Aug-02-21

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

August 2, 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

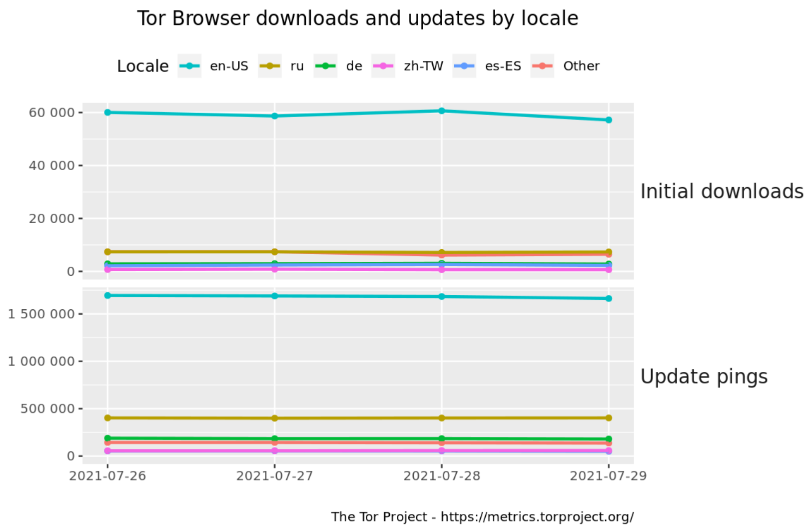
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.](Subscribe) 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

* CISA Launches Own Vulnerability Disclosure Program
* Microsoft Warns Of Sneakier Than Usual Phishing Attack
* SolarWinds Attackers Breached Email Of US Prosecutors, Says Department Of Justice
* Novel Meteor Wiper Used In Attack That Crippled Iranian Train System
* Vultur Bank Malware Infests Thousands Of Devices
* Cisco Researchers Spotlight Solarmarker Malware
* Security Team Finds Crimea Manifesto Buried In VBA Rat
* Inside The Bitcoin Mine With Its Own Power Plant
* Israeli Authorities Inspect NSO Offices After Damning Investigation
* Call For Hungarian Ministers To Resign In Wake Of Pegasus Revelations
* Reboot Of PunkSpider Tool At DEF CON Stirs Debate
* Feds List The Top 30 Most Exploited Vulnerabilities
* Three Zero-Day Bugs Plague Kaseya Unitrends Backup Servers
* LEAs, CISA Lobby For Breach Reporting Requirement
* Enterprise Data Breach Cost Reached Record High During Pandemic
* Biden: Major Cyber Attack Could Lead To A Real Shooting War
* Babuk Ransomware Gang Ransomed
* Microsoft Rushes Fix For PetitPotam Attack PoC
* VPN Servers Seized By Ukrainian Authorities Weren't Encrypted
* Olympics Broadcaster Announces His Password On Live TV
* Mitre Releases 2021 Top 25 Most Dangerous Software Weaknesses
* Microsoft Outlines How To Protect Against PetitPotam
* An Explosive Spyware Report Shows Limits Of iOS, Android Security
* Emmanuel Macron Pushes For Israel Inquiry Into NSO Spyware Concerns
* Researchers Find New Attack Vector Against Kubernetes Clusters

Krebs on Security

* The Life Cycle of a Breached Database
* PlugwalkJoe Does the Perp Walk
* Serial Swatter Who Caused Death Gets Five Years in Prison
* Spam Kingpin Peter Levashov Gets Time Served
* Don't Wanna Pay Ransom Gangs? Test Your Backups.
* Microsoft Patch Tuesday, July 2021 Edition
* Spike in "Chain Gang" Destructive Attacks on ATMs
* Kaseya Left Customer Portal Vulnerable to 2015 Flaw in its Own Software
* Microsoft Issues Emergency Patch for Windows Flaw
* Another 0-Day Looms for Many Western Digital Users

Dark Reading

* Multiple Zero-Day Flaws Discovered in Popular Hospital Pneumatic Tube System
* 8 Security Tools to be Unveiled at Black Hat USA
* Biden Administration Responds to Geopolitical Cyber Threats
* 7 Hot Cyber Threat Trends to Expect at Black Hat
* Law Firm for Ford, Pfizer, Exxon Discloses Ransomware Attack
* US Accuses China of Using Criminal Hackers in Cyber Espionage Operations
* How Gaming Attack Data Aids Defenders Across Industries
* NSO Group Spyware Used On Journalists & Activists Worldwide
* When Ransomware Comes to (Your) Town
* 7 Ways AI and ML Are Helping and Hurting Cybersecurity
* Breaking Down the Threat of Going All-In With Microsoft Security
* Researchers Create New Approach to Detect Brand Impersonation
* Recent Attacks Lead to Renewed Calls for Banning Ransom Payments
* 4 Future Integrated Circuit Threats to Watch
* How to Attract More Computer Science Grads to the Cybersecurity Field
* Attackers Exploited 4 Zero-Day Flaws in Chrome, Safari & IE
* State Dept. to Pay Up to $10M for Information on Foreign Cyberattacks
* CISA Launches New Website to Aid Ransomware Defenders
* Microsoft: Israeli Firm's Tools Used to Target Activists, Dissidents
* IoT-Specific Malware Infections Jumped 700% Amid Pandemic

The Hacker News

* PwnedPiper PTS Security Flaws Threaten 80% of Hospitals in the U.S.
* New APT Hacking Group Targets Microsoft IIS Servers with ASP.NET Exploits
* PyPI Python Package Repository Patches Critical Supply Chain Flaw
* Solarmarker InfoStealer Malware Once Again Making its Way Into the Wild
* Experts Uncover Several C&C Servers Linked to WellMess Malware
* Several Malicious Typosquatted Python Libraries Found On PyPI Repository
* A New Wiper Malware Was Behind Recent Cyberattack On Iranian Train System
* Phony Call Centers Tricking Users Into Installing Ransomware and Data-Stealers
* Hackers Exploit Microsoft Browser Bug to Deploy VBA Malware on Targeted PCs
* New Ransomware Gangs - Haron and BlackMatter - Emerge on Cybercrime Forums
* Best Practices to Thwart Business Email Compromise (BEC) Attacks
* New Android Malware Uses VNC to Spy and Steal Passwords from Victims
* Top 30 Critical Security Vulnerabilities Most Exploited by Hackers
* UBEL is the New Oscorp - Android Credential Stealing Malware Active in the Wild
* Chinese Hackers Implant PlugX Variant on Compromised MS Exchange Servers

Security Week

* Potential RCE Flaw Patched in PyPI's GitHub Repository
* OT Security Firm Nozomi Networks Raises $100 Million
* Chipotle's Email Marketing Account Hacked to Spread Malware
* Cybersecurity M&A Roundup: 38 Deals Announced in July 2021
* Cisco, Sonatype and Others Join Open Source Security Foundation
* Amazon Fined 746 Mn Euros in Luxembourg Over Data Privacy
* NSA Shares Guidance for Government Employees on Securing Wireless Devices in Public
* Flaws in Pneumatic Tube System Can Facilitate Cyberattacks on North American Hospitals
* Zoom to Settle US Privacy Lawsuit for $85 Mn
* Justice Department Says Russians Hacked Federal Prosecutors
* Android Banking Trojan 'Vultur' Abusing Accessibility Services
* Russia's APT29 Still Actively Delivering Malware Used in COVID-19 Vaccine Spying
* New Chinese Threat Group 'GhostEmperor' Targets Governments, Telecom Firms
* Window of Exposure is Expanding and Hackers Know Exactly Where to Strike
* Remote Code Execution Flaws Patched in WordPress Download Manager Plugin
* Microsoft Shares More Information on Protecting Systems Against PetitPotam Attacks
* 21-Year-Old Woman Pleads Guilty to Sending Phishing Emails to Political Candidates
* S.Africa's Port Terminals Restored Following Cyber-Attack
* Belarusian Nationals Arrested for Hacking ATMs Across Europe
* Researchers Publish Details on Recent Critical Hyper-V Vulnerability
* How Low-level Hackers Access High-end Malware
* BlackCloak Raises $11 Million for Its Executive Protection Platform
* Leaked Files From Offensive Cyber Unit Show Iran's Interest in Targeting ICS
* Turn Off, Turn On: Simple Step Can Thwart Top Phone Hackers

Infosecurity Magazine

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

KnowBe4 Security Awareness Training Blog RSS Feed

* New Phishing Campaign Uses Blackmail to Lure Victims
* Visit KnowBe4 at Black Hat USA 2021 - Virtual & In Person Event
* Two of the Most Common and Successful Ransomware Attack Methods are Exposed
* Ransomware Attacks This Year Are Already Higher Than 2020
* Happy 22nd Annual SysAdmin Day from KnowBe4!
* Scammers Use Milanote App to Host Phishing Content and Avoid Detection by Secure Email Gateways
* The World's Most Impersonated Brand in Phishing Attacks Is… (and it's NOT Microsoft!)
* Over 700 Ransomware Victim Organizations are Named on Data Leak Sites in Q2
* Image Inversion as a Phishing Technique
* Cybercriminals Are Growing More Organized

ISC2.org Blog

* READY for What's New at (ISC)² Security Congress in 2021?
* Relevance Requires More than Just Paying Attention
* The Role of Culture in Compliance
* Malware, Cybercrime and Cloud Security
* Cybersecurity Professionals to Newcomers: Focus on Vendor-Neutral Certifications

HackRead

* New WeTransfer phishing attack spoofs file-sharing to steal credential
* Calgary Parking Authority exposed sensitive data of residents
* Crooks using phony call centers to spread ransomware via BazaCall attacks
* Crippling attack on Iranian trains linked to Meteor file wiper malware
* 2 new ransomware gangs Haron, BlackMatter appear after REvil, DarkSide
* Hackers posed as aerobics instructors in malware attack on defense contractors
* 5 must-try user flow diagramming tools for UX designing 2021

Koddos

* New WeTransfer phishing attack spoofs file-sharing to steal credential
* Calgary Parking Authority exposed sensitive data of residents
* Crooks using phony call centers to spread ransomware via BazaCall attacks
* Crippling attack on Iranian trains linked to Meteor file wiper malware
* 2 new ransomware gangs Haron, BlackMatter appear after REvil, DarkSide
* Hackers posed as aerobics instructors in malware attack on defense contractors
* 5 must-try user flow diagramming tools for UX designing 2021

Naked Security

* S3 Ep43: Apple 0-day, pygmy hippos, hive nightmares and Twitter hacker bust [Podcast]
* Microsoft researcher found Apple 0-day in March, didn't report it
* Apple emergency zero-day fix for iPhones and Macs - get it now!
* Windows "PetitPotam" network attack - how to protect against it
* US court gets UK Twitter hack suspect arrested in Spain
* S3 Ep42: Viruses, Nightmares, patches, rewards and scammers [Podcast]
* Windows "HiveNightmare" bug could leak passwords - here's what to do!
* Apple iPhone patches are out - no news if recent Wi-Fi bug is fixed
* S3 Ep41: Crashing iPhones, PrintNightmares, and Code Red memories [Podcast]
* More PrintNightmare: "We TOLD you not to turn the Print Spooler back on!"

Threat Post

* NSA Warns Public Networks are Hacker Hotbeds
* Novel Meteor Wiper Used in Attack that Crippled Iranian Train System
* UC San Diego Health Breach Tied to Phishing Attack
* CISA's Top 30 Bugs: One's Old Enough to Buy Beer
* Israeli Government Agencies Visit NSO Group Offices
* Six Malicious Linux Shell Scripts Used to Evade Defenses and How to Stop Them
* BlackMatter & Haron: Evil Ransomware Newborns or Rebirths
* Reboot of PunkSpider Tool at DEF CON Stirs Debate
* Podcast: Why Securing Active Directory Is a Nightmare
* No More Ransom Saves Victims Nearly â,¬1 billion Over 5 Years

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

* 5 Ways to Increase Password Safety
* Building Effective Business Cases to Cover Cybersecurity Costs
* July 2021 Security Intelligence Roundup: Ransomware, Security by Design and How to Analyze in Windows
* Data Breach Costs at Record High, Zero Trust, AI and Automation Help Reduce Costs
* What's New in the 2021 Cost of a Data Breach Report
* Double Encryption: When Ransomware Recovery Gets Complicated
* How AI Will Transform Data Security
* API Abuse Is a Data Security Issue Here to Stay
* Thriving in Chaos: How Cyber Resilience Works
* This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered

InfoWorld

* GitHub Copilot is 'unacceptable and unjust,' says Free Software Foundation
* What is the color of cloud money?
* Data science is a lot of drudgery, and that's good
* What is Docker? The spark for the container revolution
* Are your agile and devops processes good enough?
* Jetpack Compose for Android turns GA
* Could you survive a cloud architecture walkthrough?
* "Do More with R" video tutorials
* OpenAI debuts Python-based Triton for GPU-powered machine learning
* Microsoft .NET adoption gets boost from open source

C4ISRNET - Media for the Intelligence Age Military

* Electronic attack system to provide Navy more capabilities, flexible options
* Navy nears production decision on fleet's electronic warfare system
* Geomatics is vital to US national security; our advantage is at risk
* Here's how Shield AI wants to boost V-Bat's capability on a contested battlefield
* Space Force launches small satellite to test new sensor possibilities
* IAI and Hensoldt team up for German ballistic missile defense radar
* Military-funded research looks for the secret to GPS-free navigation in a bird's eye
* Lawmakers want answers on US Army plans to protect vehicles from drones
* House panel concerned over DoD's approach to the information environment
* Commander of the Space and Missile Systems Center retires

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

* An EPYC escape: Case-study of a KVM breakout
* Fuzzing iOS code on macOS at native speed

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.

* RaRCTF 2021
* ~~TSG CTF 2021~~ (postponed)
* BSides Noida CTF
* InCTF 2021
* Really Awesome CTF 2021
* Hacker's Playground 2021
* corCTF 2021
* Midnight Sun CTF 2021 Finals
* WORMCON 0x01
* ALLES! CTF 2021

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

* Hack Me Please: 1
* Corrosion: 1
* ContainMe: 1
* Hms?: 1
* doli: 1

Tools & Techniques

Packet Storm Security Tools Links

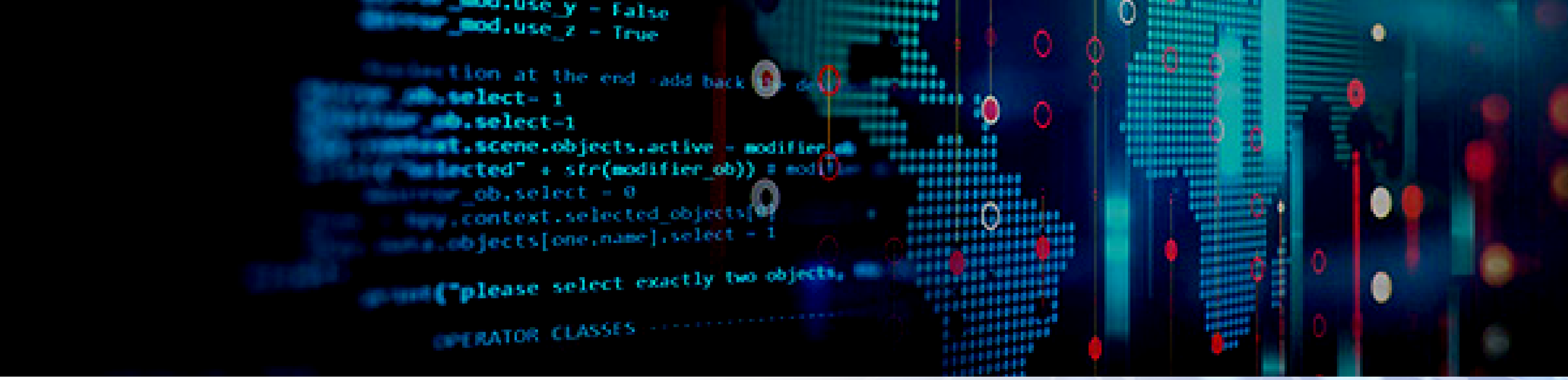
* SQLMAP - Automatic SQL Injection Tool 1.5.8
* Logwatch 7.5.6
* Lynis Auditing Tool 3.0.6
* American Fuzzy Lop plus plus 3.14c
* Hashcat Advanced Password Recovery 6.2.3 Source Code
* Hashcat Advanced Password Recovery 6.2.3 Binary Release
* Wireshark Analyzer 3.4.7
* UFONet 1.7
* Global Socket 1.4.33
* Zeek 4.0.3

Kali Linux Tutorials

* Radare2 : UNIX-like Reverse Engineering Framework And Command-Line Toolset
* CredPhish : A PowerShell Script Designed To Invoke Legitimate Credential Prompts And Exfiltrate Passw
* LoGiC.NET : A More Advanced Free And Open .NET Obfuscator Using Dnlib
* Dorothy : Tool To Test Security Monitoring And Detection For Okta Environments
* Reconmap : VAPT (Vulnerability Assessment And Penetration Testing) Automation And Reporting Platform
* TokenTactics : Azure JWT Token Manipulation Toolset
* Juumla : Tool Designed To Identify And Scan For Version, Config Files In The CMS Joomla!
* Rconn : Rconn Is A Multiplatform Program For Creating Generic Reverse Connections
* Ppmap : A Scanner/Exploitation Tool Written In GO, Which Leverages Prototype Pollution To XSS By Expl
* MANSPIDER : Spider Entire Networks For Juicy Files Sitting On SMB Shares. Search Filenames Or File Co

GBHackers Analysis

* SolarWinds Actors Hacked 27 State Attorneys' Offices in the U.S.
* Critical Oracle Weblogic Flaw Let Remote Attacker Take Control of The System
* Millions of Printers Worldwide Vulnerable To The 16-Year-Old Bug
* Russian APT Hackers Launched A Mass Global Brute Force Attack to Hack Enterprise & Cloud Networks
* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Getting started in DFIR: Testing 1,2,3
* DFIR Summit 2021
* STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign
* FOR585: Smartphone Forensic Analysis In-Depth

Defcon Conference

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

Hak5

* Hacking a Wii Nunchuk for Big Robots w/Glytch
* HakByte: How to use Postman to Reverse Engineer Private APIs
* Pegasus Project Reveals Phone Spyware Targets - ThreatWire

The PC Security Channel [TPSC]

* Discord Ransomware
* Windows 11: Better Security?

Eli the Computer Guy

* Cyber Security Introduction
* eBeggar Wednesday - MASK MANDATE Edition
* Hacking Introduction
* "Easy" Computer Speech Recognition with Azure Cognitive Services and Python

Security Now

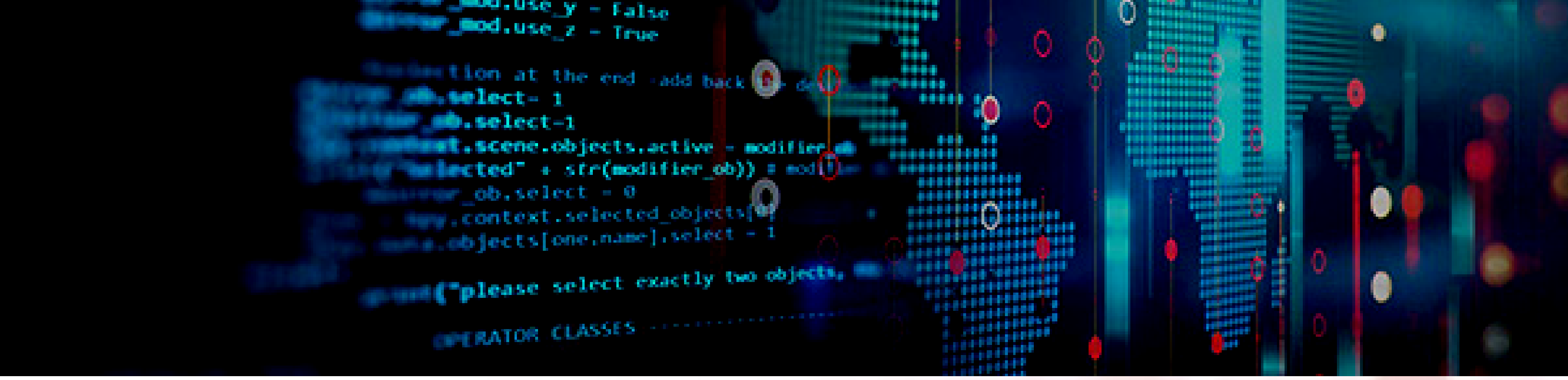
* SeriousSAM & PetitPotam - Kaseya Universal Decryptor, Window's Process Hacker, Chrome 92
* REvil Vanishes! - Chrome Zero-Day Vulnerability, iOS WiFi SSID Bug, Patch Tuesday Review

Troy Hunt

* Weekly Update 254

Intel Techniques: The Privacy, Security, & OSINT Show

* 227-Eleven Topics
* 226-Personal Ransomware Exposure



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

* 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
* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think

FireEye

* 3 Steps to Integrate Rapid7 Products Into the DevSecOps Cycle
* Metasploit Wrap-Up
* [Security Nation] Philipp Amann on No More Ransom
* Multiple Open Source Web App Vulnerabilities Fixed
* Decrypter FOMO No Mo': Five Years of the No More Ransom Project
* Metasploit Wrap-Up
* What's New in InsightAppSec and tCell: Q2 2021 in Review
* [Security Nation] Brian Honan on creating Ireland's first CERT
* Microsoft SAM File Readability CVE-2021-36934: What You Need to Know
* Grow Your Career at Rapid7: North America Sales

Proof of Concept (PoC) & Exploits

Packet Storm Security

* [Packet Storm New Exploits For July, 2021]
* [Online Hotel Reservation System 1.0 Cross Site Scripting]
* [Neo4j 3.4.18 Remote Code Execution]
* [Men Salon Management System 1.0 SQL Injection]
* [Pi-Hole Remove Commands Linux Privilege Escalation]
* [Panasonic Sanyo CCTV Network Camera 2.03-0x Cross Site Request Forgery]
* [ObjectPlanet Opinio 7.13 Shell Upload]
* [ObjectPlanet Opinio 7.13 Expression Language Injection]
* [ObjectPlanet Opinio 7.13 / 7.14 XML Injection]
* [Microsoft Exchange AD Schema Misconfiguration Privilege Escalation]
* [Oracle Fatwire 6.3 Cross Site Scripting / SQL Injection]
* [Longjing Technology BEMS API 1.21 Remote Arbitrary File Download]
* [Denver IP Camera SHO-110 Snapshot Disclosure]
* [ObjectPlanet Opinio 7.12 Cross Site Scripting]
* [CloverDX 5.9.0 Code Execution / Cross Site Request Forgery]
* [Care2x Integrated Hospital Info System 2.7 SQL Injection]
* [IntelliChoice eFORCE Software Suite 2.5.9 Username Enumeration]
* [Backdoor.Win32.WinShell.40 Code Execution]
* [Event Registration System With QR Code 1.0 Shell Upload]
* [Denver Smart Wifi Camera SHC-150 Remote Code Execution]
* [eGain Chat 15.5.5 Cross Site Scripting]
* [TripSpark VEO Transportation SQL Injection]
* [PHP 7.3.15-3 PHP_SESSION_UPLOAD_PROGRESS Session Data Injection]
* [WordPress Social Warfare 3.5.2 Remote Code Execution]
* [WordPress SP Project And Document Remote Code Execution]

CXSecurity

* [Pi-Hole Remove Commands Linux Privilege Escalation]
* [PHP 7.3.15-3 PHP_SESSION_UPLOAD_PROGRESS Session Data Injection]
* [NoteBurner 2.35 Denial Of Service]
* [Leawo Prof. Media 11.0.0.1 Denial Of Service]
* [Linux Kernel 2.6.19]
* [Microsoft SharePoint Server 2019 Remote Code Execution (2)]
* [ElasticSearch 7.13.3 Memory Disclosure]

Proof of Concept (PoC) & Exploits

Exploit Database

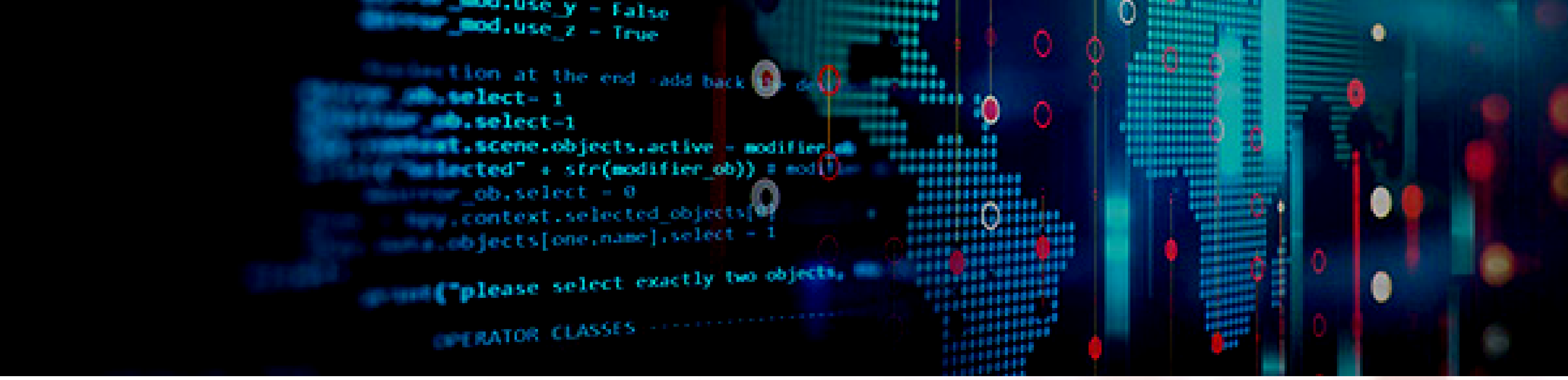
* [webapps] Panasonic Sanyo CCTV Network Camera 2.03-0x - 'Disable Authentication / Change Password' CS
* [webapps] Online Hotel Reservation System 1.0 - 'Multiple' Cross-site scripting (XSS)
* [remote] Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)
* [webapps] Men Salon Management System 1.0 - SQL Injection Authentication Bypass
* [webapps] Oracle Fatwire 6.3 - Multiple Vulnerabilities
* [webapps] CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)
* [webapps] Care2x Integrated Hospital Info System 2.7 - 'Multiple' SQL Injection
* [webapps] IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration
* [webapps] Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download
* [webapps] Denver IP Camera SHO-110 - Unauthenticated Snapshot
* [webapps] TripSpark VEO Transportation - Blind SQL Injection
* [remote] Denver Smart Wifi Camera SHC-150 - 'Telnet' Remote Code Execution (RCE)
* [webapps] Event Registration System with QR Code 1.0 - Authentication Bypass & RCE
* [webapps] Customer Relationship Management System (CRM) 1.0 - Sql Injection Authentication Bypass
* [webapps] PHP 7.3.15-3 - 'PHP_SESSION_UPLOAD_PROGRESS' Session Data Injection
* [webapps] XOS Shop 1.0.9 - 'Multiple' Arbitrary File Deletion (Authenticated)
* [webapps] NoteBurner 2.35 - Denial Of Service (DoS) (PoC)
* [dos] Leawo Prof. Media 11.0.0.1 - Denial of Service (DoS) (PoC)
* [webapps] Elasticsearch ECE 7.13.3 - Anonymous Database Dump
* [webapps] Microsoft SharePoint Server 2019 - Remote Code Execution (2)
* [webapps] WordPress Plugin Simple Post 1.1 - 'Text field' Stored Cross-Site Scripting (XSS)
* [webapps] ElasticSearch 7.13.3 - Memory disclosure
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Arbitrary File Deletion
* [webapps] KevinLAB BEMS 1.0 - File Path Traversal Information Disclosure (Authenticated)

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*

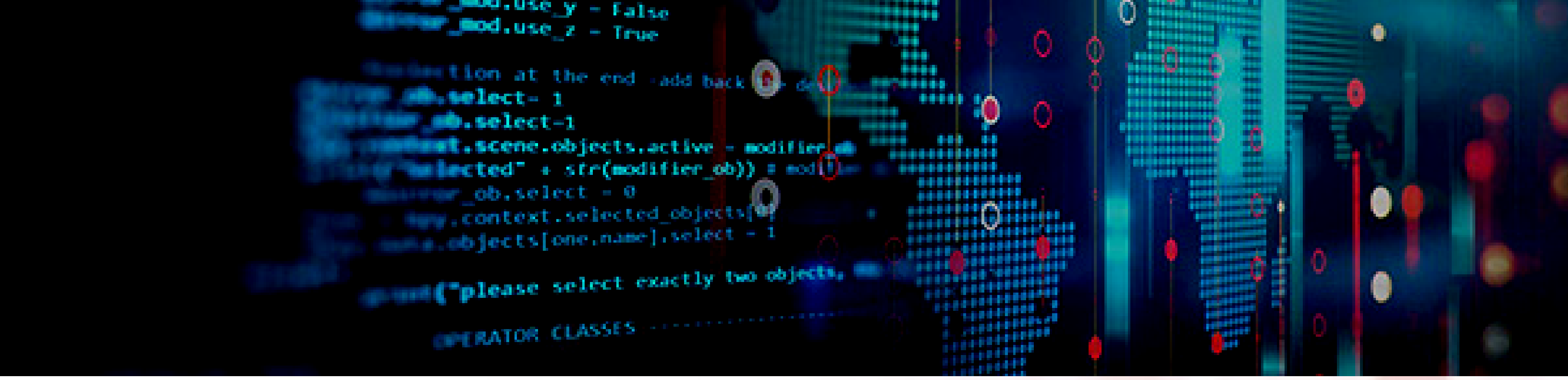
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



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.



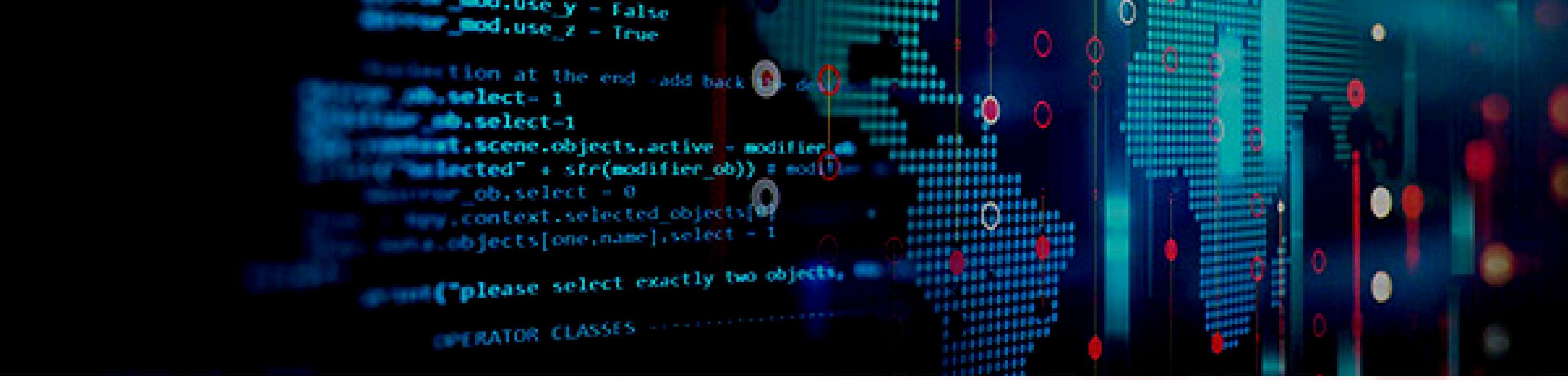
Dark Web News

Darknet Live

[Large-Scale Cocaine Dealer Sentenced to Prison]
A man living in Bristol, Connecticut, was sentenced to prison for his role in a conspiracy to traffic kilograms of cocaine from through the U.S. mail system. (via darknetlive.com)
[Prolific Cocaine Vendor "Insta" Arrested by the DEA in Nevada]
An investigation by the Drug Enforcement Administration resulted in the arrest of the prolific cocaine vendor "Insta.” (via darknetlive.com)
[Ethereum Dev Violated Bail Conditions by Signing into Coinbase]
Former Ethereum Foundation member Virgil Griffith has been taken into custody after violating the terms of his bail by signing into his Coinbase account. (via darknetlive.com)
[Jury Convicts "XanaxKing2" of Selling Fentanyl Analogues]
A jury convicted a California man of conspiring and manufacturing and distributing fentanyl pills through the darkweb. (via darknetlive.com)

Dark Web Link

[Is This The Finale Of The Path For Ransomware?]
Hackers appear to have developed a conscience, but they are unlikely to disappear forever. Ransomware, a sort of malware that threatens to issue or block access to a victim's personal data permanently unless a ransom is paid, has long had disastrous consequences for businesses.Organizations have lost critical business data as a result of such attacks, [...] The post [Is This The Finale Of The Path For Ransomware?] appeared first on [Dark Web Link | Deep web Onion Links | Darknet News].
[Bitcoin Superstar Review 2021: Is It Legit, Or A Scam?]
The high volatility of cryptocurrency is a source of concern for some investors because it makes it difficult to predict future price movements. For some traders, however, high volatility is a fantastic opportunity.As a result, smart traders are devising new and advancedpolicies to profit from fast price fluctuations irrespective of market direction, thanks to stagesfor [...] The post [Bitcoin Superstar Review 2021: Is It Legit, Or A Scam?] appeared first on [Dark Web Link | Deep web Onion Links | Darknet News].
[Zerofox'speripheral Threat Hunting Competences Give Analysts Toral Access To Raw Threat Intelligence]
Within the ZeroFoxpolicy, ZeroFox released advanced external threat hunting capabilities, planned to offer real-time threat aptitude to threat analysts, hunters, and cyber responders. This new threat hunting capability adds to ZeroFox's already comprehensive threat intelligence solutions. Direct entree to enhanced and raw intelligence footage, as well as searching throughout the firm's whole global data lake [...] The post [Zerofox'speripheral Threat Hunting Competences Give Analysts Toral Access To Raw Threat Intelligence] appeared first on [Dark Web Link | Deep web Onion Links | Darknet News].



Advisories

US-Cert Alerts & bulletins

* [CISA Announces Vulnerability Disclosure Policy (VDP) Platform]
* [NSA Releases Guidance on Securing Wireless Devices While in Public]
* [Top Routinely Exploited Vulnerabilities]
* [CISA Releases Security Advisory for Geutebruck Devices]
* [Apple Releases Security Updates]
* [Microsoft Releases Guidance for Mitigating PetitPotam NTLM Relay Attacks]
* [Cisco Releases Security Updates]
* [Drupal Releases Security Updates]
* [AA21-209A: Top Routinely Exploited Vulnerabilities]
* [AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013]
* [Vulnerability Summary for the Week of July 26, 2021]
* [Vulnerability Summary for the Week of July 19, 2021]

Zero Day Initiative Advisories

ZDI-CAN-14767: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14664: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14699: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14761: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14137: Fortinet
A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'brsn' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14727: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14518: Microsoft
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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14566: Fatek Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14225: Fatek Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14465: Fatek Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14517: Fatek Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14527: BMC
A CVSS score 6.4 (AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L) severity vulnerability discovered by 'Brandin Perry' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14600: Inkscape
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 'khangkito' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14599: Inkscape
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 'khangkito' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-13892: Schneider Electric
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-13891: Schneider Electric
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Vyacheslav Moskvin' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14668: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14237: VMware
A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14665: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14669: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14670: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14750: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14725: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 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-14765: Open Design Alliance (ODA)
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: 2021-07-30, 3 days ago. The vendor is given until 2021-11-27 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

[Ubuntu Security Notice USN-5026-1]

Ubuntu Security Notice 5026-1 - It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to consume resources, resulting in a denial of service. This issue only affected Ubuntu 18.04 LTS. It was discovered that QPDF incorrectly handled certain malformed PDF files. A remote attacker could use this issue to cause QPDF to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

[Ubuntu Security Notice USN-5027-1]

Ubuntu Security Notice 5027-1 - It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

[Ubuntu Security Notice USN-5025-2]

Ubuntu Security Notice 5025-2 - USN-5025-1 fixed a vulnerability in libsndfile. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

[Ubuntu Security Notice USN-5025-1]

Ubuntu Security Notice 5025-1 - It was discovered that libsndfile incorrectly handled certain malformed files. A remote attacker could use this issue to cause libsndfile to crash, resulting in a denial of service, or possibly execute arbitrary code.

[Ubuntu Security Notice USN-4944-2]

Ubuntu Security Notice 4944-2 - USN-4944-1 fixed vulnerabilities in MariaDB. It caused a regression. This update fixes the problem. Ubuntu 20.04 has been updated to MariaDB 10.3.30.

[Ubuntu Security Notice USN-5024-1]

Ubuntu Security Notice 5024-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

[Red Hat Security Advisory 2021-2932-01]

Red Hat Security Advisory 2021-2932-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, and out of bounds read vulnerabilities.

[Red Hat Security Advisory 2021-2931-01]

Red Hat Security Advisory 2021-2931-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service, information leakage, and out of bounds read vulnerabilities.

[Red Hat Security Advisory 2021-2438-01]

Red Hat Security Advisory 2021-2438-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include bypass, code execution, denial of service, open redirection, resource exhaustion, and remote shell upload vulnerabilities.

[Red Hat Security Advisory 2021-2437-01]

Red Hat Security Advisory 2021-2437-01 - 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 4.8.2. Issues addressed include bypass, cross site scripting, and denial of service vulnerabilities.

[Ubuntu Security Notice USN-5023-1]

Ubuntu Security Notice 5023-1 - It was discovered that Aspell incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

[Red Hat Security Advisory 2021-2914-01]

Red Hat Security Advisory 2021-2914-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.12.0. Issues addressed include man-in-the-middle, out of bounds write, and use-after-free vulnerabilities.

[Jira Ehcache RMI Missing Authentication]

Jira Data Center, Jira Core Data Center, Jira Software Data Center, and Jira Service Management Data Center exposed a Ehcache RMI network service which attackers, who can connect to the service, on port 40001 and potentially 40011, could execute arbitrary code of their choice in Jira through deserialization due to a missing authentication vulnerability. While Atlassian strongly suggests restricting access to the Ehcache ports to only Data Center instances, fixed versions of Jira will now require a shared secret in order to allow access to the Ehcache service. Various versions of Jira Data Center, Jira Core Data Center, Jira Software Data Center, and Jira Service Management Data Center are affected.

[Red Hat Security Advisory 2021-2763-01]

Red Hat Security Advisory 2021-2763-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. The kernel packages contain the Linux kernel, the core of any Linux operating system. The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Ansible is a SSH-based configuration management, deployment, and task execution system. The openshift-ansible packages contain Ansible code and playbooks for installing and upgrading OpenShift Container Platform 3.

[Ubuntu Security Notice USN-5022-1]

Ubuntu Security Notice 5022-1 - Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues. MySQL has been updated to 8.0.26 in Ubuntu 20.04 LTS and Ubuntu 21.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.35. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes. Various other issues were also addressed.

[Red Hat Security Advisory 2021-2881-01]

Red Hat Security Advisory 2021-2881-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.12.0. Issues addressed include man-in-the-middle, out of bounds write, and use-after-free vulnerabilities.

[Gentoo Linux Security Advisory 202107-55]

Gentoo Linux Security Advisory 202107-55 - Multiple vulnerabilities have been found in libsdl2, the worst of which could result in a Denial of Service condition. Versions less than 2.0.14-r1 are affected.

[Kernel Live Patch Security Notice LSN-0079-1]

It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. It was discovered that the virtual file system implementation in the Linux kernel contained an unsigned to signed integer conversion error. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

[Gentoo Linux Security Advisory 202107-54]

Gentoo Linux Security Advisory 202107-54 - Multiple vulnerabilities have been found in libyang, the worst of which could result in a Denial of Service condition. Versions less than 1.0.236 are affected.

[Red Hat Security Advisory 2021-2883-01]

Red Hat Security Advisory 2021-2883-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.12.0. Issues addressed include man-in-the-middle, out of bounds write, and use-after-free vulnerabilities.

[Red Hat Security Advisory 2021-2882-01]

Red Hat Security Advisory 2021-2882-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.12.0. Issues addressed include man-in-the-middle, out of bounds write, and use-after-free vulnerabilities.

[Gentoo Linux Security Advisory 202107-53]

Gentoo Linux Security Advisory 202107-53 - Multiple vulnerabilities have been found in Leptonica, the worst of which could result in a Denial of Service condition. Versions less than 1.80.0 are affected.

[Apple Security Advisory 2021-07-21-7]

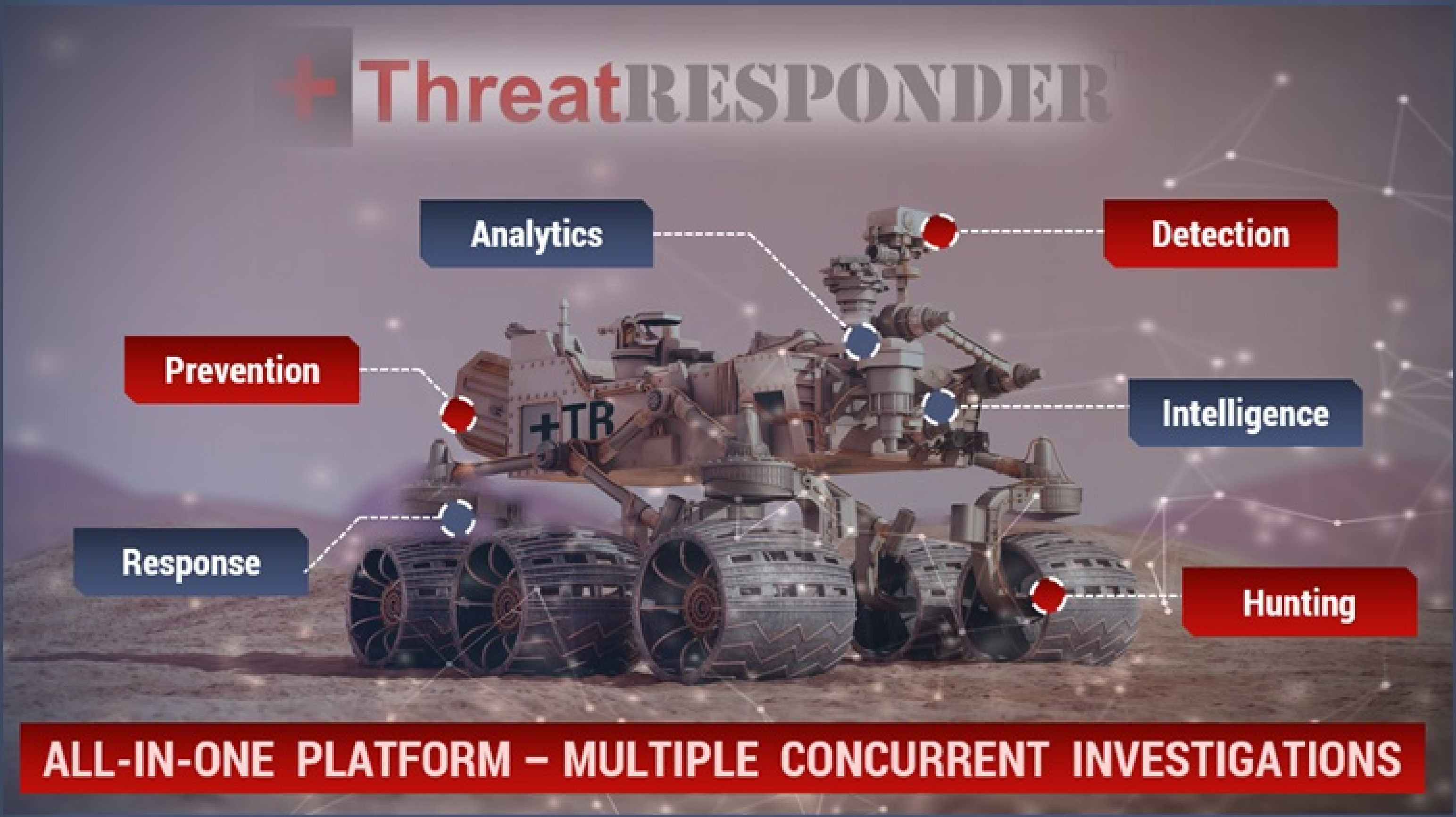
Apple Security Advisory 2021-07-21-7 - Safari 14.1.2 addresses code execution and use-after-free vulnerabilities.
Apple Security Advisory 2021-07-21-6
Apple Security Advisory 2021-07-21-6 - tvOS 14.7 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.2

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:

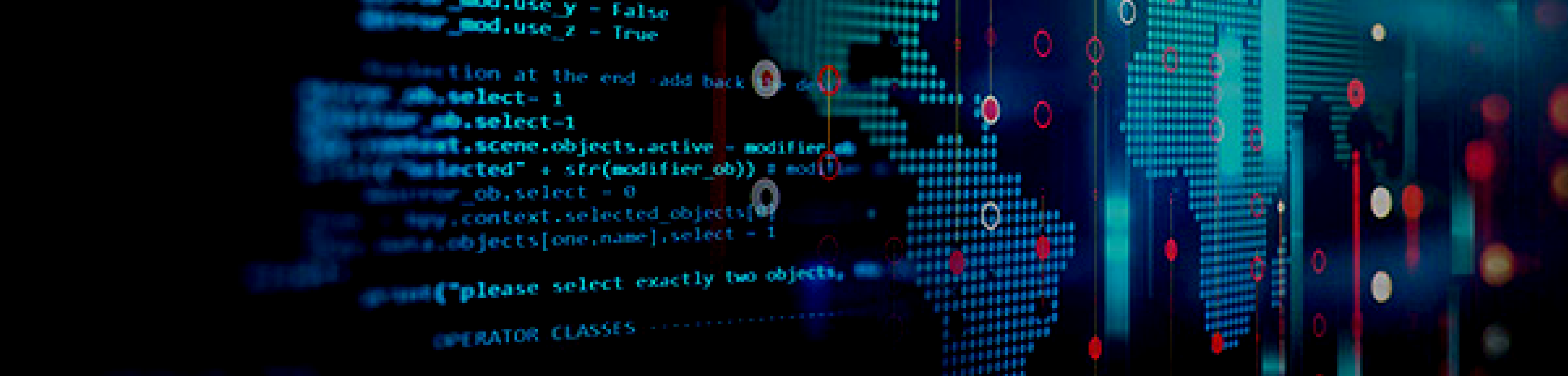
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

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

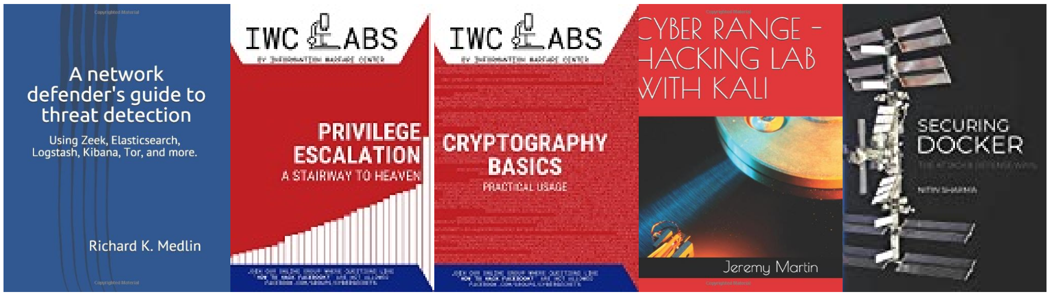


The Cyber Secrets publications on Amazon

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