Nov-01-21

CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

November 1, 2021

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

Internet Storm Center Infocon Status

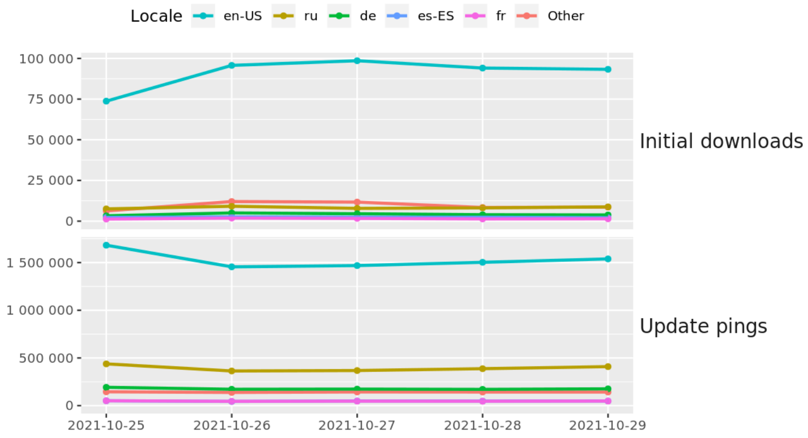
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.

Tor Browser downloads and updates by locale



The Tor Project - https://metrics.torproject.org/

Interesting News

* Subscribe to this OSINT resource to recieve it in in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

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

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

Index of Sections

LATEST NEWS

Packet Storm Security

* Android Has Its Head In The Sand With AbstractEmu Malware
* Signal Unveils How Far US Law Enforcement Will Go To Get Information About People
* Microsoft Found A Way To Evade SIP On macOS
* China's Personal Data Protection Law Kicks In Today
* Ransomware Has Disrupted Almost 1,000 Schools In The US This Year
* Suspected REvil Gang Insider Identified
* Luxury Hotel Chain In Thailand Reports Data Breach
* Google Fixes Two High Severity Zero Day Flaws In Chrome
* Location Data Collection Firm Admits Privacy Breach
* Feds Cuff Russian Said To Be Developer Of Trickbot Ransomware
* NPM Packages Disguised As Roblox API Code Caught Carrying Ransomware
* HTTPS Threats Grow More Than 314% Through 2021: Report
* Grief Ransomware Gang Pwns The NRA
* Cyberattack Cripples Iranian Fuel Distribution Network
* Microsoft Warns Over Uptick In Password Spraying Attacks
* Weeks Early: Adobe Dumps Massive Security Patch Update
* Cyber Attack Hits UK Internet Phone Providers
* As Fewer Victims Pay Ransoms, Conti Gang Looks To Sell Victim Data
* BlackMatter Botched Millions In Ransoms Due To Coding Flaw
* Facebook Admits Site Appears Hardwired For Misinformation
* Amazon Given Contract To Store Data For MI5, MI6, And GCHQ
* Millions Of Android Users Scammed In SMS Fraud Driven By Tik-Tok Ads
* CISA Warns Of Remote Code Execution Vulnerability With Discourse
* Ransomware Group Targets Financial Firms With Phishing
* Facebook Whistleblower Frances Haugen Faces UK Parliament

Krebs on Security

* 'Trojan Source' Bug Threatens the Security of All Code
* Zales.com Leaked Customer Data, Just Like Sister Firms Jared, Kay Jewelers Did in 2018
* FBI Raids Chinese Point-of-Sale Giant PAX Technology
* Conti Ransom Gang Starts Selling Access to Victims
* Missouri Governor Vows to Prosecute St. Louis Post-Dispatch for Reporting Security Vulnerability
* How Coinbase Phishers Steal One-Time Passwords
* Patch Tuesday, October 2021 Edition
* What Happened to Facebook, Instagram, & WhatsApp?
* FCC Proposal Targets SIM Swapping, Port-Out Fraud
* The Rise of One-Time Password Interception Bots

LATEST NEWS

Dark Reading

* Understanding the Human Communications Attack Surface
* Enterprises Allocating More IT Dollars on Cybersecurity
* Snyk Agrees to Acquire CloudSkiff, Creators of driftctl
* APTs, Teleworking, and Advanced VPN Exploits: The Perfect Storm
* Russian National Accused of Role in Trickbot Is Extradited to US
* Cybercriminals Take Aim at Connected Car Infrastructure
* What Exactly Is Secure Access Service Edge (SASE)?
* A Treehouse of Security Horrors
* Finding the Right Approach to Cloud Security Posture Management (CSPM)
* 6 Ways to Rewrite the Impossible Job Description
* SEO Poisoning Used to Distribute Ransomware
* Top Hardware Weaknesses List Debuts
* ICS Security Firm Dragos Reaches $1.7B Valuation in Latest Funding Round
* Ordr Unveils Cybersecurity Innovations and Ransom-Aware Rapid Assessment Service to Expand Its Leader
* NSA-CISA Series on Securing 5G Cloud Infrastructures
* Tech Companies Create Security Baseline for Enterprise Software
* US to Create Diplomatic Bureau to Lead Cybersecurity Policy
* Stop Zero-Day Ransomware Cold With AI
* 3 Security Lessons Learned From the Kaseya Ransomware Attack
* You've Just Been Ransomed ... Now What?

The Hacker News

* Critical Flaws Uncovered in Pentaho Business Analytics Software
* Securing SaaS Apps - CASB vs. SSPM
* New 'Trojan Source' Technique Lets Hackers Hide Vulnerabilities in Source Code
* Researchers Uncover 'Pink' Botnet Malware That Infected Over 1.6 Million Devices
* Police Arrest Suspected Ransomware Hackers Behind 1,800 Attacks Worldwide
* This New Android Malware Can Gain Root Access to Your Smartphones
* New 'Shrootless' Bug Could Let Attackers Install Rootkit on macOS Systems
* Winter is Coming for CentOS 8
* Russian TrickBot Gang Hacker Extradited to U.S. Charged with Cybercrime
* Google Releases Urgent Chrome Update to Patch 2 Actively Exploited 0-Day Bugs
* A Guide to Shift Away from Legacy Authentication Protocols in Microsoft 365
* Israeli Researcher Cracked Over 3,500 Wi-Fi Networks in Tel Aviv City
* New Wslink Malware Loader Runs as a Server and Executes Modules in Memory
* Malicious NPM Libraries Caught Installing Password Stealer and Ransomware
* Hackers Using Squirrelwaffle Loader to Deploy Qakbot and Cobalt Strike

LATEST NEWS

Security Week

* Atlanta Man Charged for Role in BEC Fraud Scheme
* 'Trojan Source' Attack Abuses Unicode to Inject Vulnerabilities Into Code
* Hackers Threaten to Out Israeli LGBTQ Dating Site Users
* Cybersecurity M&A Roundup: 41 Deals Announced in October 2021
* Iran Suspects Israel and US Behind Fuel Cyber Attack
* Google Introduces New Open-Source Data Privacy Protocol
* Apparent Iran-Linked Hackers Breach Israeli Internet Firm
* MITRE, CISA Announce 2021 List of Most Common Hardware Weaknesses
* NSA, CISA Release 5G Cloud Security Guidance
* HelpSystems Expands Shopping Spree With Digital Guardian Acquisition
* Massachusetts Health Network Hacked; Patient Info Exposed
* Shrootless: macOS Vulnerability Found by Microsoft Allows Rootkit Installation
* Russian Man Extradited to U.S. for Role in TrickBot Malware Development
* 12 People Arrested Over Ransomware Attacks on Critical Infrastructure
* Ransomware Attack Hits PNG Finance Ministry
* Chrome 95 Update Patches Exploited Zero-Days, Flaws Disclosed at Tianfu Cup
* India's Top Court Orders Probe Into Pegasus Snooping
* FBI Publishes Indicators of Compromise for Ranzy Locker Ransomware
* Free Decryption Tools Available for Babuk, AtomSilo and LockFile Ransomware
* Critical GoCD Authentication Flaw Exposes Software Supply Chain
* Scottish Cybersecurity Startup Unveils Versatile AI-Based Deception
* Vendor-Neutral Initiative Sets Bare-Minimum Baseline for Security
* 3 Questions for MDRs Helping to Get Your Enterprise to XDR
* Phishing Protection Provider SlashNext Raises $26 Million
* Cisco Patches High-Severity DoS Vulnerabilities in ASA, FTD Software

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Hacking Your Organization: 7 Steps Cybercriminals Use to Take Total Control of Your Network
* Misconceptions and Assumptions about Cybersecurity
* Multi-Stage Vishing Attacks are Coming to an Inbox Near You
* Eight Romance Phishing Scammers with Ties to Nigerian Organized Crime Arrested After Stealing Nearly
* Over Half of all Impersonation Attacks Target Non-Executive Employees
* KnowBe4's Q3 2021 Top-Clicked Phishing Email Report Includes New Global Data [INFOGRAPHIC]
* Nuclear Ransomware 3.0: It Is About To Get Much Worse
* Cybercriminals are using Craigslist email notifications to send phishing links
* CyberheistNews Vol 11 #42 [EYE OPENER] Why Security Awareness Testing Alone Isn't Enough
* Russian SolarWinds Hackers Newly Attack Supply Chain With Password-Spraying and Phishing

ISC2.org Blog

* (ISC)&sup2; CEO Clar Rosso Receives Cyber Futurist Executive Award
* New! Improvements to Your (ISC)&sup2; Cybersecurity Online Continuing Education
* Security does not end with Implementing Controls
* (ISC)2 Cybersecurity Workforce Study: Skills Gap Narrows But More Help Is Needed
* CISSP: The Time is Now

HackRead

* Trojan Source attack lets hackers exploit source code
* All About Ring's New Virtual Security Guard
* 10 Free and Best OSINT Tools 2021
* Researcher found 70% Wi-Fi networks in Tel Aviv are hackable
* Iranian Gas Stations Crippled After Suffering Cyberattack
* Millions of Android devices abused by UltimaSMS Adware Scam
* SolarWinds hackers, Nobelium, hit cloud providers and resellers

Koddos

* Trojan Source attack lets hackers exploit source code
* All About Ring's New Virtual Security Guard
* 10 Free and Best OSINT Tools 2021
* Researcher found 70% Wi-Fi networks in Tel Aviv are hackable
* Iranian Gas Stations Crippled After Suffering Cyberattack
* Millions of Android devices abused by UltimaSMS Adware Scam
* SolarWinds hackers, Nobelium, hit cloud providers and resellers

LATEST NEWS

Naked Security

* Europol announces "targeting" of 12 suspects in ransomware attacks
* Microsoft documents "SHROOTLESS" hack patched in latest Apple updates
* Microsoft Edge finally arrives on Linux - "Official" build lands in repos
* S3 Ep56: Cryptotrading rodent, ransomware hackback, and a Docusign phish [Podcast]
* Apple ships Monterey with security updates, fixes 0-day in Watch and TV products, updates iDevices
* Banking scam uses Docusign phish to thieve 2FA codes
* Cybersecurity Awareness Month: Listen up - CYBER&shy;SECURITY FIRST!
* Listen up 2 - CYBERSECURITY FIRST! How to protect yourself from supply chain attacks
* Listen up 3 - CYBERSECURITY FIRST! Cyberinsurance, help or hindrance?
* Listen up 4 - CYBERSECURITY FIRST! Purple teaming - learning to think like your adversaries

Threat Post

* 'Trojan Source' Hides Invisible Bugs in Source Code
* Google Chrome is Abused to Deliver Malware as 'Legit' Win 10 App
* All Sectors Are Now Prey as Cyber Threats Expand Targeting
* Suspected REvil Gang Insider Identified
* EU's Green Pass Vaccination ID Private Key Leaked
* Grief Ransomware Targets NRA
* WordPress Plugin Bug Lets Subscribers Wipe Sites
* Ransomware Attacks Are Evolving. Your Security Strategy Should, Too
* Teen Rakes in $2.74M Worth of Bitcoin in Phishing Scam
* Adobe's Surprise Security Bulletin Dominated by Critical Patches

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

LATEST NEWS

IBM Security Intelligence

* A Journey in Organizational Resilience: Security by Design
* What's New in the OWASP Top 10 2021?
* From Thanos to Prometheus: When Ransomware Encryption Goes Wrong
* 7 Ways to Improve Your Cybersecurity Team's Employee Satisfaction
* Remote Work Security: Handling Setbacks in the Time of COVID-19
* Identity and Access Management: What's Driving the Rush?
* 2021 Cyber Resilient Organization Study: Rise of Ransomware Shows the Need for Zero Trust and XDR
* How Shopping Bots Can Compromise Retail Cybersecurity
* Roundup: 2021 Energy & Utility Data Breaches and Defenses in the News
* Why Containers in the Cloud Can Be An Attacker's Paradise

InfoWorld

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

C4ISRNET - Media for the Intelligence Age Military

* The Pentagon is moving away from the Joint Regional Security Stacks
* C4ISRNET announces keynote speakers for CyberCon 2021
* Unmanned tech dominates Turkey's border security summit
* The Army wants to bolster its local cybersecurity defenders
* Following protest, Space Development Agency cancels, then reissues reworked satellite solicitation
* DISA director announces agency reorganization
* L3Harris awarded $121 million to upgrade Space Force weapons
* Why some Army users had email problems this week
* Army CIO's top priority is budgeting for new digital transformation strategy
* US Air Force teams with UK on machine learning demo

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

* Windows Exploitation Tricks: Relaying DCOM Authentication
* Using Kerberos for Authentication Relay Attacks

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.

* CTF Internacional MetaRed 2021 - 3rd STAGE
* DamCTF 2021
* DUNGEON - BSides Ahmedabad CTF 2021
* eHaCON CTF 2K21
* HK Cyber Security New Generation CTF Challenge 2021
* Winja CTF | c0c0n 2021
* K3RN3LCTF
* CSAW CTF Final Round 2021
* Intent CTF 2021
* SPbCTF's Student CTF 2021 Finals

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

* Napping: 1
* Empire: Breakout
* Empire: LupinOne
* Thales: 1
* ICA: 1

Tools & Techniques

Packet Storm Security Tools Links

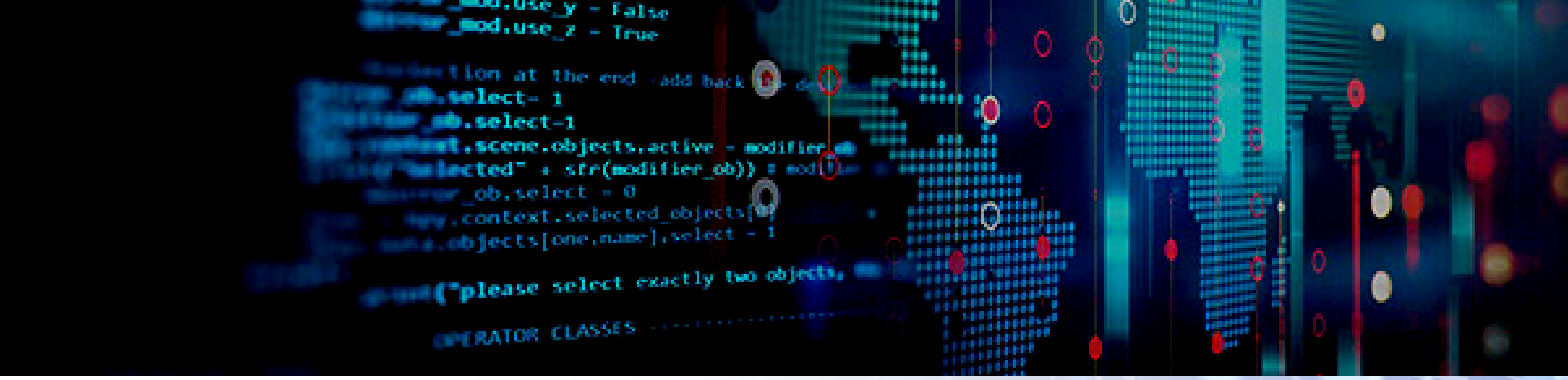
* GRAudit Grep Auditing Tool 3.2
* TOR Virtual Network Tunneling Tool 0.4.6.8
* Zeek 4.1.1
* GNU Privacy Guard 2.3.3
* GNU Privacy Guard 2.2.32
* Faraday 3.18.0
* AntiRansom 5
* nfstream 6.3.5
* Zed Attack Proxy 2.11.0 Cross Platform Package
* Wireshark Analyzer 3.4.9

Kali Linux Tutorials

* Limelighter : A Tool For Generating Fake Code Signing Certificates Or Signing Real Ones
* LazyCSRF : A More Useful CSRF PoC Generator
* Karma_V2 : A Passive Open Source Intelligence (OSINT) Automated Reconnaissance (Framework)
* Inceptor : Template-Driven AV/EDR Evasion Framework
* DorkScout : Golang Tool To Automate Google Dork Scan Against The Entiere Internet Or Specific Targets
* Fapro : Free, Cross-platform, Single-file mass network protocol server simulator
* ImpulsiveDLLHijack : C# Based Tool Which Automates The Process Of Discovering And Exploiting DLL Hija
* Rethink Network Access with Perimeter 81: a ZTNA Leader
* Packet-Sniffer : A pure-Python Network Packet Sniffing Tool
* Domain-Protect : Protect Against Subdomain Takeover

GBHackers Analysis

* Two European Men Sentenced for Providing 'Bulletproof Hosting' to Hackers
* Iranian Hackers Attack the US & Israeli Defense Technology - Microsoft Warns
* Company That Routes Billions of SMS For U.S Carriers Silently Says It Was Hacked
* New Attack Let Hackers Steal Data From Air-Gapped Networks Using Ethernet Cable
* Critical RCE Flaw in the core Netgear Firmware Let Remote Attackers to Take Control of an Affected Sy


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
.select= 1
.select=1
.scene.objects.active = modifier
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Weekly Cyber Security Video and Podcasts

SANS DFIR

* AC3 Threat Sightings: El Poder de la Observaci&oacute;n
* Identifying Opportunities to Collaborate and Contribute back
* Threat Hunting: Lotta Ins, Lotta Outs, Lotta What Have Yous
* Hunting mediante la detecci&oacute;n de anomal&iacute;as con Machine Learning y DAISY

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelg&auml;nger Your H&auml;x 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

* Spot Known WiFi Devices Nearby w/ the WiFi Nugget | HakByte
* YouTubers Targeted In Malware Attacks; REvil Goes Offline - ThreatWire
* How Companies Catch Ransomware Hackers

The PC Security Channel [TPSC]

* Vice Society Ransomware & Print Nightmare
* Windows 11 vs Memz

Eli the Computer Guy

* WHITE GUY FIRED for BEING A WHITE GUY... wins discrimination lawsuit for $10 MILLION
* FACEBOOK CHANGES NAME TO META... evil ceo changes name, not immoral actions...
* Office Hours - Tech Question and Answers
* GETTING COVID BOOSTER - "Fully Vaccinated" Definition May Change by CDC

Security Now

* The More Things Change... - Gummy Browsers Attack, What Happened to REvil, Comms Hub, Win 11 Fixes
* Minh Duong's Epic Rickroll - REvil Gone for Good? Tianfu Cup 2021, Patch Tuesday Aftermath

Troy Hunt

* Weekly Update 267

Intel Techniques: The Privacy, Security, & OSINT Show

* 239-Health Portals, Vulnerability Reports, and Voice Cloning
* 238-Tying Up Loose Ends

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For October, 2021
* Backdoor.Win32.Agent.sah Heap Corruption
* Trojan.Win32.Delf.bna Information Disclosure
* Trojan.Win32.Phires.zm Insecure Permissions
* My Movie Collection Sinatra App Login Cross Site Scripting
* My Movie Collection Sinatra App Movie Cross Site Scripting
* WordPress Hotel Listing 3.x Cross Site Scripting
* PHPJabbers Simple CMS 5 Cross Site Scripting
* Trojan.Win32.Pasta.mca Insecure Permissions
* WebCTRL OEM 6.5 Cross Site Scripting
* WordPress NextScripts: Social Networks Auto-Poster 4.3.20 XSS
* Movable Type 7 r.5002 XMLRPC API Remote Command Injection
* Android NFC Type Confusion
* Mini-XML 3.2 Heap Overflow
* Umbraco 8.14.1 Server-Side Request Forgery
* Sophos UTM WebAdmin SID Command Injection
* Backdoor.Win32.Prorat.ntz Weak Hardcoded Password
* Backdoor.Win32.Prorat.ntz Man-In-The-Middle
* Microsoft OMI Management Interface Authentication Bypass
* Virus.Win32.Ipamor.c Unauthenticated Reboot
* Backdoor.Win32.Antilam.14.o Remote Command Execution
* HEUR.Backdoor.Win32.Generic Unauthenticated Open Proxy
* Backdoor.Win32.Mazben.es Unauthenticated Open Proxy
* Hostel Management System 2.1 Cross Site Request Forgery / Cross Site Scripting
* Backdoor.Win32.Hupigon.afjk Authentication Bypass / Code Execution

CXSecurity

* Apache HTTP Server 2.4.50 Remote Code Execution
* Sophos UTM WebAdmin SID Command Injection
* Druva inSync Windows Client 7.5.2 - Local Privilege Escalation
* Hikvision Web Server Build 210702 Command Injection
* Keycloak 12.0.1 Server-Side Request Forgery
* Moodle Teacher Enrollment Privilege Escalation / Remote Code Execution
* Moodle Authenticated Spelling Binary Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

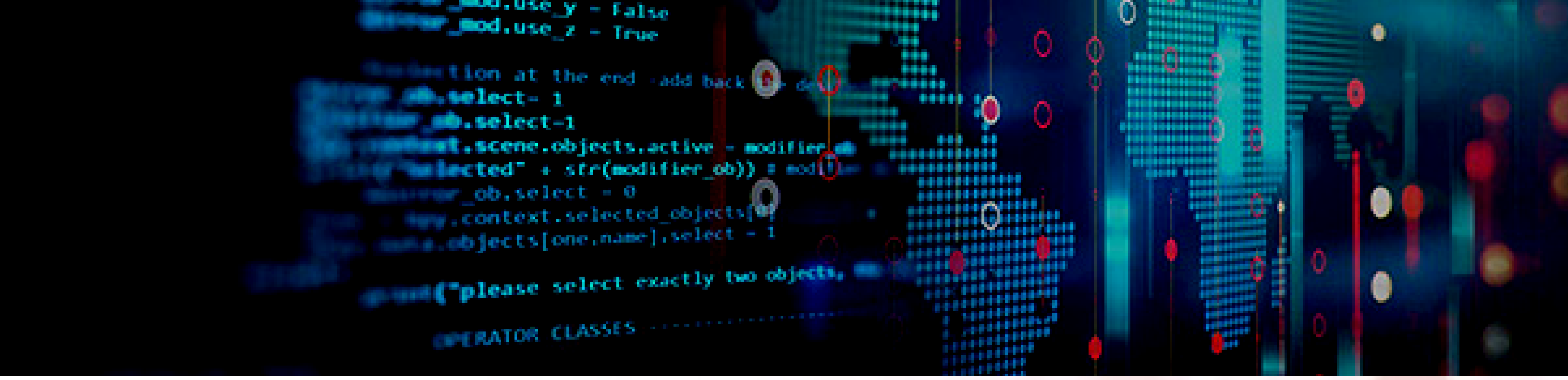
* [local] Mini-XML 3.2 - Heap Overflow
* [webapps] Movable Type 7 r.5002 - XMLRPC API OS Command Injection (Metasploit)
* [webapps] WebCTRL OEM 6.5 - 'locale' Reflected Cross-Site Scripting (XSS)
* [webapps] Umbraco v8.14.1 - 'baseUrl' SSRF
* [webapps] PHPGurukul Hostel Management System 2.1 - Cross-site request forgery (CSRF) to Cross-site S
* [webapps] WordPress Plugin Supsystic Contact Form 1.7.18 - 'label' Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Filterable Portfolio Gallery 1.0 - 'title' Stored Cross-Site Scripting (XS
* [webapps] phpMyAdmin 4.8.1 - Remote Code Execution (RCE)
* [webapps] Wordpress 4.9.6 - Arbitrary File Deletion (Authenticated) (2)
* [webapps] WordPress Plugin Ninja Tables 4.1.7 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Media-Tags 3.2.0.2 - Stored Cross-Site Scripting (XSS)
* [webapps] Engineers Online Portal 1.0 - 'id' SQL Injection
* [webapps] Engineers Online Portal 1.0 - 'multiple' Authentication Bypass
* [webapps] Engineers Online Portal 1.0 - 'multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Online Event Booking and Reservation System 1.0 - 'reason' Stored Cross-Site Scripting (XSS
* [local] Gestionale Open 11.00.00 - Local Privilege Escalation
* [local] OpenClinic GA 5.194.18 - Local Privilege Escalation
* [webapps] Balbooa Joomla Forms Builder 2.0.6 - SQL Injection (Unauthenticated)
* [webapps] Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)
* [webapps] Build Smart ERP 21.0817 - 'eidValue' SQL Injection (Unauthenticated)
* [webapps] Engineers Online Portal 1.0 - File Upload Remote Code Execution (RCE)
* [local] Netgear Genie 2.4.64 - Unquoted Service Path
* [webapps] WordPress Plugin TaxoPress 3.0.7.1 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Hikvision Web Server Build 210702 - Command Injection
* [webapps] Online Course Registration 1.0 - Blind Boolean-Based SQL Injection (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*

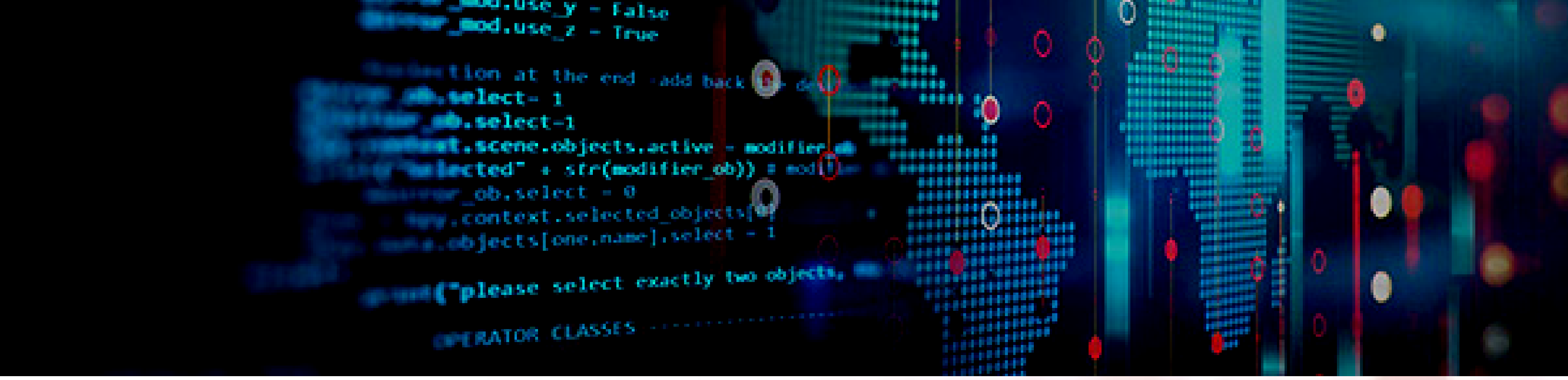
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://verify.laspec.gov.ng/z.html
https://verify.laspec.gov.ng/z.html notified by Zer0FauLT
http://undergroundriver.puertoprincesa.gov.ph/z.html
http://undergroundriver.puertoprincesa.gov.ph/z.html notified by Zer0FauLT
http://tourism.puertoprincesa.gov.ph/z.html
http://tourism.puertoprincesa.gov.ph/z.html notified by Zer0FauLT
http://main.puertoprincesa.gov.ph/z.html
http://main.puertoprincesa.gov.ph/z.html notified by Zer0FauLT
http://ocbo.puertoprincesa.gov.ph/z.html
http://ocbo.puertoprincesa.gov.ph/z.html notified by Zer0FauLT
http://liga.puertoprincesa.gov.ph/z.html
http://liga.puertoprincesa.gov.ph/z.html notified by Zer0FauLT
https://sdc.haryanapost.gov.in/z.html
https://sdc.haryanapost.gov.in/z.html notified by Zer0FauLT
https://report.haryanapost.gov.in/z.html
https://report.haryanapost.gov.in/z.html notified by Zer0FauLT
https://pman.haryanapost.gov.in/z.html
https://pman.haryanapost.gov.in/z.html notified by Zer0FauLT
https://e-dakiya.haryanapost.gov.in/z.html
https://e-dakiya.haryanapost.gov.in/z.html notified by Zer0FauLT
https://dakiya.haryanapost.gov.in/z.html
https://dakiya.haryanapost.gov.in/z.html notified by Zer0FauLT
https://covidwarriors.haryanapost.gov.in/z.html
https://covidwarriors.haryanapost.gov.in/z.html notified by Zer0FauLT
http://survey.mcludhiana.gov.in/z.html
http://survey.mcludhiana.gov.in/z.html notified by Zer0FaulT
http://testesuwidha.mcludhiana.gov.in/z.html
http://testesuwidha.mcludhiana.gov.in/z.html notified by Zer0FaulT
http://bamboocomposites.ipirti.gov.in/z.html
http://bamboocomposites.ipirti.gov.in/z.html notified by Zer0FaulT
http://services.mcludhiana.gov.in/z.html
http://services.mcludhiana.gov.in/z.html notified by Zer0FaulT
http://grievance.mcludhiana.gov.in/z.html
http://grievance.mcludhiana.gov.in/z.html notified by Zer0FaulT


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier
ected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

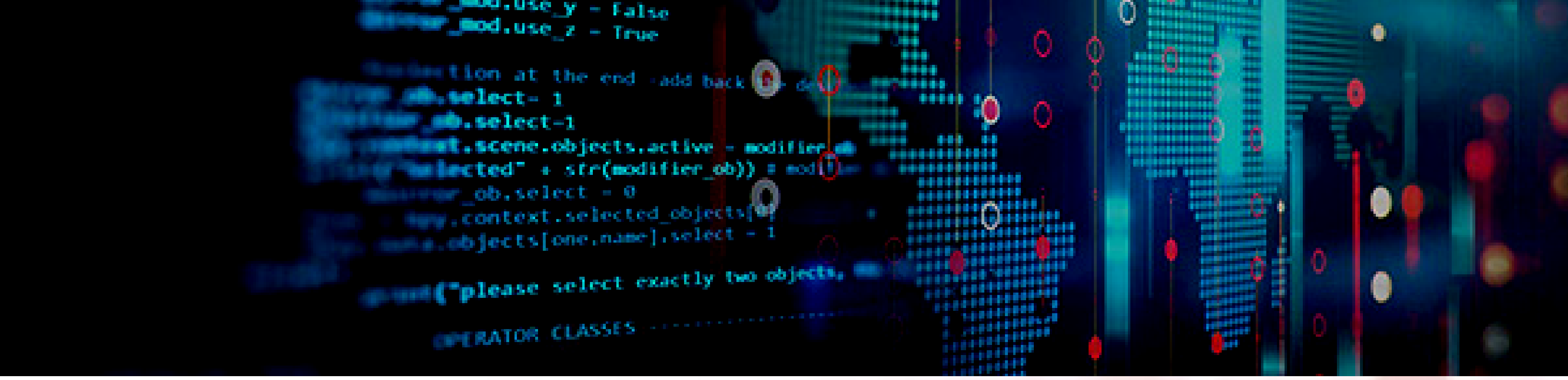
Dark Web News

Darknet Live

[39 Arrested in Italy for Selling Drugs on the Darkweb](#)
Italian law enforcement arrested 39 people for allegedly selling GHB, heroin, and cannabis, among others, on the darkweb. (via darknetlive.com)
[Europol: 150 Vendors Arrested in operation "Dark HunTOR"](#)
During operation Dark HunTOR, law enforcement arrested the administrators of DeepSea Market, Berlusconi Market, and 150 darkweb vendors. (via darknetlive.com)
[Czech Republic: Five Sentenced for Reselling Ecstasy](#)
Five Czech citizens were sentenced for reselling ecstasy purchased on the darkweb. (via darknetlive.com)
[Michigan Man Imprisoned for Selling PII on the Darkweb](#)
A Michigan man was sentenced to prison for hacking, stealing, and selling Personally Identifiable Information of thousands of victims on the darkweb. (via darknetlive.com)

Dark Web Link

[Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats](#)
Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from &#8220;Dark web&#8221; persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that &#8220;you didn't take any shit from anyone.&#8221; During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug](#)
Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[The Dark Web Has An Eye On YOU! Hackers Use 'Brute Force' To Attack Online Accounts](#)
The dark web is a shadowy part of the internet where criminals may interact in secret forums, share scamming tactics and services, and coordinate ransomware assaults. Because criminals operate in the shadows, authorities have a difficult time combating the threat. This implies that you must defend yourself. The internet works on three levels. The traditional [...] The post The Dark Web Has An Eye On YOU! Hackers Use 'Brute Force' To Attack Online Accounts appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

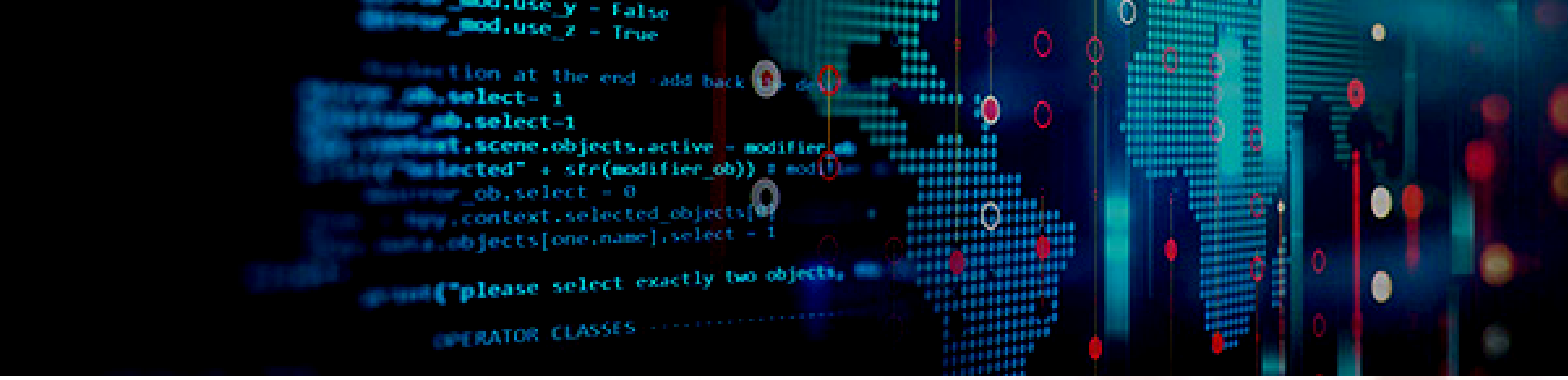
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

RiskIQ

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

FireEye

* GitLab Unauthenticated Remote Code Execution CVE-2021-22205 Exploited in the Wild
* Metasploit Wrap-Up
* 2022 Planning: Straight Talk on Zero Trust
* Sneaking Through Windows: Infostealer Malware Masquerades as Windows Application
* Hands-On IoT Hacking: Rapid7 at DefCon IoT Village, Part 2
* [Security Nation] Jack Cable on Ransomwhere
* Automation Enables Innovation in the Cloud
* Securely Advancing in the Sunshine State: Rapid7 Announces Tampa Office Opening
* NPM Library (ua-parser-js) Hijacked: What You Need to Know
* Recog: Data Rules Everything Around Me



Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* GoCD Authentication Vulnerability
* NSA-CISA Series on Securing 5G Cloud Infrastructures
* Cisco Releases Security Updates for Multiple Products
* ISC Releases Security Advisory for BIND
* 2021 CWE Most Important Hardware Weaknesses
* FBI Releases Indicators of Compromise Associated with Ranzy Locker Ransomware
* Adobe Releases Security Updates for Multiple Products
* AA21-291A: BlackMatter Ransomware
* AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems
* Vulnerability Summary for the Week of October 25, 2021
* Vulnerability Summary for the Week of October 18, 2021

Zero Day Initiative Advisories

ZDI-CAN-15671: Autodesk
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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15667: Autodesk
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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15449: Ivanti
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 'chudy' was reported to the affected vendor on: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15448: Ivanti
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 'chudy' was reported to the affected vendor on: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15665: Autodesk
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: 2021-10-29, 3 days ago. The vendor is

given until 2022-02-26 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-15668: Autodesk

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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15669: Autodesk

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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15664: Autodesk

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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15666: Autodesk

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: 2021-10-29, 3 days ago. The vendor is given until 2022-02-26 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-15296: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15587: Microsoft

A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15187: Microsoft

A CVSS score 2.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15446: Microsoft

A CVSS score 4.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15522: Autodesk

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 'Anonymous' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15443: Microsoft

A CVSS score 7.0 (AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Thomas

Bouzerar (@MajorTomSec) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15047: Trend Micro

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L) severity vulnerability discovered by 'Elias Martinez (filenotfound - https://www.linkedin.com/in/eli-martinez07/)' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15585: Microsoft

A CVSS score 2.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15521: Autodesk

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 'Anonymous' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15445: Microsoft

A CVSS score 2.2 (AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-15675: Autodesk

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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-10-27, 5 days ago. The vendor is given until 2022-02-24 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-14740: Orckestra

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 'Le Ngoc Anh - Sun* Cyber Security Research Team' was reported to the affected vendor on: 2021-10-25, 7 days ago. The vendor is given until 2022-02-22 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-15056: xhyve

A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Alisa Esage of Zero Day Engineering (zerodayengineering.com)' was reported to the affected vendor on: 2021-10-22, 10 days ago. The vendor is given until 2022-02-19 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-15541: WordPress

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'ngocnb and khuyenn from GiaoHangTietKiem JSC' was reported to the affected vendor on: 2021-10-22, 10 days ago. The vendor is given until 2022-02-19 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-15301: Ivanti

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 'chudy' was reported to the affected vendor on: 2021-10-22, 10 days ago. The vendor is given until 2022-02-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Red Hat Security Advisory 2021-4033-01
Red Hat Security Advisory 2021-4033-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Red Hat Security Advisory 2021-4034-01
Red Hat Security Advisory 2021-4034-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Red Hat Security Advisory 2021-4035-01
Red Hat Security Advisory 2021-4035-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Red Hat Security Advisory 2021-4039-01
Red Hat Security Advisory 2021-4039-01 - The GNU Compiler Collection is a portable compiler suite with support for various programming languages, including C, C++, and Fortran. The devtoolset-10-gcc packages provide the Red Hat Developer Toolset 10 version of GCC, as well as related libraries.
Red Hat Security Advisory 2021-4036-01
Red Hat Security Advisory 2021-4036-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
CODESYS 2.4.7.0 Denial Of Service
CODESYS Runtime Toolkit 32-bit versions prior to 2.4.7.56 suffer from a denial of service vulnerability.
Red Hat Security Advisory 2021-4038-01
Red Hat Security Advisory 2021-4038-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Red Hat Security Advisory 2021-4037-01
Red Hat Security Advisory 2021-4037-01 - The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Ubuntu Security Notice USN-5126-2
Ubuntu Security Notice 5126-2 - USN-5126-1 fixed a vulnerability in Bind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Kishore Kumar Kothapalli discovered that Bind incorrectly handled the lame cache when processing responses. A remote attacker could possibly use this issue to cause Bind to consume resources, resulting in a denial of service. Various other issues were also addressed.
Ubuntu Security Notice USN-5126-1
Ubuntu Security Notice 5126-1 - Kishore Kumar Kothapalli discovered that Bind incorrectly handled the lame cache when processing responses. A remote attacker could possibly use this issue to cause Bind to consume resources, resulting in a denial of service.
Red Hat Security Advisory 2021-3915-01
Red Hat Security Advisory 2021-3915-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.
Red Hat Security Advisory 2021-4012-01
Red Hat Security Advisory 2021-4012-01 - Red Hat support for Spring Boot provides an application platform that reduces the complexity of developing and operating applications for OpenShift as a containerized platform. This release of Red Hat support for Spring Boot 2.4.9 serves as a replacement for Red Hat support for Spring Boot 2.3.10 and includes security, bug fixes, and enhancements. For more information, see the release notes

listed in the References section.

Ubuntu Security Notice USN-5125-1

Ubuntu Security Notice 5125-1 - It was discovered that PHP-FPM in PHP incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code.

Apple Security Advisory 2021-10-26-11

Apple Security Advisory 2021-10-26-11 - tvOS 15 addresses bypass, code execution, denial of service, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-10

Apple Security Advisory 2021-10-26-10 - watchOS 8 addresses bypass, code execution, denial of service, out of bounds read, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-9

Apple Security Advisory 2021-10-26-9 - iOS 15 and iPadOS 15 addresses code execution, denial of service, out of bounds read, spoofing, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-8

Apple Security Advisory 2021-10-26-8 - Safari 15 addresses bypass, code execution, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-7

Apple Security Advisory 2021-10-26-7 - tvOS 15.1 addresses buffer overflow, code execution, cross site scripting, information leakage, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-6

Apple Security Advisory 2021-10-26-6 - watchOS 8.1 addresses buffer overflow, code execution, cross site scripting, information leakage, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-5

Apple Security Advisory 2021-10-26-5 - Security Update 2021-007 Catalina addresses code execution, integer overflow, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2021-10-26-4

Apple Security Advisory 2021-10-26-4 - macOS Big Sur 11.6.1 addresses code execution, integer overflow, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2021-10-26-3

Apple Security Advisory 2021-10-26-3 - macOS Monterey 12.0.1 addresses buffer overflow, bypass, code execution, cross site scripting, information leakage, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-2

Apple Security Advisory 2021-10-26-2 - iOS 14.8.1 and iPadOS 14.8.1 addresses code execution, information leakage, integer overflow, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-10-26-1

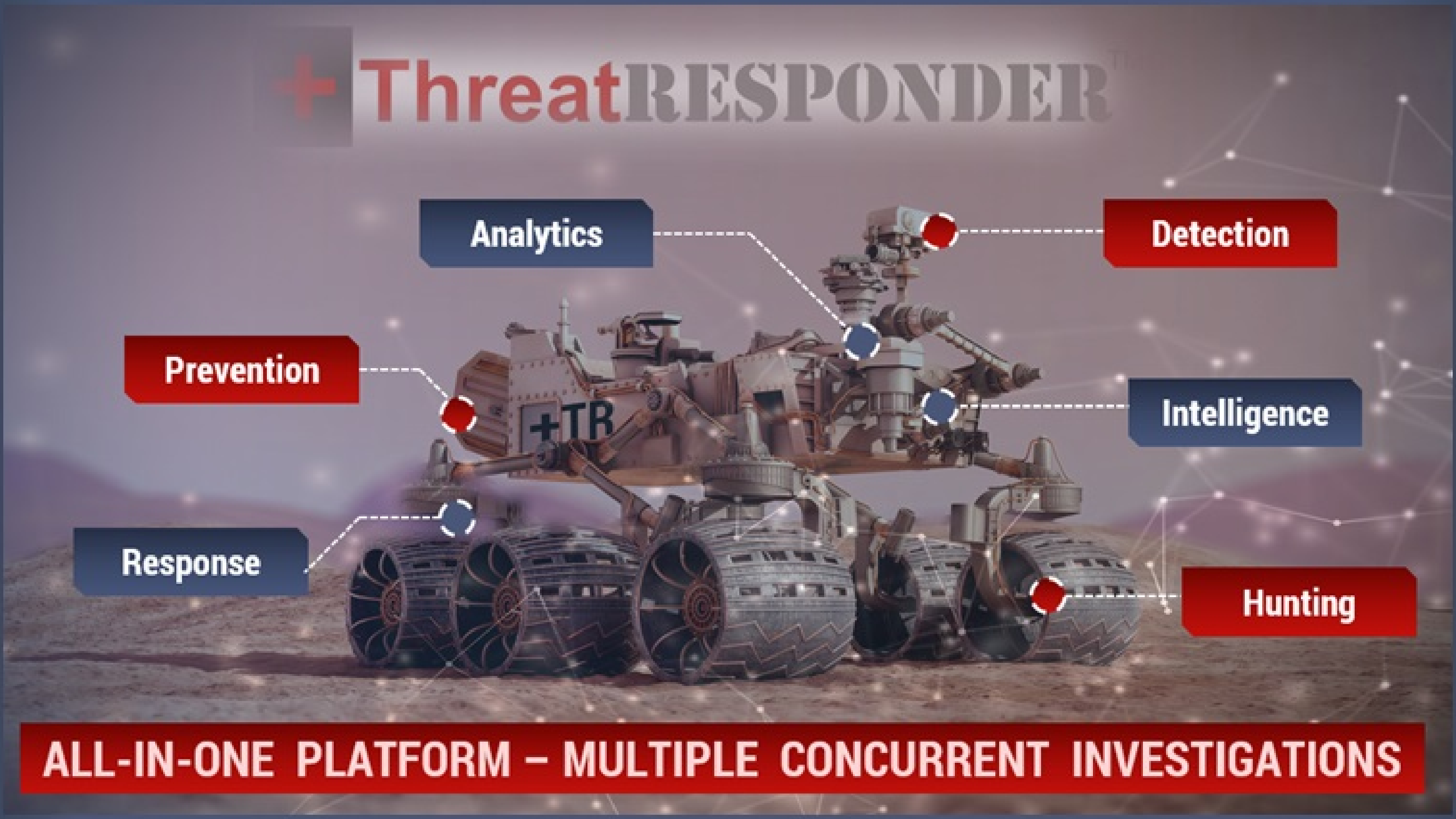
Apple Security Advisory 2021-10-26-1 - iOS 15.1 and iPadOS 15.1 addresses buffer overflow, code execution, cross site scripting, information leakage, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

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



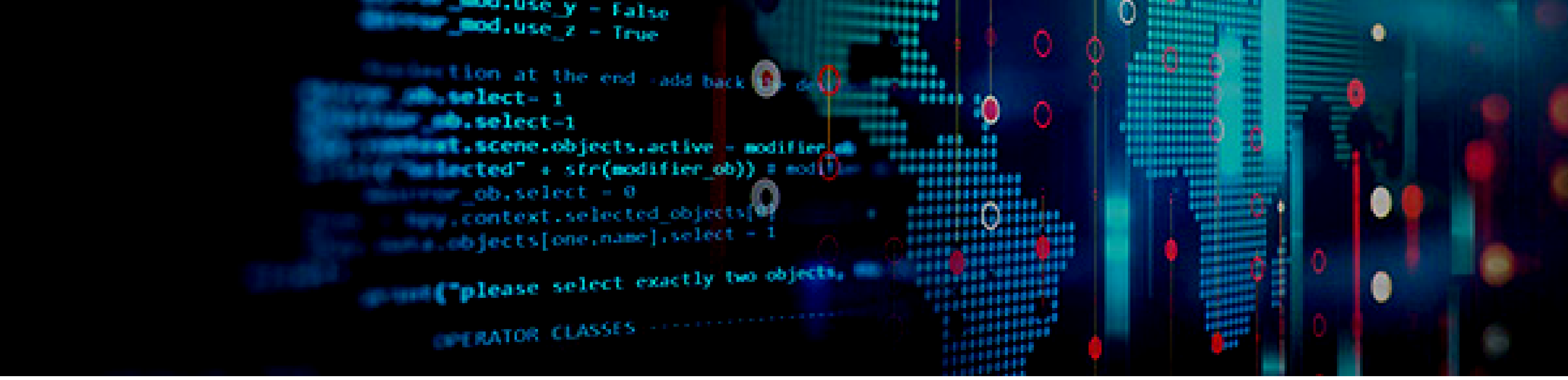
The Solution – ThreatResponder® Platform

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

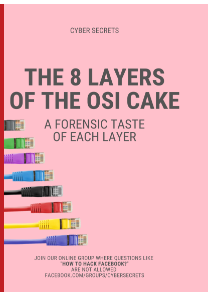


The Cyber Secrets publications on Amazon

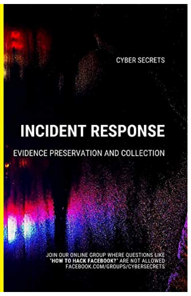
The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

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.

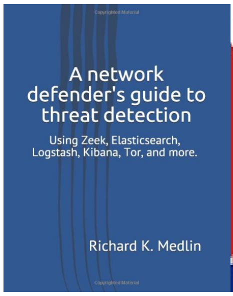
CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel

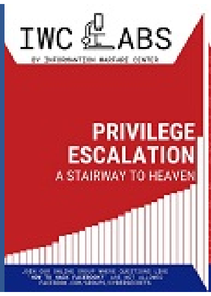


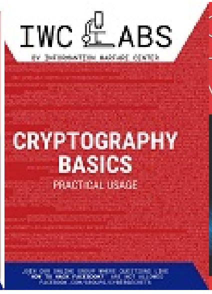
CYBER SECRETS
LAUNCHING
EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
INCIDENT RESPONSE

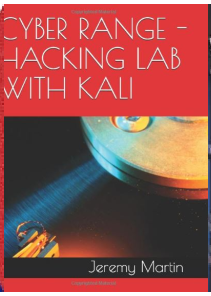


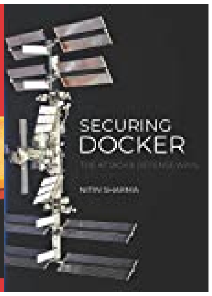
Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin









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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP