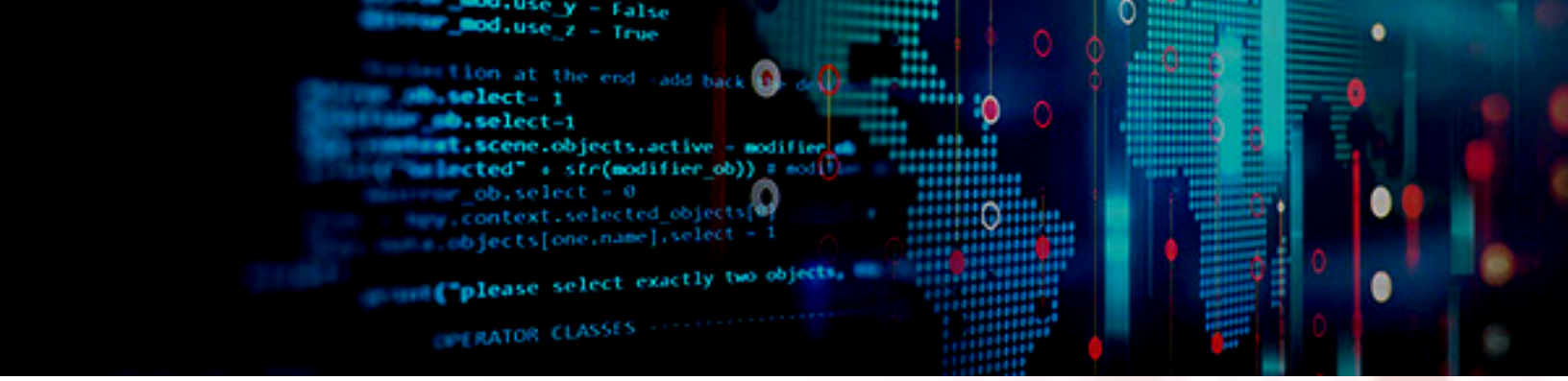
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

Unfortunately, at the time of this report, the Zone-H.org last hacked feed was not availible.



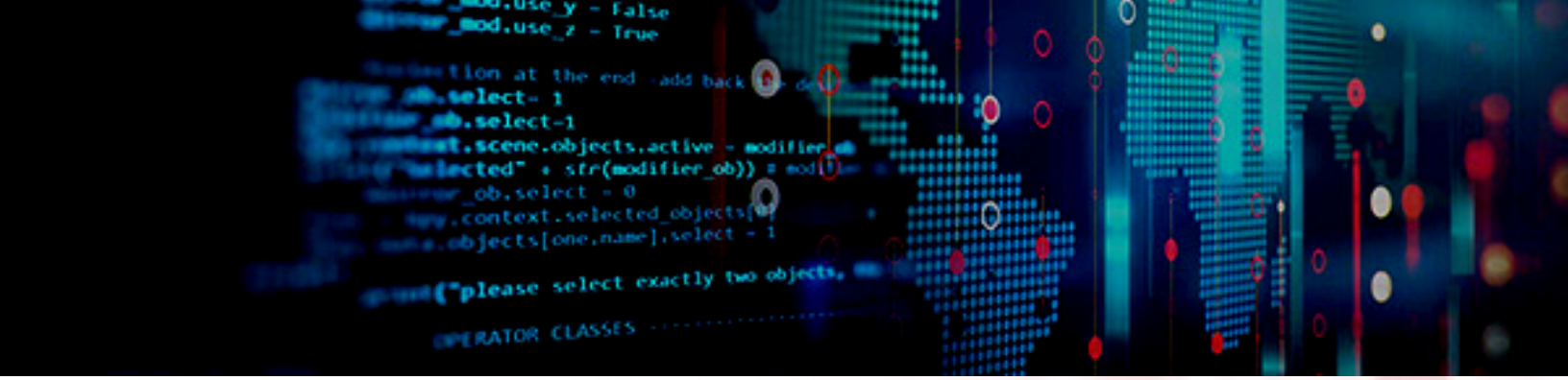
Dark Web News

Darknet Live

[PSA: White House Market is Retiring]
White House Market is retiring, according to a signed message from the market's administrator. (via darknetlive.com)
[Steroid Vendor "Phantomlabs" Sentenced to Three Years in Prison]
The California resident behind the darkweb vendor account "Phantomlabs” will spend three years in prison for selling steroids. (via darknetlive.com)
[First "EastSideHigh" Defendant Enters Guilty Plea]
A Brockton man pleaded guilty to selling MDMA, ketamine, and alprazolam through the darkweb vendor account "EastSideHigh.” (via darknetlive.com)
[North Carolina Man Sentenced for Buying and Selling Oxycodone]
A North Carolina man is will be spending 26 months in prison following a conviction for purchasing oxycodone from a vendor on the darkweb. (via darknetlive.com)

Dark Web Link

[A Brockton Man Has Begged Guilty To Trafficking Drugs On The Dark Web In Federal Court]
A Brockton man admitted in federal court, to making pharmaceuticals in Stoughton as well as distributing them on the dark web. BinhThanh Le, 25, admitted to conspiring to produce, distribute, and possess with intent to distribute methylenedioxymethamphetamine (MDMA), also known as ecstasy, ketamine, and Xanax, on Wednesday. Judge Rya W. Zobel of the United States [...] The post A Brockton Man Has Begged Guilty To Trafficking Drugs On The Dark Web In Federal Court appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Dark Web Boom: Process You Can Protect Your Corporate Data]
A police sting on the German-Danish border in January 2021 resulted in the arrest of a 34-year-old Australian who is accused of running one of the world's largest illegal online marketplaces. DarkMarket, as it was dubbed, was a dark web marketplace with half a million users and 2400 vendors selling everything from drugs to fake [...] The post Dark Web Boom: Process You Can Protect Your Corporate Data appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[The Dark Web Design Rise: How Sites Operate You Into Clicking]
A pop-up now greets you on the vast majority of websites you visit. The “cookie banner” is an obtrusive stumbling block to your unified web browsing. It's intended to gain your agreement, as required by internet privacy regulations, for websites to keep information about you between browsing sessions. The cookie banner claims to give you [...] The post The Dark Web Design Rise: How Sites Operate You Into Clicking appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* CISA and NSA Release Guidance on Selecting and Hardening VPNs
* RCE Vulnerability in Hikvision Cameras (CVE-2021-36260)
* VMware vCenter Server Vulnerability CVE-2021-22005 Under Active Exploit
* Google Releases Security Updates for Chrome
* Apple Releases Security Updates
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Guidance: IPv6 Considerations for TIC 3.0
* AA21-265A: Conti Ransomware
* AA21-259A: APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus
* Vulnerability Summary for the Week of September 27, 2021
* Vulnerability Summary for the Week of September 20, 2021

Zero Day Initiative Advisories

ZDI-CAN-15409: Bentley
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15416: Bentley
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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15403: Bentley
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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15458: Bentley
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15464: Bentley
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: 2021-10-01, 3 days ago. The vendor is given until

2022-01-29 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-15391: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15377: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15457: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15371: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15313: 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 'kpc' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15453: Bentley

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15379: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15366: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15463: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15369: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until

2022-01-29 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-15461: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15212: Microsoft

A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15370: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15376: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15380: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15314: 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 'kpc' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15372: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15367: Bentley

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: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-15412: Bentley

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-01, 3 days ago. The vendor is given until 2022-01-29 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-5101-1

Ubuntu Security Notice 5101-1 - It was discovered that MongoDB incorrectly handled certain wire protocol messages. A remote attacker could possibly use this issue to cause MongoDB to crash, resulting in a denial of service.

Ubuntu Security Notice USN-5100-1

Ubuntu Security Notice 5100-1 - It was discovered that containerd insufficiently restricted permissions on container root and plugin directories. If a user or automated system were tricked into launching a specially crafted container image, a remote attacker could traverse directory contents and modify files and execute programs on the host filesystem, possibly leading to privilege escalation.

Ubuntu Security Notice USN-5099-1

Ubuntu Security Notice 5099-1 - It was discovered that Imlib2 incorrectly handled certain ICO images. An attacker could use this issue to cause a denial of service and possibly execute arbitrary code.

Ubuntu Security Notice USN-4973-2

Ubuntu Security Notice 4973-2 - USN-4973-1 fixed this vulnerability previously, but it was re-introduced in python3.8 in focal because of the SRU in LP: #1928057. This update fixes the problem. It was discovered that the Python stdlib ipaddress API incorrectly handled octal strings. A remote attacker could possibly use this issue to perform a wide variety of attacks, including bypassing certain access restrictions. Various other issues were also addressed.

Red Hat Security Advisory 2021-3646-01

Red Hat Security Advisory 2021-3646-01 - 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.

Ubuntu Security Notice USN-5094-2

Ubuntu Security Notice 5094-2 - It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. An attacker who could start and control a VM could possibly use this to expose sensitive information or execute arbitrary code. It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-3704-01

Red Hat Security Advisory 2021-3704-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include buffer overflow, integer overflow, null pointer, out of bounds access, and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-5091-2

Ubuntu Security Notice 5091-2 - Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack. An attacker could use this to expose sensitive information. It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-3703-01

Red Hat Security Advisory 2021-3703-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include buffer overflow, integer overflow, null pointer, out of bounds access, and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-5096-1

Ubuntu Security Notice 5096-1 - Valentina Palmiotti discovered that the io_uring subsystem in the Linux kernel could be coerced to free adjacent memory. A local attacker could use this to execute arbitrary code. Benedict Schlueter discovered that the BPF subsystem in the Linux kernel did not properly protect against Speculative Store Bypass side-channel attacks in some situations. A local attacker could possibly use this to expose sensitive information. Various other issues were also addressed.

Red Hat Security Advisory 2021-3700-01

Red Hat Security Advisory 2021-3700-01 - AMQ Broker is a high-performance messaging implementation based on

ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms. This release of Red Hat AMQ Broker 7.9.0 serves as a replacement for Red Hat AMQ Broker 7.8.2, and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include bypass, denial of service, information leakage, resource exhaustion, and traversal vulnerabilities.

Ubuntu Security Notice USN-5095-1

Ubuntu Security Notice 5095-1 - It was discovered that Apache Commons IO incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information.

Red Hat Security Advisory 2021-3694-01

Red Hat Security Advisory 2021-3694-01 - The Migration Toolkit for Containers enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-3635-01

Red Hat Security Advisory 2021-3635-01 - 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 4.7.32.

Red Hat Security Advisory 2021-3642-01

Red Hat Security Advisory 2021-3642-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

Ubuntu Security Notice USN-5092-2

Ubuntu Security Notice 5092-2 - Valentina Palmiotti discovered that the io_uring subsystem in the Linux kernel could be coerced to free adjacent memory. A local attacker could use this to execute arbitrary code. Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack. An attacker could use this to expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5094-1

Ubuntu Security Notice 5094-1 - It was discovered that the KVM hypervisor implementation in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. An attacker who could start and control a VM could possibly use this to expose sensitive information or execute arbitrary code. It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-5090-4

Ubuntu Security Notice 5090-4 - USN-5090-1 fixed vulnerabilities in Apache HTTP Server. One of the upstream fixes introduced a regression in UDS URIs. This update fixes the problem. James Kettle discovered that the Apache HTTP Server HTTP/2 module incorrectly handled certain crafted methods. A remote attacker could possibly use this issue to perform request splitting or cache poisoning attacks. It was discovered that the Apache HTTP Server incorrectly handled certain malformed requests. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. Li Zhi Xin discovered that the Apache mod_proxy_uwsgi module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. It was discovered that the Apache HTTP Server incorrectly handled escaping quotes. If the server was configured with third-party modules, a remote attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that the Apache mod_proxy module incorrectly handled certain request uri-paths. A remote attacker could possibly use this issue to cause the server to forward requests to arbitrary origin servers. Various other issues were also addressed.

Ubuntu Security Notice USN-5090-3

Ubuntu Security Notice 5090-3 - USN-5090-1 fixed vulnerabilities in Apache HTTP Server. One of the upstream fixes introduced a regression in UDS URIs. This update fixes the problem.

Red Hat Security Advisory 2021-3675-01

Red Hat Security Advisory 2021-3675-01 - The shim package contains a first-stage UEFI boot loader that handles chaining to a trusted full boot loader under secure boot environments. The fwupd packages provide a service that allows session software to update device firmware. Issues addressed include buffer overflow, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-3676-01

Red Hat Security Advisory 2021-3676-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Ubuntu Security Notice USN-5093-1

Ubuntu Security Notice 5093-1 - Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 21.04. Brian Carpenter discovered that vim incorrectly handled memory when opening certain files. If a user was tricked into opening a specially crafted file, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. Various other issues were also addressed.

Ubuntu Security Notice USN-5092-1

Ubuntu Security Notice 5092-1 - Valentina Palmiotti discovered that the io_uring subsystem in the Linux kernel could be coerced to free adjacent memory. A local attacker could use this to execute arbitrary code. Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack. An attacker could use this to expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5091-1

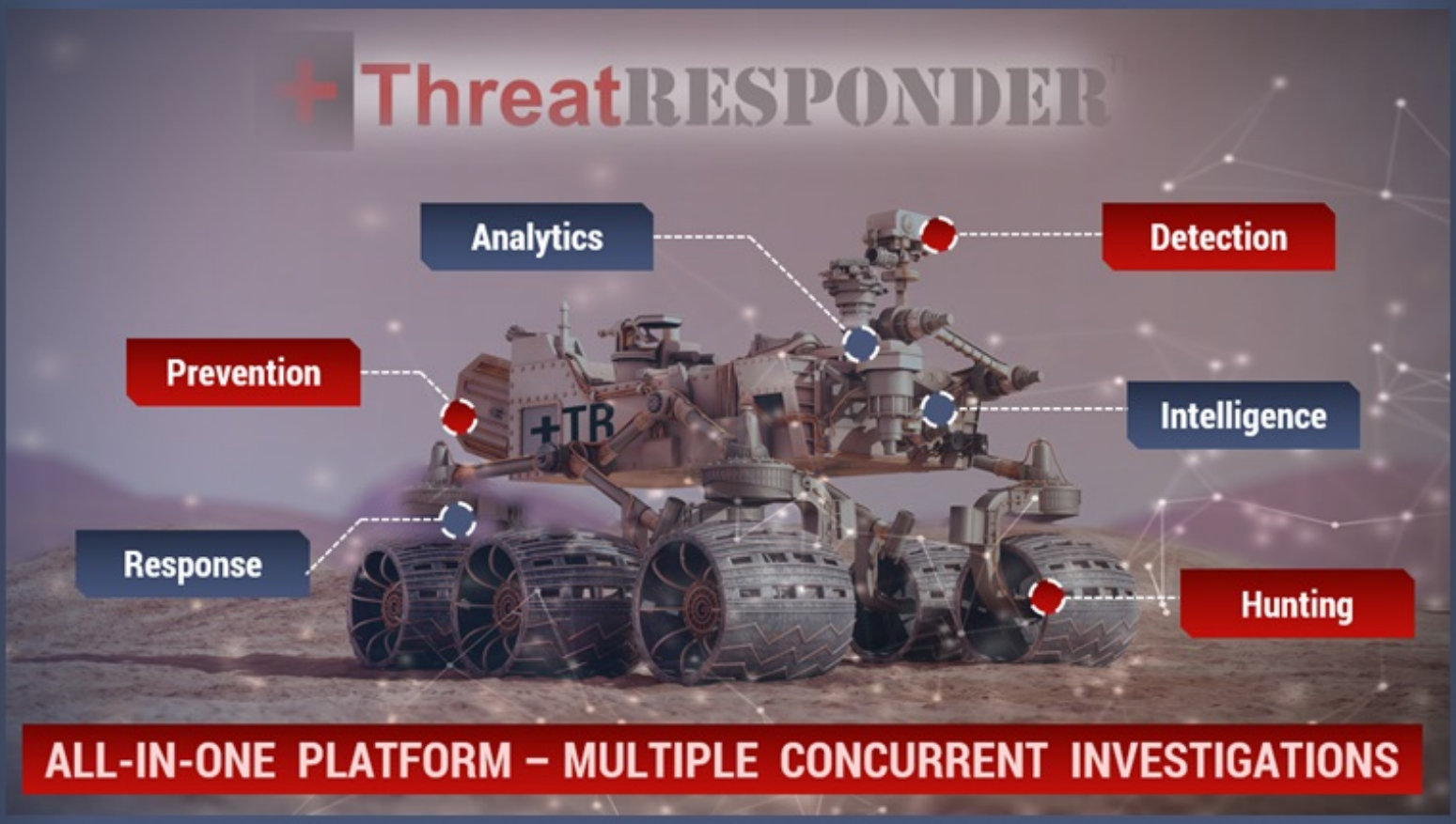
Ubuntu Security Notice 5091-1 - Ofek Kirzner, Adam Morrison, Benedict Schlueter, and Piotr Krysiuk discovered that the BPF verifier in the Linux kernel missed possible mispredicted branches due to type confusion, allowing a side-channel attack. An attacker could use this to expose sensitive information. It was discovered that the tracing subsystem in the Linux kernel did not properly keep track of per-cpu ring buffer state. A privileged attacker could use this to cause a denial of service. Various other issues were also addressed.

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: 2021.2

Download here.

CSI Linux is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux 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:

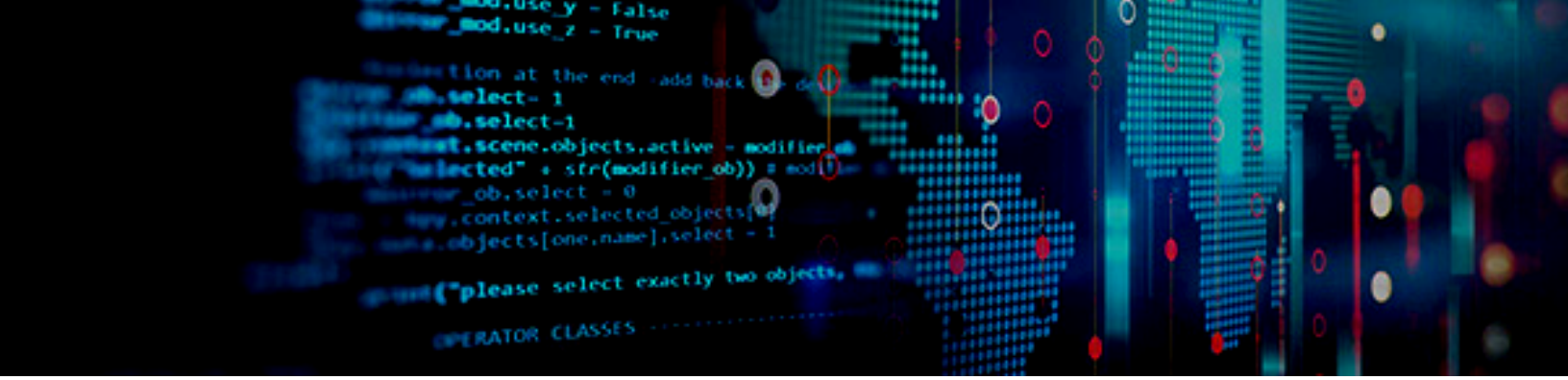
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

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

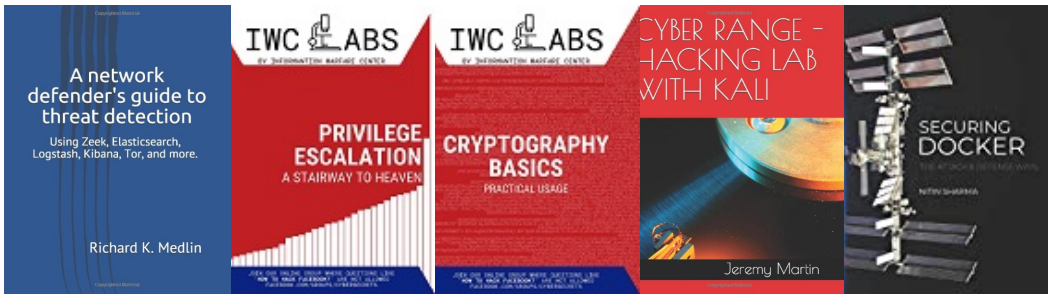


The Cyber Secrets publications on Amazon

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