Dec-12-22

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

December 12, 2022

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:GREEN
http://isc.sans.edu

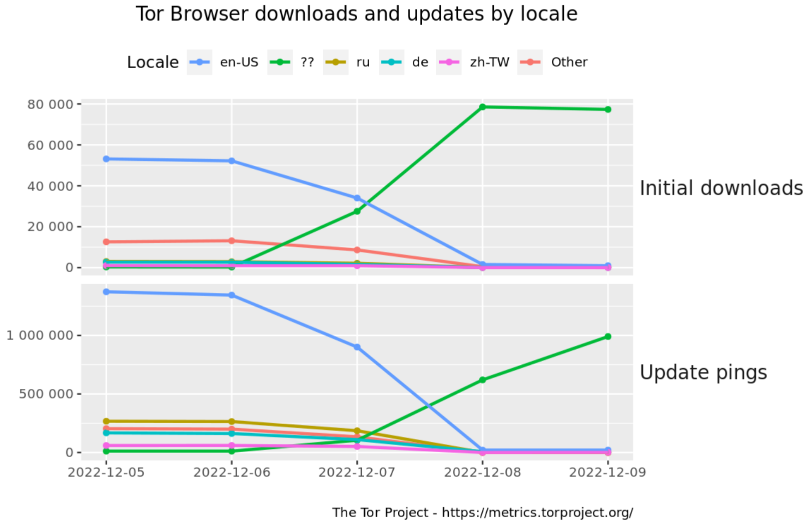
Internet Storm Center Infocon Status

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.



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

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

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* REvil-Hit Medibank To Pull Plug On IT, Shore Up Defenses
* North Korean Hackers Exploit Internet Explorer's Leftover Bits
* 2022's Greatest Hacks And Leaks, Ranked
* North Korea Using Freelance Techies To Fund Missiles And Nukes
* Apple Adds End-To-End Encryption To iCloud Device Backups
* Bad Software Cost US Businesses $2.1 Trillion In 2022
* Jack To Elon: Can We Just Get The Doxxing Over With?
* Five British Companies Fined For Making Half A Million Nuisance Calls
* South Pacific Vacations May Be Wrecked By Ransomware
* Ethereum Change Cut Cryptocurrency Power Demand
* San Francisco Makes U-Turn On Killer Robots Plan
* Uber, Motional Launch Robotaxi Service In Las Vegas
* This Privacy Ruling Against Meta Could Spell The End Of Targeted Ads
* Amnesty International Canada Claims Attack By China-Backed Forces
* Four Suspects Cuffed, Face Extradition Over Tax Refund Scam Plot
* CommonSpirit Confirms Network Accessed A Week Before Ransomware Attack
* Want To Detect Cobalt Strike On The Network? Look To Process Memory
* TSA To Expand Facial Recognition Across America
* Russian State-Owned Bank VTB Hit By Massive DDoS Attack
* KmsdBot Botnet Is Down After Operator Sends Typo In Command
* Explainer: ChatGPT - What Is OpenAI's Chatbot And What Is It Used For?
* FBI Warning: This Ransomware Gang Has Hit Over 100 Targets And Made More Than $60 Million
* AI Bot ChatGPT Stuns Academics With Essay Writing Skills / Usability
* Rackspace Customers Rage As Email Outage Continues
* Journalist Sues NSO After Being Hacked By Pegasus Spyware

Krebs on Security

* New Ransom Payment Schemes Target Executives, Telemedicine
* Judge Orders U.S. Lawyer in Russian Botnet Case to Pay Google
* ConnectWise Quietly Patches Flaw That Helps Phishers
* U.S. Govt. Apps Bundled Russian Code With Ties to Mobile Malware Developer
* Researchers Quietly Cracked Zeppelin Ransomware Keys
* Disneyland Malware Team: It's a Puny World After All
* Top Zeus Botnet Suspect "Tank" Arrested in Geneva
* Lawsuit Seeks Food Benefits Stolen By Skimmers
* Patch Tuesday, November 2022 Election Edition
* LinkedIn Adds Verified Emails, Profile Creation Dates

LATEST NEWS

Dark Reading

* TikTok Banned on Govt. Devices; Will Private Sector Follow Suit?
* Iran-Backed MuddyWater's Latest Campaign Abuses Syncro Admin Tool
* 7 Ways Gaming Companies Can Battle Cybercrime on Their Platforms
* 43 Trillion Security Data Points Illuminate Our Most Pressing Threats
* Iranian APT Targets US With Drokbk Spyware via GitHub
* How Naming Can Change the Game in Software Supply Chain Security
* Google: Use SLSA Framework for Better Software Security
* 3 Ways Attackers Bypass Cloud Security
* CNAPP Shines a Light Into Evolving Cloud Environments
* Agrius Iranian APT Group Cuts Into Diamond Industry
* How Do I Use the Domain Score to Determine Whether a Domain Is a Threat?
* Single Sign-on: It's Only as Good as Your Ability to Use It
* Lack of Cybersecurity Expertise Poses Threat for Public-Safety Orgs
* APT37 Uses Internet Explorer Zero-Day to Spread Malware
* Phishing in the Cloud: We're Gonna Need a Bigger Boat
* (ISC)&sup2; Recruits 110,000 People Interested in a Cybersecurity Career in Three Months
* Interpres Security Emerges from Stealth to Help Companies to Optimize Security Performance
* Where to Find the Best Open Source Security Technology
* Report: Air-Gapped Networks Vulnerable to DNS Attacks
* Hacker Fails for the Win

The Hacker News

* Keep Your Grinch at Bay: Here's How to Stay Safe Online this Holiday Season
* Royal Ransomware Threat Takes Aim at U.S. Healthcare System
* Hack-for-Hire Group Targets Travel and Financial Entities with New Janicab Malware Variant
* Researchers Detail New Attack Method to Bypass Popular Web Application Firewalls
* Cisco Warns of High-Severity Unpatched Flaw Affecting IP Phones Firmware
* Using XDR to Consolidate and Optimize Cybersecurity Technology
* New TrueBot Malware Variant Leveraging Netwrix Auditor Bug and Raspberry Robin Worm
* Why is Robust API Security Crucial in eCommerce?
* Researchers Uncover New Drokbk Malware that Uses GitHub as a Dead Drop Resolver
* What Stricter Data Privacy Laws Mean for Your Cybersecurity Policies
* MuddyWater Hackers Target Asian and Middle East Countries with Updated Tactics
* Researchers Uncover Darknet Service Allowing Hackers to Trojanize Legit Android Apps
* COVID-bit: New COVert Channel to Exfiltrate Data from Air-Gapped Computers
* Apple Boosts Security With New iMessage, Apple ID, and iCloud Protections
* Best Year-End Cybersecurity Deals from Uptycs, SANS Institute, and Bitdefender

LATEST NEWS

Security Week

* Python, JavaScript Developers Targeted With Fake Packages Delivering Ransomware
* Rackspace Hit With Lawsuits Over Ransomware Attack
* Device Exploits Earn Hackers Nearly $1 Million at Pwn2Own Toronto 2022
* As Wiretap Claims Rattle Government, Greece Bans Spyware
* Video: Deep Dive on PIPEDREAM/Incontroller ICS Attack Framework
* Interpres Security Emerges From Stealth Mode With $8.5 Million in Funding
* Healthcare Organizations Warned of Royal Ransomware Attacks
* Cisco Working on Patch for Publicly Disclosed IP Phone Vulnerability
* LF Electromagnetic Radiation Used for Stealthy Data Theft From Air-Gapped Systems
* SOHO Exploits Earn Hackers Over $100,000 on Day 3 of Pwn2Own Toronto 2022
* Over 4,000 Vulnerable Pulse Connect Secure Hosts Exposed to Internet
* EU Court: Google Must Delete Inaccurate Search Info If Asked
* Removing the Barriers to Security Automation Implementation
* Apple Scraps CSAM Detection Tool for iCloud Photos
* Vulnerabilities Allow Researcher to Turn Security Products Into Wipers
* WAFs of Several Major Vendors Bypassed With Generic Attack Method
* Iranian Hackers Deliver New 'Fantasy' Wiper to Diamond Industry via Supply Chain Attack
* Lighting Giant Acuity Brands Discloses Two Data Breaches
* TikTok Hit by US Lawsuits Over Child Safety, Security Fears
* CloudSEK Blames Hack on Another Cybersecurity Company
* Pwn2Own Toronto 2022, Day 2: Smart Speaker Exploits Earn Big Chunk of $280,000 Total
* Apple Adding End-to-End Encryption to iCloud Backup
* Google Documents IE Browser Zero-Day Exploited by North Korean Hackers
* Cyberattack on Top Indian Hospital Highlights Security Risk
* Big Tech Vendors Object to US Gov SBOM Mandate
* Investors Pour $200 Million Into Compliance Automation Startup Drata

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* [EYE OPENER] How ChatGPT Can Be Used For Social Engineering
* Incident Response Actions are Systematically Reversed by Hackers to Maintain Persistence
* New Modular Attack Chain Found That Allows Attackers to Change Payloads Mid-Breach
* Scammer Group Uses Business Email Compromise to Impersonate European Investment Portals
* [Eye Opener] Cybersecurity Resilience Emerges as Top Priority as 62% of Companies Say Security Incide
* Cyber Insurers Focus on Catastrophic Attacks and Required Minimum Defenses as Premiums Double
* Archives Overtake Office Documents as the Most Popular File Type to Deliver Malware
* Ransomware, Ransom-war and Ran-some-where: What We Can Learn When the Hackers Get Hacked
* Russian Threat Actor Impersonates Aerospace and Defense Companies
* Holiday Shopping Scams Online Are Too Good to be True

ISC2.org Blog

* Level Up Your Cloud Security Skills and Your Career Options
* Latest Cyberthreats and Advisories - December 9, 2022
* Working with the U.S. Government: An Overview of the U.S. Cybersecurity Maturity Model Certification
* What It Takes to be a Cybersecurity Professional: The Non-Technical Skills You Need
* Latest Cyberthreats and Advisories - December 2, 2022

HackRead

* Zombinder on Dark Web Lets Hackers Add Malware to Legit Apps
* Cyber Security Firm CloudSEK Points Finger at Rival Over Breach
* Phishing Scams: How To Recognize A Scam Email, VOIP call, or Text
* Pwn2Own Day 1 and 2: Samsung, HP, MikroTik & Netgear Pwned
* The Onyx Fms: Monitor And Prevent Telecom Fraud In Real-time
* DeFiChain's Grand Central Hard Fork Is Now LIVE
* Leading Crypto Exchange Bybit Announces ApeX Pro Integration

Koddos

* Zombinder on Dark Web Lets Hackers Add Malware to Legit Apps
* Cyber Security Firm CloudSEK Points Finger at Rival Over Breach
* Phishing Scams: How To Recognize A Scam Email, VOIP call, or Text
* Pwn2Own Day 1 and 2: Samsung, HP, MikroTik & Netgear Pwned
* The Onyx Fms: Monitor And Prevent Telecom Fraud In Real-time
* DeFiChain's Grand Central Hard Fork Is Now LIVE
* Leading Crypto Exchange Bybit Announces ApeX Pro Integration

LATEST NEWS

Naked Security

* S3 Ep112: Data breaches can haunt you more than once! [Audio + Text]
* Credit card skimming - the long and winding road of supply chain failure
* SIM swapper sent to prison for 2FA cryptocurrency heist of over $20m
* Number Nine! Chrome fixes another 2022 zero-day, Edge patched too
* Ping of death! FreeBSD fixes crashtastic bug in network tool
* Apple pushes out iOS security update that's more tight-lipped than ever
* LastPass admits to customer data breach caused by previous breach
* The CHRISTMA EXEC network worm - 35 years and counting!
* S3 Ep111: The business risk of a sleazy "nudity unfilter" [Audio + Text]
* Serious Security: MD5 considered harmful - to the tune of $600,000

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

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

* Why Cybersecurity Risk Assessment Matters in the Banking Industry
* What CISOs Should Know About CIRCIA Incident Reporting
* Containers, Security, and Risks within Containerized Environments
* Inside the Second White House Ransomware Summit
* Did Brazil DSL Modem Attacks Change Device Security?
* Who Carries the Weight of a Cyberattack?
* Transitioning to Quantum-Safe Encryption
* Securing Your SAP Environments: Going Beyond Access Control
* How Do You Plan to Celebrate National Computer Security Day?
* Deploying Security Automation to Your Endpoints

InfoWorld

* Open source security fought back in 2022
* What to do when your devops team is downsized
* Full-stack engineering is one-third as good
* Visual Studio Code 1.74 boosts remote development
* Airtable becomes latest company to announce layoffs, cutting 20% of its workforce
* GitHub Copilot for Business plans unveiled
* Who is invited to your cloud strategy party?
* JDK 20: The new features in Java 20
* Intro to Alpine.js: A JavaScript framework for minimalists
* How to use BufferedStream and MemoryStream in C#

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

The Hacker Corner

Conferences

* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* Exploiting CVE-2022-42703 - Bringing back the stack attack
* Mind the Gap

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.

* INTENT CTF 2022
* X-MAS CTF 2022
* pingCTF 2022
* BackdoorCTF 2022
* ISITDTU CTF 2022 Finals
* Damncon 2022
* niteCTF
* ASIS CTF Finals 2022
* Real World CTF 5th
* IrisCTF 2023

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

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

Tools & Techniques

Packet Storm Security Tools Links

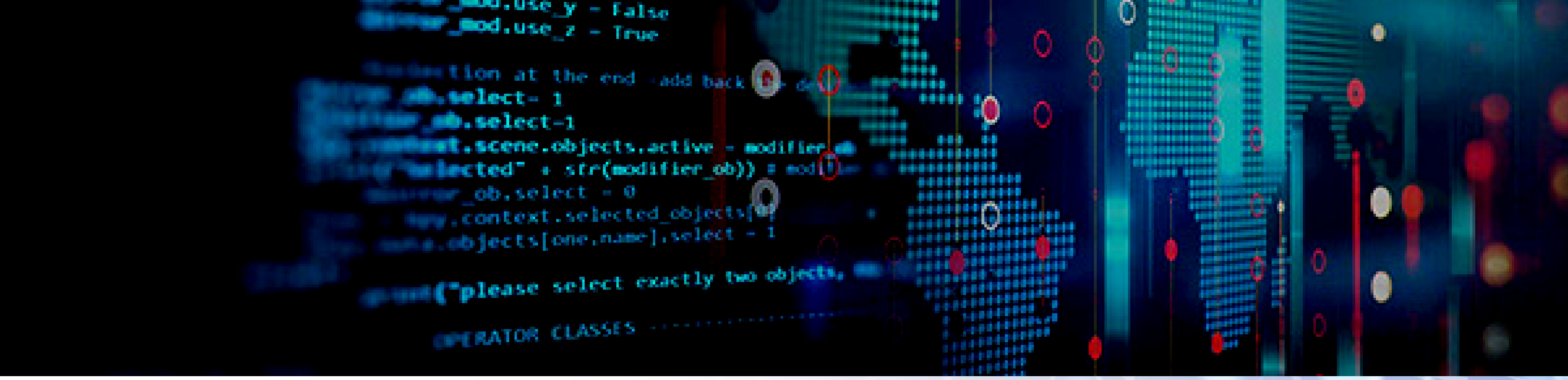
* Wireshark Analyzer 4.0.2
* TOR Virtual Network Tunneling Tool 0.4.7.12
* GNUnet P2P Framework 0.19.0
* Faraday 4.3.0
* Clam AntiVirus Toolkit 1.0.0
* Suricata IDPE 6.0.9
* Falco 0.33.1
* Zeek 5.0.4
* Packet Fence 12.1.0
* Stegano 0.11.1

Kali Linux Tutorials

* Neton : A Sandbox Information Gathering Tool
* Shells : Little Script For Generating Revshells
* Pywirt : Python Windows Incident Response Toolkit
* DomainDouche - OSINT Tool to Abuse SecurityTrails Domain
* D4TA-HUNTER : GUI OSINT Framework With Kali Linux
* Pycrypt : Python Based Crypter That Can Bypass Any Antivirus Products
* EvilTree : A Remake Of The Classic "Tree" Command
* Kubeeye : Tool To Find Various Problems On Kubernetes
* MSMAP : Memory WebShell Generator
* SharpSCCM : A C# Utility For Interacting With SCCM

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input



Weekly Cyber Security Video and Podcasts

SANS DFIR

- Analysis Paralysis? Setting the Right Goal for Your Incident Analysis
- Hunting Threat Actors Using OSINT
- Updates in DFIR
- Threat Hunting in Microsoft 365 Environment

Defcon Conference

- DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
- DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
- DEF CON 30 - Silk - DEF CON Memorial Interview
- DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

- Twitter API Bug Affects Millions of Users - ThreatWire
- OS Detection - USB Rubber Ducky
- Live Hacking Q&A with Kody and Michael

The PC Security Channel [TPSC]

- Best Virus Removal Tools: Cleaning a deeply infected system
- Fake MSI Afterburner with Hidden Malware

Eli the Computer Guy

- BLUE APRON LAYOFFS - Tech Sector IMPLODING
- CARVANA going BANKRUPT - Tech Industry FAILING
- BUZZFEED LAYOFFS - Stock is at $1!
- COVID MASK MANDATES are COMING BACK

Security Now

- LastPass Again - South Dakota bans TikTok, Anker Eufy Camera debacle, Mozilla yanks trusted root
- Freebie Bots & Evil Cameras - iSpoofer no more, Boa server vulnerability, CISA on Mastodon

Troy Hunt

- Weekly Update 325

Intel Techniques: The Privacy, Security, & OSINT Show

- 285-Travel Security Revisited
- 284-Password Managers & 2FA Revisited

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Spitfire CMS 1.0.475 PHP Object Injection
* Senayan Library Management System 9.1.0 SQL Injection
* Senayan Library Management System 9.0.0 SQL Injection
* Senayan Library Management System 9.0.0 Cross Site Scripting
* Senayan Library Management System 9.4.0 Cross Site Scripting
* ILIAS eLearning 7.15 Command Injection / XSS / LFI / Open Redirect
* Intel Data Center Manager 4.1 SQL Injection
* Intel Data Center Manager 5.1 Local Privilege Escalation
* Zhuhai Suny Technology ESL Tag Forgery / Replay Attacks
* snap-confine must_mkdir_and_open_with_perms() Race Condition
* Planet eStream Code Execution / SQL Injection / XSS / Broken Control
* Delta Electronics DVW-W02W2-E2 2.42 Command Injection
* Delta Electronics DX-2100-L1-CN 1.5.0.10 Command Injection / XSS
* Windows HTTP.SYS Kerberos PAC Verification Bypass / Privilege Escalation
* py7zr 0.20.0 Directory Traversal
* pixman pixman_sample_floor_y Integer Overflow
* VMware vCenter vScalation Privilege Escalation
* Senayan Library Management System 9.5.1 SQL Injection
* Drupal H5P Module 2.0.0 Zip Slip Traversal
* Automotive Shop Management System 1.0 SQL Injection
* Zillya Total Security 3.0.2367.0 / 3.0.2368.0 Local Privilege Escalation
* Packet Storm New Exploits For November, 2022
* Backdoor.Win32.Delf.gj MVID-2022-0663 Information Disclosure
* IBM Websphere Application Server 7.0 Cross Site Scripting
* perfSONAR 4.4.5 Cross Site Request Forgery

CXSecurity

* VMware vCenter vScalation Privilege Escalation
* Microsoft Exchange ProxyNotShell Remote Code Execution
* vBulletin 5.5.2 PHP Object Injection
* Remote Control Collection Remote Code Execution
* F5 BIG-IP iControl Remote Command Execution
* ChurchInfo 1.2.13-1.3.0 Remote Code Execution
* ZTE ZXHN-H108NS Stack Buffer Overflow / Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

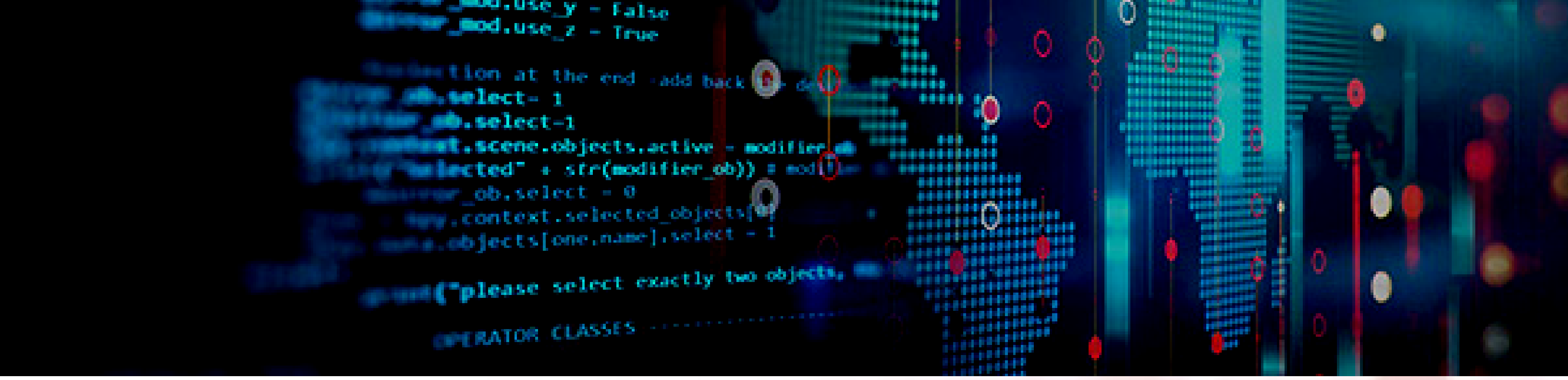
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [webapps] Open Web Analytics 1.7.3 - Remote Code Execution
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - Stored Cross-Site Scripting (XSS)

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.


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

Latest Hacked Websites

Published on Zone-h.org

http://dishub.nttprov.go.id

http://dishub.nttprov.go.id notified by Galang10

http://disnak.nttprov.go.id

http://disnak.nttprov.go.id notified by Galang10

http://nongbua.nfe.go.th/ok.htm

http://nongbua.nfe.go.th/ok.htm notified by Mr. BDKR28

https://ptun-bandarlampung.go.id

https://ptun-bandarlampung.go.id notified by Galang10

http://ingaf.gov.in/KHC.html

http://ingaf.gov.in/KHC.html notified by B3g0k&#91;Kurdish Hacker&#93;

http://vigyanlekha.gov.in/KHC.html

http://vigyanlekha.gov.in/KHC.html notified by B3g0k&#91;Kurdish Hacker&#93;

http://www.skhos.go.th/img/readme.html

http://www.skhos.go.th/img/readme.html notified by Mr&#039;Pl4Nkt0N

https://simasmatamoros.gob.mx/by.html

https://simasmatamoros.gob.mx/by.html notified by z7F HaCkEr

https://www.matamoroscoahuila.gob.mx/by.html

https://www.matamoroscoahuila.gob.mx/by.html notified by z7F HaCkEr

http://procurement.dgr.go.th/show_file/

http://procurement.dgr.go.th/show_file/ notified by Jaring

http://sipa.pt-bandung.go.id/el.htm

http://sipa.pt-bandung.go.id/el.htm notified by ./An9el4-137

https://nathalie.pn-tanjungpinangkota.go.id/el.htm

https://nathalie.pn-tanjungpinangkota.go.id/el.htm notified by ./An9el4-137

https://ptsp.pn-tanjungpinangkota.go.id/el.htm

https://ptsp.pn-tanjungpinangkota.go.id/el.htm notified by ./An9el4-137

https://sipp.pn-tanjungpinangkota.go.id/el.htm

https://sipp.pn-tanjungpinangkota.go.id/el.htm notified by ./An9el4-137

https://angola.mofa.go.ug

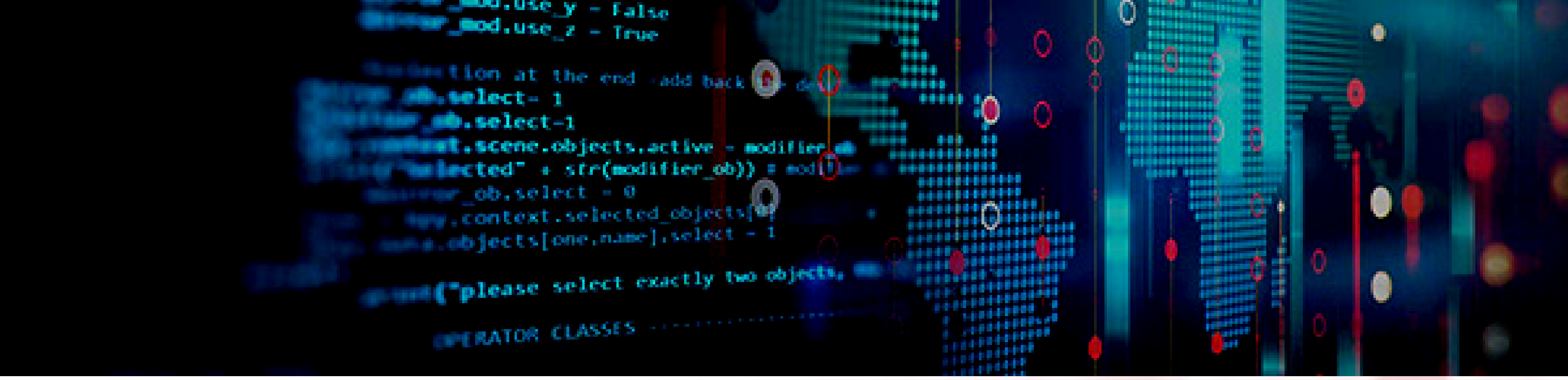
https://angola.mofa.go.ug notified by z7F HaCkEr

https://algiers.mofa.go.ug

https://algiers.mofa.go.ug notified by z7F HaCkEr

https://dmu.ict.go.ug

https://dmu.ict.go.ug notified by z7F HaCkEr

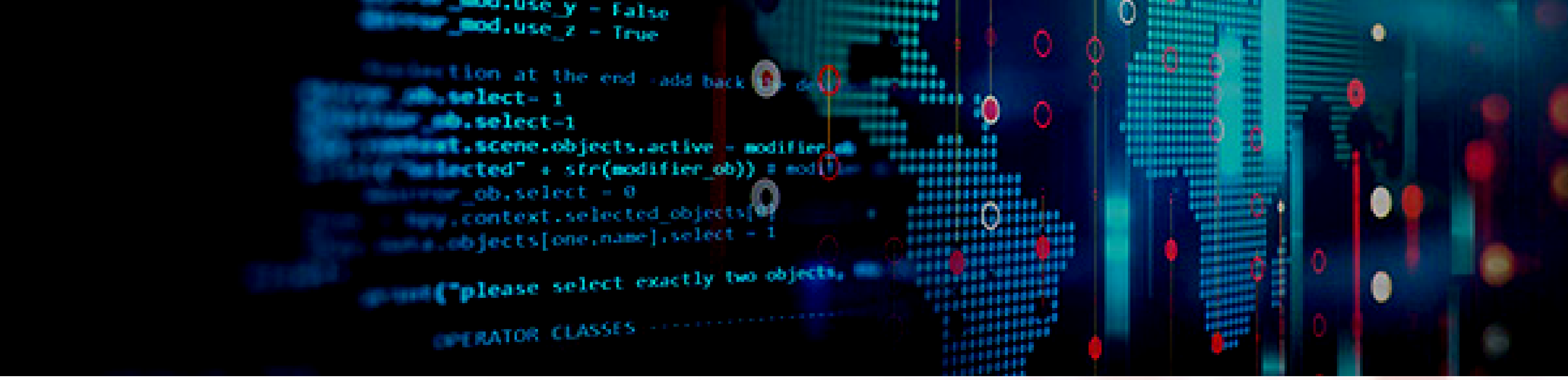

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Dark Web News

Darknet Live

[Flugsvamp 2.0 Admin added to Europe "Most Wanted" list]()
[German Dark Web Drugs Vendor Indicted]()
[Florida Dark Web Drugs Vendor Sentenced to Prison]()
[Training by OSCE on cryptocurrencies and Dark Web investigations in Kyrgyzstan]()

Dark Web Link



Trend Micro Anti-Malware Blog

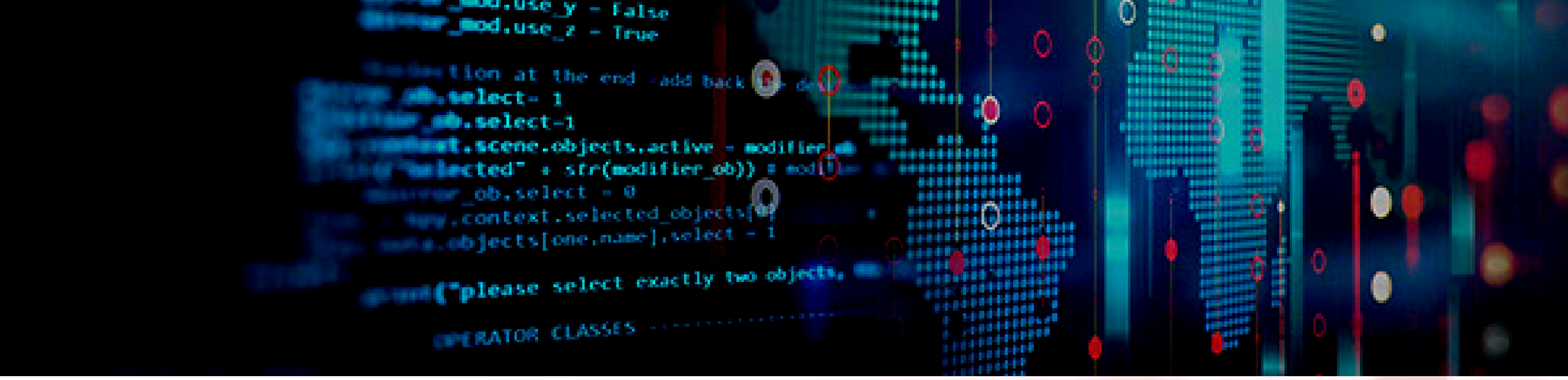
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Wrap-Up
* AWS Graviton Processor Support on Insight Agent
* 2023 Cybersecurity Industry Predictions
* About Anomalous Data Transfer detection in InsightIDR
* CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED)
* ISO 27001 Certification: What it is and why it matters
* Get your head in the cloud(s)
* Leaked Android Platform Certificates Create Risks for Users
* Metasploit Weekly Wrap-Up
* Velociraptor Version 0.6.7: Better Offline Collection, Encryption, and an Improved NTFS Parser Dig De



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Advisory for IP Phone 7800 and 8800 Series
* CISA Releases Phishing Infographic
* CISA Releases Three Industrial Control Advisories
* CISA Adds One Known Exploited Vulnerability to Catalog
* #StopRansomware: Cuba Ransomware
* CISA Releases Three Industrial Control Systems Advisories
* CISA Releases Seven Industrial Control Systems Advisories
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of November 28, 2022
* Vulnerability Summary for the Week of November 21, 2022

Zero Day Initiative Advisories

ZDI-CAN-19746: Western Digital
A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19678: Western Digital
A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19604: Synology
A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19744: Synology
A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19743: Synology
A CVSS score 4.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor

on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19741: Synology

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19708: Synology

A CVSS score 7.5 (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19742: Synology

A CVSS score 5.7 (AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19191: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19192: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19188: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-18935: Microsoft

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 'insu of 78ResearchLab' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19648: SolarWinds

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 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19107: VBASE

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19530: X.Org

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 'Jan-Niklas

Sohn' was reported to the affected vendor on: 2022-12-02, 10 days ago. The vendor is given until 2023-04-01 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-19621: Adobe

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19620: Adobe

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19606: Adobe

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19516: Adobe

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: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19515: Adobe

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: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19617: Adobe

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19517: Adobe

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: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19605: Adobe

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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-19406: Delta Electronics

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 'Anonymous' was reported to the affected vendor on: 2022-11-30, 12 days ago. The vendor is given until 2023-03-30 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 2022-8889-01

Red Hat Security Advisory 2022-8889-01 - This is an Openshift Logging bug fix release. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5770-1

Ubuntu Security Notice 5770-1 - Todd Eisenberger discovered that certain versions of GNU Compiler Collection could be made to clobber the status flag of RDRAND and RDSEED with specially crafted input. This could potentially lead to less randomness in random number generation.

Ubuntu Security Notice USN-5769-1

Ubuntu Security Notice 5769-1 - It was discovered that protobuf did not properly manage memory when serializing large messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that protobuf did not properly manage memory when parsing specifically crafted messages. An attacker could possibly use this issue to cause applications using protobuf to crash, resulting in a denial of service.

Red Hat Security Advisory 2022-8902-01

Red Hat Security Advisory 2022-8902-01 - This release of Camel for Spring Boot 3.18.3 serves as a replacement for Camel for Spring Boot 3.14.2 and includes bug fixes and enhancements, which are documented in the Release Notes document linked in the References. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-8897-01

Red Hat Security Advisory 2022-8897-01 - An update for instack-undercloud is now available for Red Hat OpenStack Platform 13 (Queens).

Red Hat Security Advisory 2022-8896-01

Red Hat Security Advisory 2022-8896-01 - A virtual BMC for controlling virtual machines using IPMI commands.

Red Hat Security Advisory 2022-8900-01

Red Hat Security Advisory 2022-8900-01 - The grub2 packages provide version 2 of the Grand Unified Boot Loader, a highly configurable and customizable boot loader with modular architecture. The packages support a variety of kernel formats, file systems, computer architectures, and hardware devices.

Red Hat Security Advisory 2022-8840-01

Red Hat Security Advisory 2022-8840-01 - Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience. This release of Red Hat JBoss Core Services Apache HTTP Server 2.4.51 Service Pack 1 serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.51, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include buffer overflow, bypass, code execution, denial of service, double free, and out of bounds read vulnerabilities.

Red Hat Security Advisory 2022-8841-01

Red Hat Security Advisory 2022-8841-01 - Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience. This release of Red Hat JBoss Core Services Apache HTTP Server 2.4.51 Service Pack 1 serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.51, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include buffer over-read, buffer overflow, bypass, code execution, denial of service, double free, integer overflow, out of bounds read, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5767-1

Ubuntu Security Notice 5767-1 - Nicky Mouha discovered that Python incorrectly handled certain SHA-3 internals. An attacker could possibly use this issue to cause a crash or execute arbitrary code. It was discovered that Python incorrectly handled certain IDNA inputs. An attacker could possibly use this issue to expose sensitive information denial of service, or cause a crash.

Ubuntu Security Notice USN-5768-1

Ubuntu Security Notice 5768-1 - Jan Engelhardt, Tavis Ormandy, and others discovered that the GNU C Library iconv feature incorrectly handled certain input sequences. An attacker could possibly use this issue to cause the GNU C Library to hang or crash, resulting in a denial of service. It was discovered that the GNU C Library did not properly handled DNS responses when ENDS0 is enabled. An attacker could possibly use this issue to cause fragmentation-based attacks.

Red Hat Security Advisory 2022-8781-01

Red Hat Security Advisory 2022-8781-01 - Logging Subsystem for Red Hat OpenShift has a security update. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-8849-01

Red Hat Security Advisory 2022-8849-01 - An update for python-XStatic-Angular is now available for Red Hat OpenStack Platform 16.2.4 (Train).

Red Hat Security Advisory 2022-8852-01

Red Hat Security Advisory 2022-8852-01 - A fast multidimensional array facility for Python. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2022-8874-01

Red Hat Security Advisory 2022-8874-01 - An update for openstack-barbican is now available for Red Hat OpenStack Platform 16.1.9 (Train) for Red Hat Enterprise Linux (RHEL) 8.2.

Red Hat Security Advisory 2022-8857-01

Red Hat Security Advisory 2022-8857-01 - Erlang is a general-purpose programming language and runtime environment. Erlang has built-in support for concurrency, distribution and fault tolerance. Erlang is used in several large telecommunication systems from Ericsson. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-8873-01

Red Hat Security Advisory 2022-8873-01 - An update for python-oslo-utils is now available for Red Hat OpenStack Platform 16.1.9 (Train) for Red Hat Enterprise Linux (RHEL) 8.2.

Red Hat Security Advisory 2022-8866-01

Red Hat Security Advisory 2022-8866-01 - An update for python-XStatic-Angular is now available for Red Hat OpenStack Platform 16.1.9 (Train) for Red Hat Enterprise Linux (RHEL) 8.2.

Red Hat Security Advisory 2022-8848-01

Red Hat Security Advisory 2022-8848-01 - An update for python-XStatic-Bootstrap-SCSS is now available for Red Hat OpenStack Platform 16.2.4 (Train). Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2022-8865-01

Red Hat Security Advisory 2022-8865-01 - An update for python-XStatic-Bootstrap-SCSS is now available for Red Hat OpenStack Platform 16.1.9 (Train) for Red Hat Enterprise Linux (RHEL) 8.2. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2022-8864-01

Red Hat Security Advisory 2022-8864-01 - UltraJSON is an ultra fast JSON encoder and decoder. Issues addressed include a double free vulnerability.

Red Hat Security Advisory 2022-8851-01

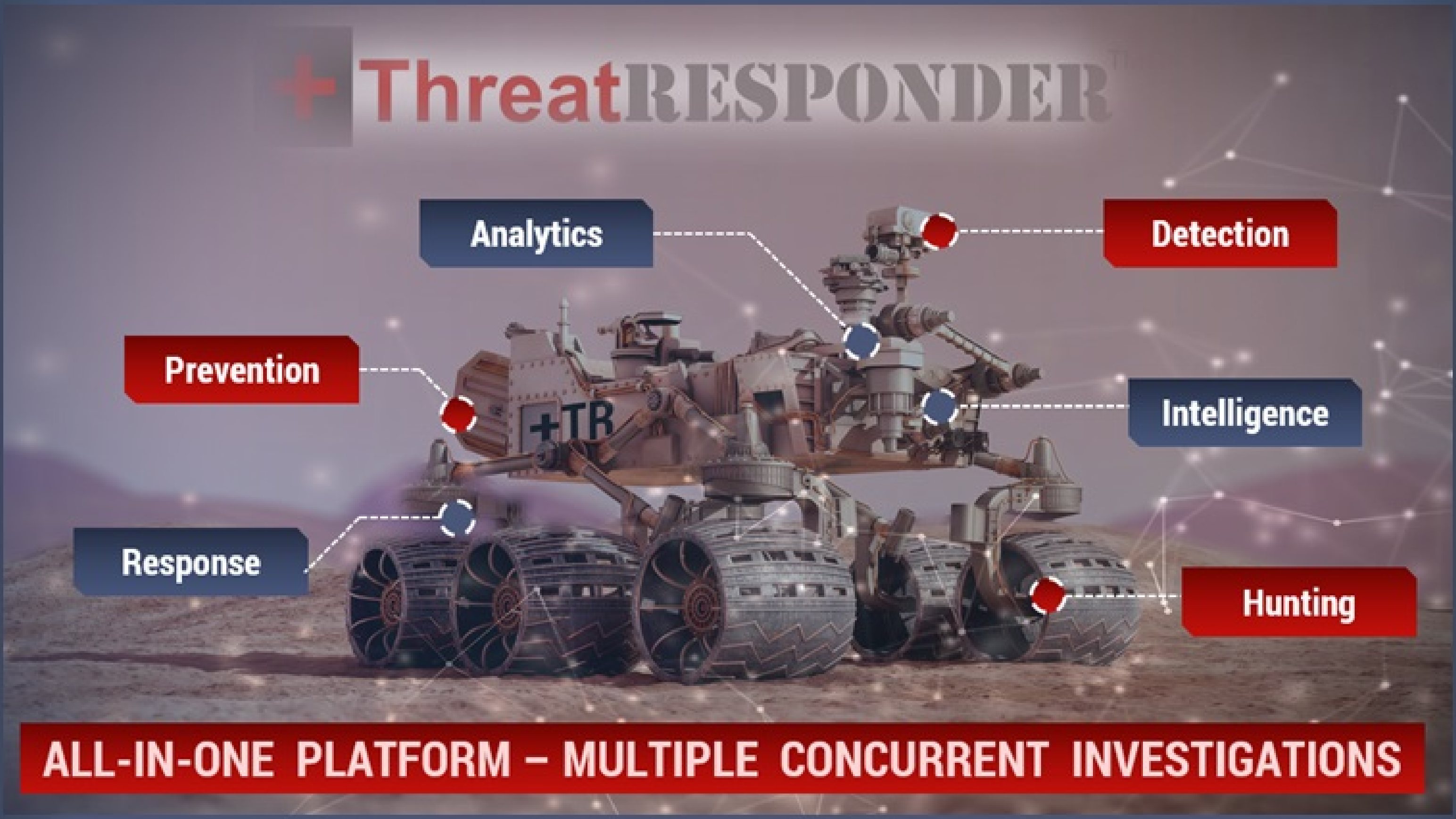
Red Hat Security Advisory 2022-8851-01 - An update for rabbitmq-server is now available for Red Hat OpenStack Platform 16.2.4 (Train) for Red Hat Enterprise Linux (RHEL) 8.4. Issues addressed include cross site scripting and improper neutralization vulnerabilities.

Red Hat Security Advisory 2022-8862-01

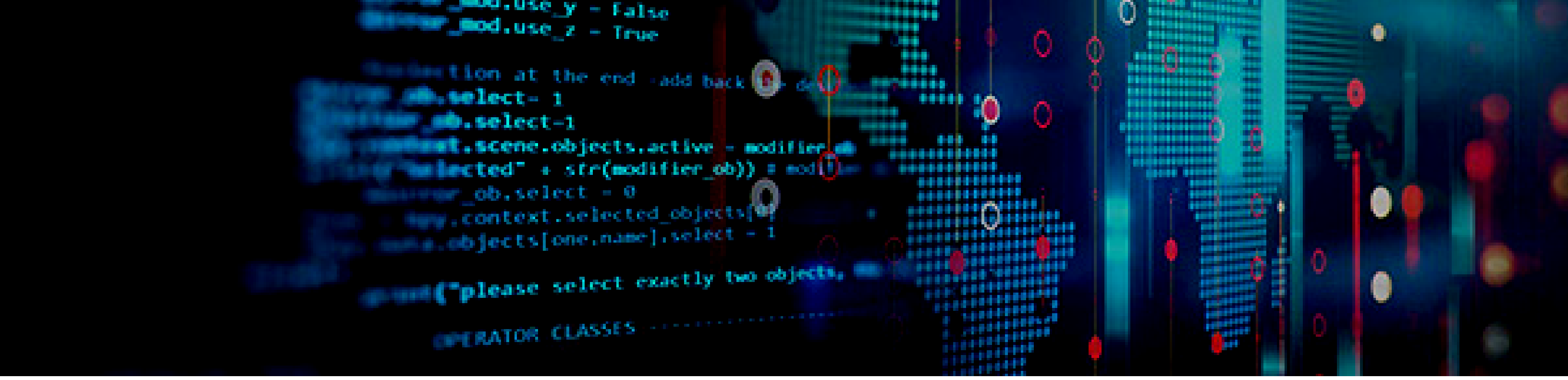
Red Hat Security Advisory 2022-8862-01 - An update for puppet is now available for Red Hat OpenStack Platform 16.1.9 (Train) for Red Hat Enterprise Linux (RHEL) 8.2.

Red Hat Security Advisory 2022-8853-01

Red Hat Security Advisory 2022-8853-01 - An update for python-django20 is now available for Red Hat OpenStack Platform 16.2.4 (Train) for Red Hat Enterprise Linux (RHEL) 8.4. Issues addressed include cross site scripting and denial of service vulnerabilities.



+ThreatRESPONDER
Analytics
Detection
Prevention
+TR
Intelligence
Response
Hunting
ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

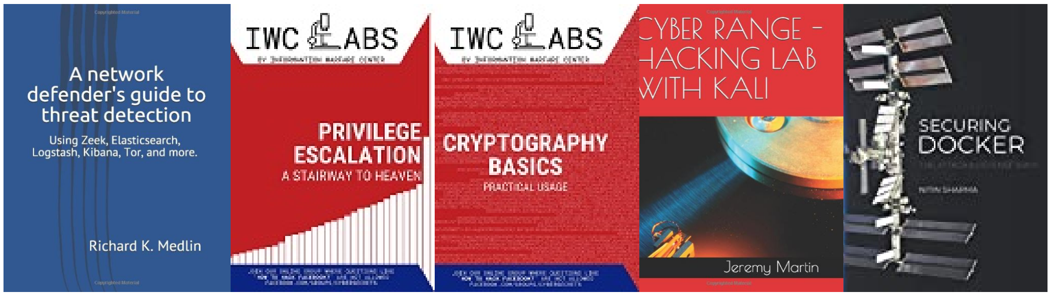


The Cyber Secrets publications on Amazon

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