Apr-24-23

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®

April 24, 2023

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

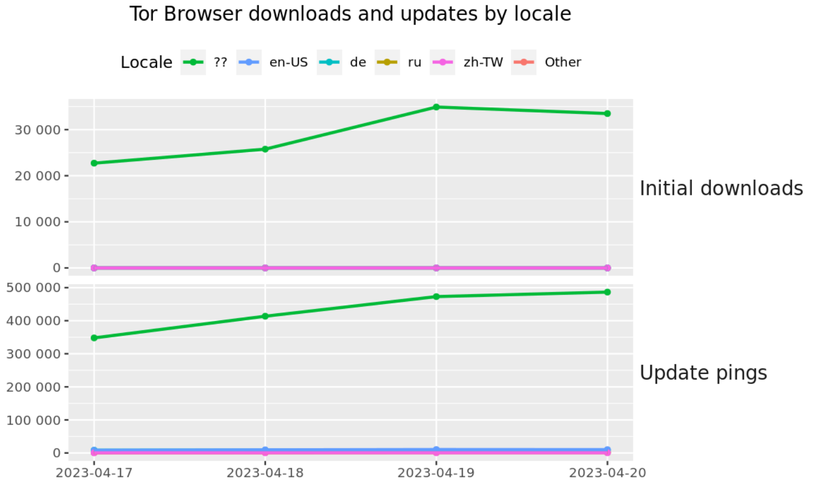
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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

* If You Haven't Patched Microsoft Process Explorer, Prepare To Get Pwned
* GhostToken Vuln Could Permanently Expose Data Of Google Users
* Pro-Russian Hackers Target European Air Traffic Control
* Capita Admits Data Stolen During Cyberattack
* APT Mint Sandstorm Quickly Exploits New PoC Hacks
* WhatsApp Used In BEC Scam To Pilfer $6.4M
* DHS Announces AI Task Force, Security Sprint On China Related Threats
* China Building Cyberweapons To Hijack Enemy Satellites, Says US Leak
* Crime Agencies Condemn Meta's Encryption Plans
* Another Supply Chain Attack Discovered During 3CX Investigation
* Experts Warn Patching Won't Protect Critical Infrastructure Against New Age Malware
* Criminal Records Service Still Disrupted 4 Weeks After Hack
* Russian Snoops Just Love Invading Unpatched Cisco Gear, America And UK Warn
* Four Charged With Pushing Pro-Kremlin Disinfo, Election Interference
* NSO Group Escalates Spyware Tactics With 3 New iPhone Zero-Click Exploit Chains
* Hikvision Denies Leaked Pentagon Spy Claim
* New Lockbit Variant Targets MacOS, Another Relies On Conti Source Code
* The Car Thieves Using Tech Disguised Inside Of Old Nokia Phones And Bluetooth Speakers
* Chrome, Edge Browsers Targeted In Zaraza Bot Malware Attacks
* Zero Day In Google Chrome Patched: Bug Exploited In The Wild
* Linux Kernel Logic Allowed Spectre Attack On Major Cloud Provider
* Ether Jumps To 11-Month High In Wake Of Software Upgrade
* Inside Look At Cybercriminal Organizations
* LinkedIn Deploys New Secure Identity Verification For All Members
* Free Public Charging Stations May Come With A Price, Federal Agencies Warn

Krebs on Security

* 3CX Breach Was a Double Supply Chain Compromise
* Giving a Face to the Malware Proxy Service 'Faceless'
* Why is 'Juice Jacking' Suddenly Back in the News?
* Microsoft (& Apple) Patch Tuesday, April 2023 Edition
* FBI Seizes Bot Shop 'Genesis Market' Amid Arrests Targeting Operators, Suppliers
* A Serial Tech Investment Scammer Takes Up Coding?
* German Police Raid DDoS-Friendly Host 'FlyHosting'
* UK Sets Up Fake Booter Sites To Muddy DDoS Market
* Google Suspends Chinese E-Commerce App Pinduoduo Over Malware
* Why You Should Opt Out of Sharing Data With Your Mobile Provider

LATEST NEWS

Dark Reading

* Millions of Artifacts, Misconfigured Enterprise Software Registries Are Ripe for Pwning
* Tangled Up: 'Tomiris' APT Uses Turla Malware, Confusing Researchers
* Google Workspace Extends Enterprise-Grade Security and Device Management for Hybrid Work With Okta an
* Bot Management Aims to Tame Attacker Automation
* Critical Infrastructure Organizations Further Affected in 3CX Breach
* Are Low-Code Apps a Ticking Access Control Time-Bomb?
* North Korean Foreign Trade Bank Representative Charged in Crypto Laundering Conspiracies
* Google Cloud Announces New Security AI Workbench and Ecosystem Expansion at RSAC 2023
* Qwiet AI Builds a Neural Net to Catch Coding Vulnerabilities
* ZeroFox to Acquire LookingGlass, Broadening Global Attack Surface Intelligence Capabilities
* Cisco Unveils Solution to Rapidly Detect Advanced Cyber Threats and Automate Response
* Cybersecurity Survival: Hide From Adversarial AI
* The New Frontier in Email Security: Goodbye, Gateways; Hello, Behavioral AI
* Zimperium Launches Unified Mobile Security Platform for Threat Detection, Visibility, and Response
* Rethinking Safer AI: Can There Really Be a 'TruthGPT'?
* Palo Alto Networks Takes Aim At Cyberattacks With the Expansion of Unit 42's Digital Forensics & Inci
* CrowdStrike Introduces CrowdStream to Accelerate and Simplify XDR Adoption
* Shields Health Breach Exposes 2.3M Users' Data
* North Korea's Kimsuky APT Keeps Growing, Despite Public Outing
* 'EvilExtractor' All-in-One Stealer Campaign Targets Windows User Data

The Hacker News

* Russian Hackers Tomiris Targeting Central Asia for Intelligence Gathering
* Ransomware Hackers Using AuKill Tool to Disable EDR Software Using BYOVD Attack
* Study: 84% of Companies Use Breached SaaS Applications - Here's How to Fix it for Free!
* Hackers Exploit Outdated WordPress Plugin to Backdoor Thousands of WordPress Sites
* New All-in-One "EvilExtractor" Stealer for Windows Systems Surfaces on the Dark Web
* Russian Hackers Suspected in Ongoing Exploitation of Unpatched PaperCut Servers
* Lazarus X_TRADER Hack Impacts Critical Infrastructure Beyond 3CX Breach
* CISA Adds 3 Actively Exploited Flaws to KEV Catalog, including Critical PaperCut Bug
* Kubernetes RBAC Exploited in Large-Scale Campaign for Cryptocurrency Mining
* GhostToken Flaw Could Let Attackers Hide Malicious Apps in Google Cloud Platform
* 14 Kubernetes and Cloud Security Challenges and How to Solve Them
* N.K. Hackers Employ Matryoshka Doll-Style Cascading Supply Chain Attack on 3CX
* Cisco and VMware Release Security Updates to Patch Critical Flaws in their Products
* Two Critical Flaws Found in Alibaba Cloud's PostgreSQL Databases
* Beyond Traditional Security: NDR's Pivotal Role in Safeguarding OT Networks

LATEST NEWS

Security Week

* Investors Place Early $4 Million Bet on Stack Identity
* Adrian Stone Joins Moderna as CISO
* Huntress: Most PaperCut Installations Not Patched Against Already-Exploited Security Flaw
* New Data Sharing Platform Serves as Early Warning System for OT Security Threats
* North Korean Hackers Target Mac Users With New 'RustBucket' Malware
* Attackers Abuse Kubernetes RBAC to Deploy Persistent Backdoor
* Critical Flaw in Inea ICS Product Exposes Industrial Organizations to Remote Attacks
* SolarWinds Platform Update Patches High-Severity Vulnerabilities
* External Signs of Narcissism - Raising Awareness to Avoid Collateral Damage
* 38 Countries Take Part in NATO's 2023 Locked Shields Cyber Exercise

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Another Perspective on ChatGPT's Social Engineering Potential
* [Heads Up] The New FedNow Service Opens Massive New Attack Surface
* FBI Warns of Sextortion Scams that Yield a New Equally Scam-Like Service: Sextortion Assistance
* Phishing for Credentials in Social Media-Based Platform Linktree
* More Companies with Cyber Insurance Are Hit by Ransomware Than Those Without
* OpenAI Transparency Report Highlights How GPT-4 Can be Used to Aid Both Sides of the Cybersecurity Ba
* Nearly One-Half of IT Pros are Told to Keep Quiet About Security Breaches
* Phishing Email Volume Doubles in Q1 as the use of Malware in Attacks Slightly Declines
* Guarding Against AI-Enabled Social Engineering: Lessons from a Data Scientist's Experiment
* That Email Isn't from the New Jersey Attorney General

ISC2.org Blog

Unfortunately, at the time of this report, the ISC2 Blog resource was not availible.

HackRead

* Preventing Malware & Cyber Attacks: Simple Tips for Your Computer
* Goldoson Android Malware Found in 60 Apps with 100M Downloads
* BlackCat (ALPHV) Gang Claims Ransomware Attack on NCR Data Center
* LockBit Ransomware Expands Attack Spectrum to Mac Devices
* QuaDream, Israeli iPhone hacking spyware firm, to shut down
* Are Smart Home Devices Invading Your Privacy?
* 10 Best Zippyshare Alternatives - Best File Sharing Services

Koddos

* Preventing Malware & Cyber Attacks: Simple Tips for Your Computer
* Goldoson Android Malware Found in 60 Apps with 100M Downloads
* BlackCat (ALPHV) Gang Claims Ransomware Attack on NCR Data Center
* LockBit Ransomware Expands Attack Spectrum to Mac Devices
* QuaDream, Israeli iPhone hacking spyware firm, to shut down
* Are Smart Home Devices Invading Your Privacy?
* 10 Best Zippyshare Alternatives - Best File Sharing Services

LATEST NEWS

Naked Security

* Double zero-day in Chrome and Edge - check your versions now!
* VMware patches break-and-enter hole in logging tools: update now!
* S3 Ep131: Can you really have fun with FORTRAN?
* Ex-CEO of breached pyschotherapy clinic gets prison sentence for bad data security
* FBI and FCC warn about "Juicejacking" - but just how useful is their advice?
* S3 Ep130: Open the garage bay doors, HAL [Audio + Text]
* Patch Tuesday: Microsoft fixes a zero-day, and two curious bugs that take the Secure out of Secure Bo
* Attention gamers! Motherboard maker MSI admits to breach, issues "rogue firmware" alert
* Apple zero-day spyware patches extended to cover older Macs, iPhones and iPads
* Popular server-side JavaScript security sandbox "vm2" patches remote execution hole

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

* How Cyber Insurance Changed Cybersecurity
* The Needs of a Modernized SOC for Hybrid Cloud
* How the Talent Shortage Impacts Cybersecurity Leadership
* What's in Your Policy: Insurance Markets and Nation State Cyberattacks
* Triple Extortion and Erased Data are the New Ransomware Norm
* Security at the Masters
* The Importance of Accessible and Inclusive Cybersecurity
* Secure-by-Design: A 2023 Cybersecurity Prime
* Securing Your Remote Workforce: How to Reduce Cyber Threats
* Embracing Automation to Unlock New Innovations

InfoWorld

* BrandPost: Unlocking the power of real-time analytics: 5 key considerations
* BrandPost: Speeding Up Geographic Commands in Redis 7
* BrandPost: Optimizing Redis' Default Compiler Flags
* BrandPost: Intel Cloud Optimizer + Intel Optimization Hub revolutionize the cloud
* BrandPost: Direct Data Accelerator: The F1 that powers Yellowbrick's Cloud Data Warehouse
* BrandPost: How Pure Storage and Intel are reducing the energy cost and environmental impact of big da
* BrandPost: Palo Alto Networks automates cybersecurity with machine learning
* BrandPost: Accelerating edge cloud services and real-time digital experiences with Lightbits and Inte
* BrandPost: SORAVIA accelerates acquisition strategy by leveraging Google Cloud, Workspot, Intel, and
* BrandPost: Introducing DigitalOcean Premium CPU-Optimized Droplets for reliable performance & higher

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

* 5 Things That Make The DEF CON Experience Special
* The 5 Most Controversial DEF CON Talks Of All Time
* 6 Notable DEF CON Moments
* Best AI Conferences To Attend in 2023
* How To Organize A Conference? Here's How To Get It Right!
* 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

Google Zero Day Project

* Release of a Technical Report into Intel Trust Domain Extensions
* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems

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.

* TAMUctf 2023
* D^3CTF 2023
* CrewCTF 2023
* RPCA CTF 2023
* UMDCTF 2023
* Punk Security DevSecOps Birthday CTF
* San Diego CTF 2023
* PwnMe Qualifications : "8 bits"
* DeadSec CTF 2023
* BSides Algiers 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

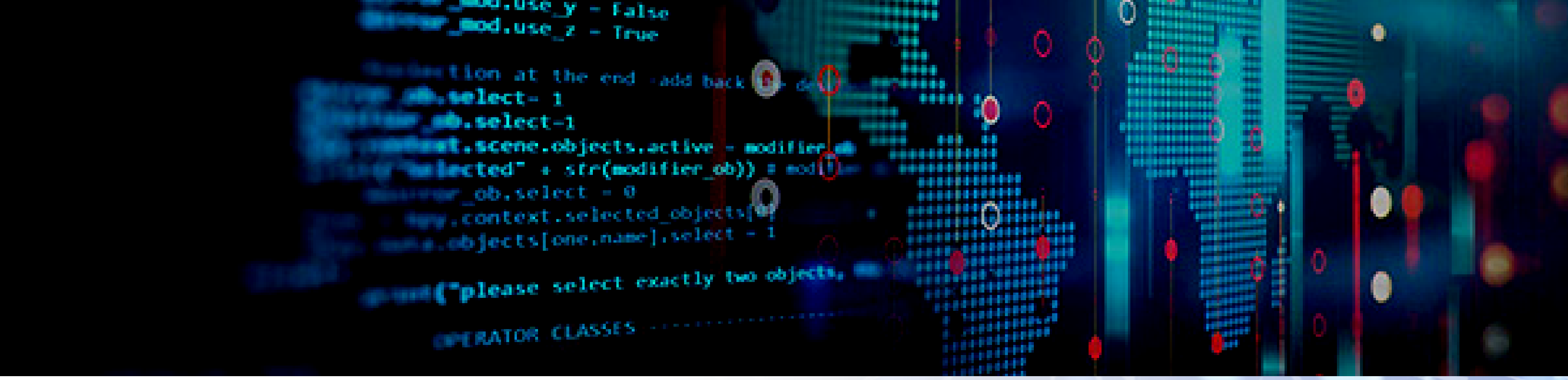
* FortiGate Brute Forcer
* American Fuzzy Lop plus plus 4.06c
* I2P 2.2.1
* Suricata IDPE 6.0.11
* Wireshark Analyzer 4.0.5
* Faraday 4.3.5
* Zeek 5.0.8
* Faraday 4.3.4
* tcpdump 4.99.4
* AIDE 0.18.2

Kali Linux Tutorials

* Decider : Process Of Mapping Adversary Behaviors To The MITRE ATT&CK Framework
* ThunderCloud : Cloud Exploit Framework
* Waf-Bypass : Check Your WAF Before An Attacker Does
* How to Secure your Browsers from Malicious Extensions?
* QRExfiltrate : Tool To Convert Any Binary File Into A QRcode Movie
* HackTools - All-in-one Red Team Browser Extension For Web Pentesters
* APCLdr : Payload Loader With Evasion Features
* PortexAnalyzerGUI : Graphical Interface For PortEx
* XSS Automation - Tool to Identify and Exploit cross-site scripting (XSS) Vulnerabilities
* Invoke-PSObfuscation : An In-Depth Approach To Obfuscating the PowerShell Payload On Windows Or Kali

GBHackers Analysis

* Accidental 'write' Permissions In Alibaba PostgreSQL Let Attackers Access Sensitive Data
* Ex-Conti and FIN7 Hackers Team Up To Develop Domino Backdoor Malware
* ChatGPT Account Takeover Bug Allows Hackers To Gain User's Online Account
* Used Routers Fully Loaded With Corporate Secrets for Just $100
* Hackers Storing Malware in Google Drive as Encrypted ZIP Files To Evade Detection



Weekly Cyber Security Video and Podcasts

SANS DFIR

* FOR498 - New Course Name, New Content & A Whole Lot of Actionable Intelligence in 90 min or less
* Cloud-Powered DFIR: Harnessing the cloud to improve investigator efficiency
* Breaking the Ransomware Tool Set: When a Threat Actor Opsec
* The Way to a Stakeholder's Heart is by Providing Value: Measuring Success of Your CTI Program

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

* The RESTRICT Act: TLDR? Watch This - ThreatWire
* Should AI Training Be Paused? - ThreatWire
* Cerebral App Leaks Telehealth Medical Data - ThreatWire

The PC Security Channel [TPSC]

* Network Security Tools to stop hackers
* 3CX: How this malware almost hacked every business

Eli the Computer Guy

* CHATGPT API and PYTHON - Hands on Class
* TKINTER INTRO - GUI APPS IN PYTHON - Hands on Class
* PYTHON INTRO - Hands on Class
* CHATGPT INTRO - Silicon Dojo Seminar

Security Now

* Forced Entry - Patch Tuesday, Google Assured Open Source Software, WhatsApp Improvements
* A Dangerous Interpretation - H26FORGE, Privatized ChatGPT, Mozilla Site Breach Monitor

Troy Hunt

* Weekly Update 344

Intel Techniques: The Privacy, Security, & OSINT Show

* 294-Preparing for Home Disaster
* 293-Financial Software Considerations

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Telit Cinterion IoT Traversal / Escalation / Bypass / Heap Overflow
* Multi-Vendor Online Groceries Management System 1.0 Remote Code Execution
* Chitor CMS 1.1.2 SQL Injection
* Nokia OneNDS 20.9 Insecure Permissions / Privilege Escalation
* Nokia OneNDS 17 Insecure Permissions / Privilege Escalation
* KODExplorer 4.49 Cross Site Request Forgery / Shell Upload
* Chrome SpvGetMappedSamplerName Out-Of-Bounds String Copy
* Chrome GL_ShaderBinary Untrusted Process Exposure
* Chrome media::mojom::VideoFrame Missing Validation
* FUXA 1.1.13-1186 Remote Code Execution
* Chitor-CMS 1.1.2 SQL Injection
* ProjeQtOr Project Management System 10.3.2 Shell Upload
* Piwigo 13.6.0 Cross Site Scripting
* Franklin Fueling Systems TS-550 Hash Disclosure / Default Credentials
* Swagger UI 4.1.3 Critical Information Misrepresentation
* Lilac-Reloaded For Nagios 2.0.8 Remote Code Execution
* Serendipity 2.4.0 Cross Site Scripting
* Serendipity 2.4.0 Shell Upload
* VMware Workspace ONE Access Privilege Escalation
* SecurePoint UTM 12.x Memory Leak
* SecurePoint UTM 12.x Session ID Leak
* SPIP Remote Command Execution
* VMware Workspace ONE Remote Code Execution
* WordPress Weaver Xtreme 5.0.7 / Weaver Show Posts 1.6 Cross Site Scripting
* CentOS Stream 9 Missing Kernel Security Fix

CXSecurity

* Lilac-Reloaded For Nagios 2.0.8 Remote Code Execution
* Chitor-CMS 1.1.2 SQL Injection
* Mware Workspace ONE Remote Code Execution
* Rocket Software Unidata 8.2.4 Build 3003 Buffer Overflow
* pfsenseCE 2.6.0 Protection Bypass
* pdfkit v0.8.7.2 Command Injection
* Kimai-1.30.10 SameSite Cookie-Vulnerability session hijacking

Proof of Concept (PoC) & Exploits

Exploit Database

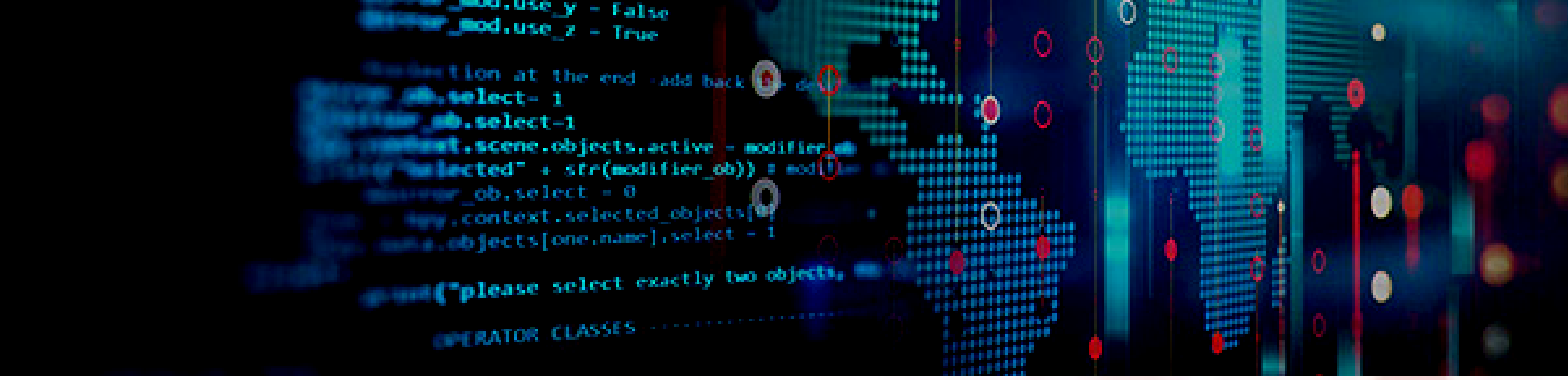
* [webapps] ProjeQtOr Project Management System 10.3.2 - Remote Code Execution (RCE)
* [webapps] Piwigo 13.6.0 - Stored Cross-Site Scripting (XSS)
* [webapps] FUXA V.1.1.13-1186 - Unauthenticated Remote Code Execution (RCE)
* [local] Linux Kernel 6.2 - Userspace Processes To Enable Mitigation
* [webapps] Chitor-CMS v1.1.2 - Pre-Auth SQL Injection
* [remote] Franklin Fueling Systems TS-550 - Default Password
* [webapps] GDidees CMS 3.9.1 - Local File Disclosure
* [local] AspEmail v5.6.0.2 - Local Privilege Escalation
* [webapps] Swagger UI 4.1.3 - User Interface (UI) Misrepresentation of Critical Information
* [webapps] Bang Resto v1.0 - 'Multiple' SQL Injection
* [webapps] Bang Resto v1.0 - Stored Cross-Site Scripting (XSS)
* [remote] Microsoft Word 16.72.23040900 - Remote Code Execution (RCE)
* [local] File Replication Pro 7.5.0 - Privilege Escalation/Password reset due Incorrect Access Control
* [webapps] Lilac-Reloaded for Nagios 2.0.8 - Remote Code Execution (RCE)
* [webapps] Serendipity 2.4.0 - Cross-Site Scripting (XSS)
* [webapps] Serendipity 2.4.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Sielco PolyEco Digital FM Transmitter 2.0.6 - Account Takeover / Lockout / EoP
* [webapps] Sielco PolyEco Digital FM Transmitter 2.0.6 - Unauthenticated Information Disclosure
* [webapps] Sielco PolyEco Digital FM Transmitter 2.0.6 - Radio Data System POST Manipulation
* [webapps] Sielco PolyEco Digital FM Transmitter 2.0.6 - Authorization Bypass Factory Reset
* [webapps] Sielco PolyEco Digital FM Transmitter 2.0.6 - Authentication Bypass Exploit
* [remote] Sielco Analog FM Transmitter 2.12 - Remote Privilege Escalation
* [webapps] Sielco Analog FM Transmitter 2.12 - Improper Access Control Change Admin Password
* [webapps] Sielco Analog FM Transmitter 2.12 - Cross-Site Request Forgery
* [webapps] Sielco Analog FM Transmitter 2.12 - 'id' Cookie Brute Force Session Hijacking

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
```

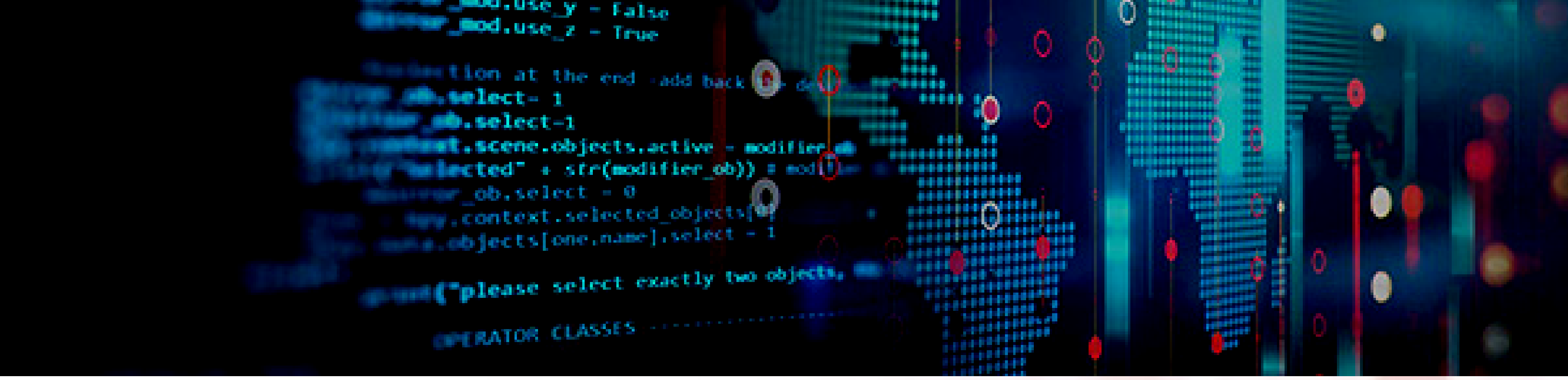
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://indetur.gov.co/nob.php
http://indetur.gov.co/nob.php notified by CapoO_TunisiAnoO
http://www.koisoong.go.th
http://www.koisoong.go.th notified by Ajoyy
http://www.namkrai.go.th
http://www.namkrai.go.th notified by Ajoyy
https://imojudiciary.gov.ng/s3cbugs.htm
https://imojudiciary.gov.ng/s3cbugs.htm notified by s3cbugs.com
https://fctmuslimpilgrims.gov.ng/kurd.html
https://fctmuslimpilgrims.gov.ng/kurd.html notified by 0x1998
https://www.gocp.gov.eg
https://www.gocp.gov.eg notified by shenzyy
https://www.pa-batang.go.id/el.htm
https://www.pa-batang.go.id/el.htm notified by ./An9el4-137
https://bappeda.rokanhulukab.go.id
https://bappeda.rokanhulukab.go.id notified by Boss Ranzen
https://oas.tbs.go.tz/s3cbugs.html
https://oas.tbs.go.tz/s3cbugs.html notified by s3cbugs.com
https://commune-haidra.gov.tn/fake.php
https://commune-haidra.gov.tn/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://revues.univ-lemans.fr/public/site/images/1/5.gif
https://revues.univ-lemans.fr/public/site/images/1/5.gif notified by Moroccan Revolution
https://www.rasp.msal.gov.ar/public/site/images/1/5.gif
https://www.rasp.msal.gov.ar/public/site/images/1/5.gif notified by Moroccan Revolution
https://arbor.revistas.csic.es/public/site/images/1/5.gif
https://arbor.revistas.csic.es/public/site/images/1/5.gif notified by Moroccan Revolution
http://www.taladnikomprasat.go.th
http://www.taladnikomprasat.go.th notified by xNot_RespondinGx
http://ok.bkipm.kkp.go.id/nero.htm
http://ok.bkipm.kkp.go.id/nero.htm notified by Indonesia Attacker
http://dishub.kolakakab.go.id/nero.htm
http://dishub.kolakakab.go.id/nero.htm notified by Indonesia Attacker
http://dinsos.kolakakab.go.id/nero.htm
http://dinsos.kolakakab.go.id/nero.htm notified by Indonesia Attacker

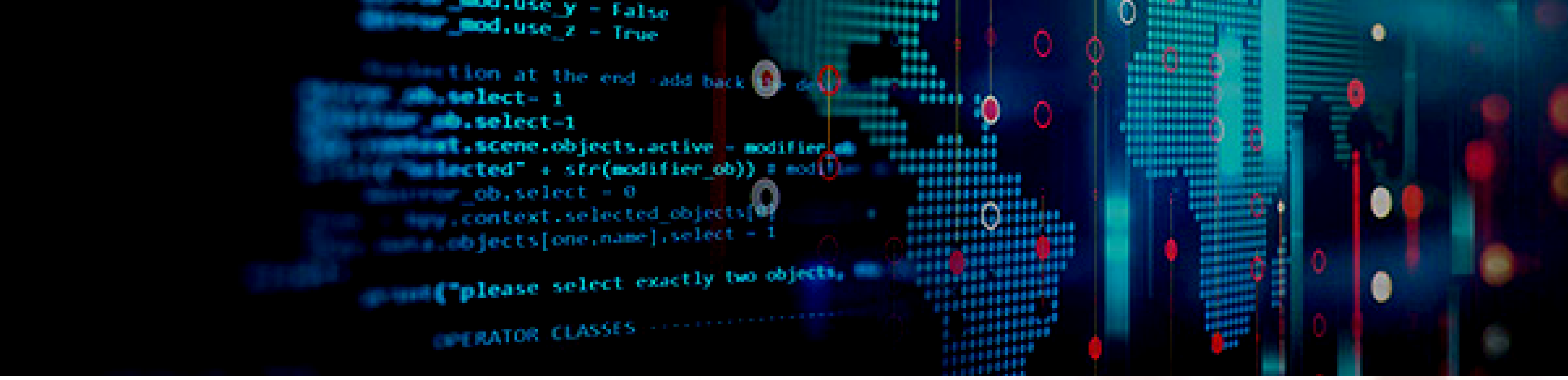


Dark Web News

Darknet Live

[Methamphetamine Vendor Sentenced to Prison]()
[The Hitchhiker's Guide to Whonix]()
[Georgia Man Imprisoned for Defrauding Silk Road]()
[Australian Vendor "Underline Cost" Jailed]()

Dark Web Link



Trend Micro Anti-Malware Blog

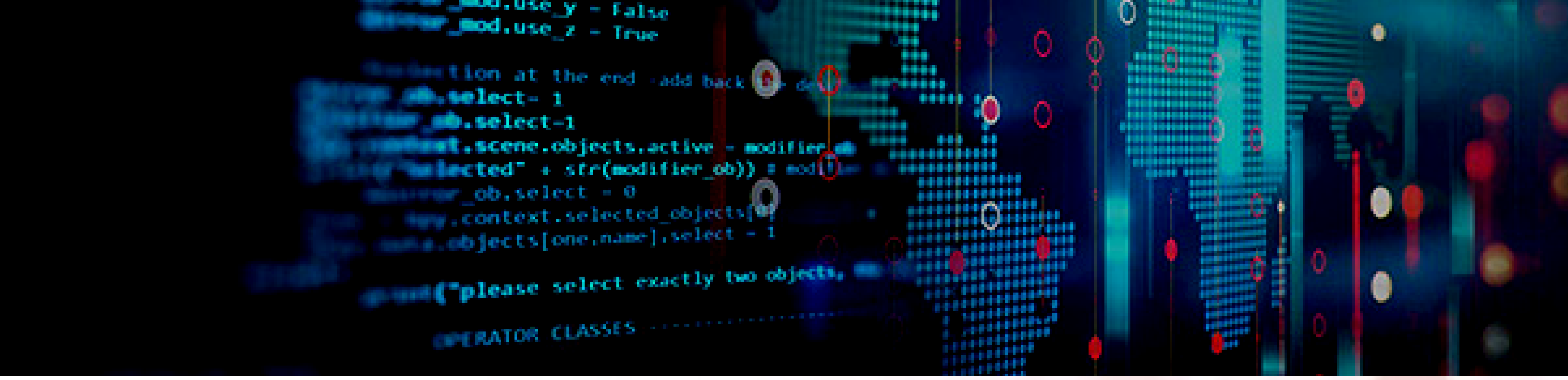
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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 Weekly Wrap-Up
* 3 Key Challenges to Clarity in Threat Intelligence: 2023 Forrester Consulting Total Economic Impact&#2013266052;
* Automating Qakbot Detection at Scale With Velociraptor
* Metasploit Weekly Wrap-Up
* Automating Qakbot decode at scale
* Anarchy in the UK? Not Quite: A look at the cyber health of the FTSE 350
* Patch Tuesday - April 2023
* 7 Rapid Questions: Lindsey Searle
* Raptor Technologies Volunteer Management Client-Side Security Controls (FIXED)
* Rapid7 Podcast Explores Hybrid-First Workplace Learnings



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Advisories for Multiple Products
* Drupal Releases Security Advisory to Address Vulnerability in Drupal Core
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* VMware Releases Security Update for Aria Operations for Logs
* CISA Releases Two SBOM Documents
* Oracle Releases Security Updates
* CISA Releases Malware Analysis Report on ICONICSTEALER
* CISA to Continue and Enhance U.K.'s Logging Made Easy Tool
* APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers
* #StopRansomware: LockBit 3.0
* Vulnerability Summary for the Week of June 17, 2019
* Vulnerability Summary for the Week of December 16, 2019

Zero Day Initiative Advisories

ZDI-CAN-20727: D-Link
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20612: VMware
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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-19823: Siemens
A CVSS score 7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Andreas Finstad' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20774: D-Link
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20778: VMware
A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on:

2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20891: PDF-XChange

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-19909: BlueZ

A CVSS score 7.1 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20729: PDF-XChange

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 'kimiya' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20730: PDF-XChange

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 'kimiya' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20295: CODESYS

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-04-13, 11 days ago. The vendor is given until 2023-08-11 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-20852: BlueZ

A CVSS score 5.4 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-07, 17 days ago. The vendor is given until 2023-08-05 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-20853: BlueZ

A CVSS score 5.4 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-07, 17 days ago. The vendor is given until 2023-08-05 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-20854: BlueZ

A CVSS score 5.4 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-07, 17 days ago. The vendor is given until 2023-08-05 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-20771: Microsoft

A CVSS score 4.4 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) & David Fiser (@anu4is) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2023-04-07, 17 days ago. The vendor is given until 2023-08-05 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-20663: PDF-XChange

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 'kimiya' was reported to the affected vendor on: 2023-04-07, 17 days ago. The vendor is given until 2023-08-05 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-20798: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20562: Ashlar-Vellum

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 'Anonymous' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20797: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20661: 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 'Mat Powell & Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20615: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20799: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20785: Delta Electronics

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 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20450: Parallels

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'war10ck' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 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-20273: Microsoft

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2023-04-06, 18 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Debian Security Advisory 5392-1

Debian Linux Security Advisory 5392-1 - Multiple security issues were discovered in Thunderbird, which could result in denial of service or the execution of arbitrary code.

Red Hat Security Advisory 2023-1931-01

Red Hat Security Advisory 2023-1931-01 - GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language, and the capability to read e-mail and news. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2023-1930-01

Red Hat Security Advisory 2023-1930-01 - GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language, and the capability to read e-mail and news. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2023-1816-01

Red Hat Security Advisory 2023-1816-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Data Foundation. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Debian Security Advisory 5391-1

Debian Linux Security Advisory 5391-1 - Several vulnerabilities were discovered in libxml2, a library providing support to read, modify and write XML and HTML files.

Ubuntu Security Notice USN-6036-1

Ubuntu Security Notice 6036-1 - It was discovered that PatchELF was not properly performing bounds checks, which could lead to an out-of-bounds read via a specially crafted file. An attacker could possibly use this issue to cause a denial of service or to expose sensitive information.

Red Hat Security Advisory 2023-1923-01

Red Hat Security Advisory 2023-1923-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6035-1

Ubuntu Security Notice 6035-1 - It was discovered that KAuth incorrectly handled some configuration parameters with specially crafted arbitrary types. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2023-1919-01

Red Hat Security Advisory 2023-1919-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2023-1916-01

Red Hat Security Advisory 2023-1916-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.

Red Hat Security Advisory 2023-1918-01

Red Hat Security Advisory 2023-1918-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2023-1915-01

Red Hat Security Advisory 2023-1915-01 - GNU Emacs is a powerful, customizable, self-documenting text editor. It provides special code editing features, a scripting language, and the capability to read e-mail and news. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-6034-1

Ubuntu Security Notice 6034-1 - It was discovered that Dnsmasq was sending large DNS messages over UDP, possibly causing transmission failures due to IP fragmentation. This update lowers the default maximum size of DNS messages to improve transmission reliability over UDP.

Red Hat Security Advisory 2023-1888-01

Red Hat Security Advisory 2023-1888-01 - Red Hat Advanced Cluster Management for Kubernetes 2.7.3 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console&mdash;with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs. Issues addressed include denial of service and server-side request forgery vulnerabilities.

Ubuntu Security Notice USN-6033-1

Ubuntu Security Notice 6033-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel did not properly perform filter deactivation in some situations. A local attacker could possibly use this to gain elevated privileges. Please note that with the fix for thisCVE, kernel support for the TCINDEX classifier has been removed. William Zhao discovered that the Traffic Control subsystem in the Linux kernel did not properly handle network packet retransmission in certain situations. A local attacker could use this to cause a denial of service.

WordPress PowerPress 10.0 Cross Site Scripting

WordPress PowerPress plugin versions 10.0 and below suffer from a persistent cross site scripting vulnerability.

Red Hat Security Advisory 2023-1899-01

Red Hat Security Advisory 2023-1899-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Ubuntu Security Notice USN-6032-1

Ubuntu Security Notice 6032-1 - Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service. Gerald Lee discovered that the USB Gadget file system implementation in the Linux kernel contained a race condition, leading to a use-after-free vulnerability in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-6031-1

Ubuntu Security Notice 6031-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the Integrity Measurement Architecture implementation in the Linux kernel did not properly enforce policy in certain conditions. A privileged attacker could use this to bypass Kernel lockdown restrictions.

Red Hat Security Advisory 2023-1893-01

Red Hat Security Advisory 2023-1893-01 - Red Hat Multicluster Engine Hotfix Security Update for Console. Red Hat Product Security has rated this update as having a security impact of Critical.

Red Hat Security Advisory 2023-1822-01

Red Hat Security Advisory 2023-1822-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Ubuntu Security Notice USN-6028-1

Ubuntu Security Notice 6028-1 - It was discovered that lixml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash.

Ubuntu Security Notice USN-6030-1

Ubuntu Security Notice 6030-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-6029-1

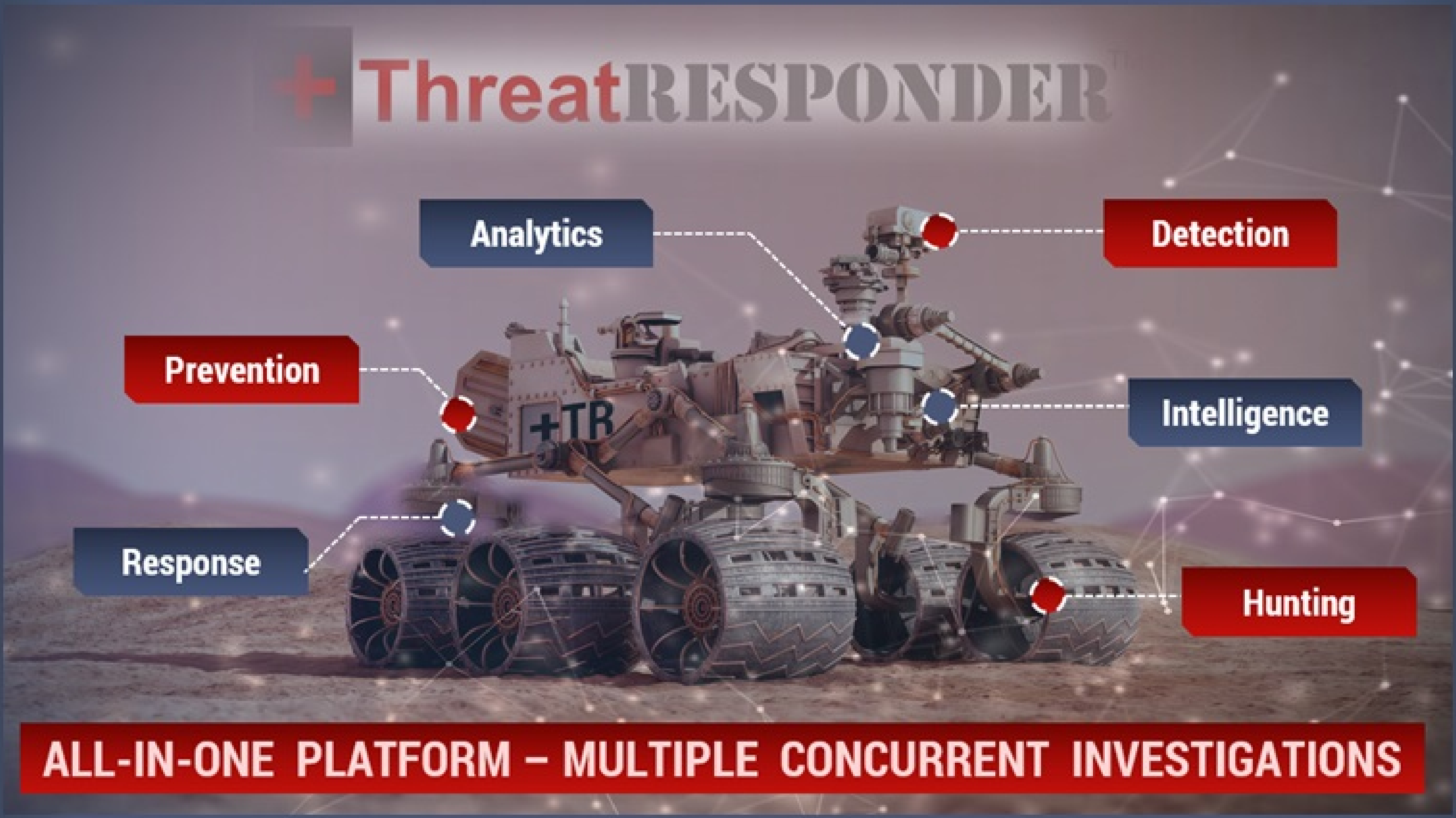
Ubuntu Security Notice 6029-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the infrared transceiver USB driver did not properly handle USB control messages. A local attacker with physical access could plug in a specially crafted USB device to cause a denial of service.

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



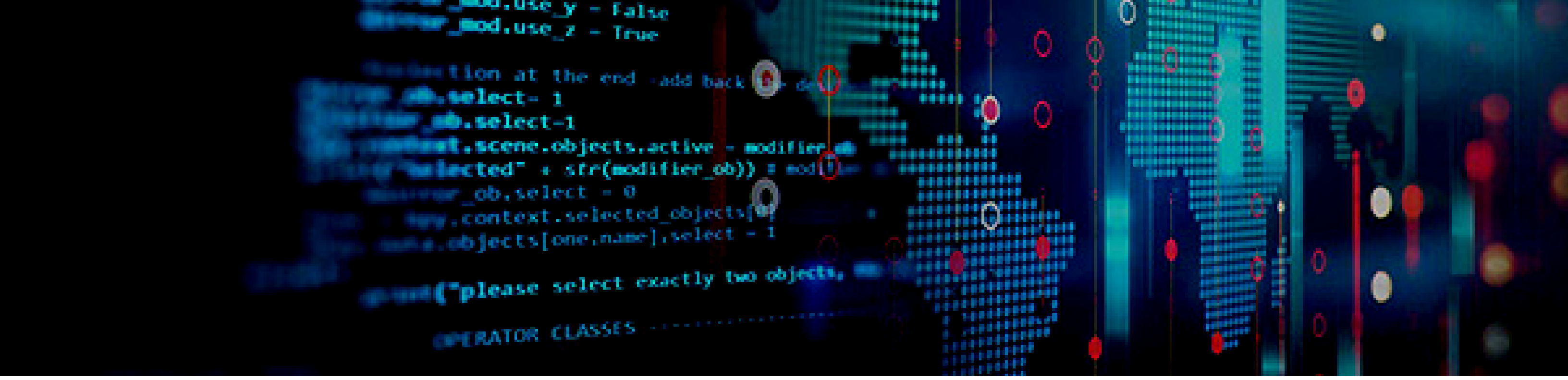
The Solution – ThreatResponder® Platform

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



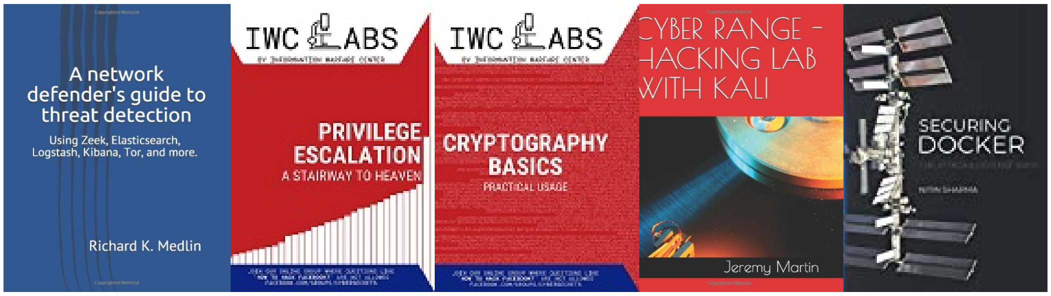
The Cyber Secrets publications on Amazon

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
What's Inside?
Threat Intelligence & Training
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
INCIDENT RESPONSE DO NOT CROSS

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