Jul-17-23

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

July 17, 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

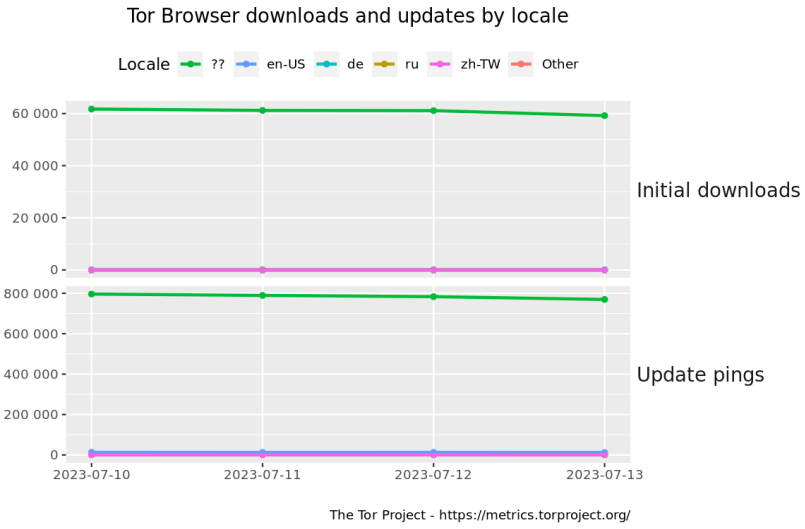
Internet Storm Center Infocon Status

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.



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

Packet Storm Security

* Fake PoC On GitHub Lures Researchers To Download Malware
* Adobe Patches Critical ColdFusion, InDesign Zero Day Bugs
* How A Cloud Flaw Gave Chinese Spies A Key To Microsoft
* Google Researchers Discover In-The-Wild Exploitation Of Zimbra Zero Day
* Juniper Networks Patches High Severity Vulnerabilities
* Microsoft Fixes 130 CVE Listed Bugs, 5 Flaws Exploited
* WordPress Security Plugin Caught Logging Plaintext Passwords
* Rockwell Automation Exploit Spurs Fears Of Critical Infrastructure Security
* Microsoft Warns Of Office Zero Day Attacks, No Patch Available
* Windows Loophole Exploited To Give Malware Kernel Access
* Coalition Presses White House To Name A New National Cyber Director
* Microsoft Warns That A Chinese Cyberattack Breached Government Email Accounts
* Privacy Activists Slam EU-US Pact On Data Sharing
* Clever Letscall Vishing Malware Targets Android Phones
* Data For 11 Million Patients Stolen In Breach Of HCA Healthcare
* Apple Releases, Quickly Pulls Rapid Security Response Update For 0-Day WebKit Bug
* Big Head Malware Threat Looms, Warn Researchers
* A Cybersecurity Wishlist Ahead Of NATO Summit
* Ex-Employee Charged For Hacking Water Treatment Facility
* Shell Confirms MOVEit-Related Breach After Ransomware Group Leaks Data
* Truebot RCE Attacks Exploit Critical Netwrix Auditor Bug
* Nickelodeon Probes Massive Data Leak As SpongeBob Fans Rejoice
* How We Found Another GitHub Action Environment Injection Vulnerability In A Google Project
* North Korean Satellite Had No Military Unit For Spying, Says South Korea
* LockBit Louts Unload At Japan's Most Prolific Cargo Port

Krebs on Security

* SEO Expert Hired and Fired By Ashley Madison Turned on Company, Promising Revenge
* Apple & Microsoft Patch Tuesday, July 2023 Edition
* Top Suspect in 2015 Ashley Madison Hack Committed Suicide in 2014
* Who's Behind the DomainNetworks Snail Mail Scam?
* Russian Cybersecurity Executive Arrested for Alleged Role in 2012 Megahacks
* U.K. Cyber Thug "PlugwalkJoe" Gets 5 Years in Prison
* SMS Phishers Harvested Phone Numbers, Shipment Data from UPS Tracking Tool
* Why Malware Crypting Services Deserve More Scrutiny
* CISA Order Highlights Persistent Risk at Network Edge
* Microsoft Patch Tuesday, June 2023 Edition

Dark Reading

* What C-Suite Leaders Need to Know About XDR
* Insider Risk Management Starts With SaaS Security
* Why CFOs & CISOs Must Collaborate to Strengthen and Protect Organizations in a Recession
* How Hackers Can Hijack a Satellite
* SBOMs Still More Mandate Than Security
* Cisco Flags Critical SD-WAN Vulnerability
* Rogue Azure AD Guests Can Steal Data via Power Apps
* Zimbra Zero-Day Demands Urgent Manual Update
* Training's New Understanding
* Electrical Grid Stability Relies on Balancing Digital Substation Security
* Brand Impersonation Scams in Middle East & Africa See Massive Growth
* White House Fills in Details of National Cybersecurity Strategy
* Secure Code Warrior Raises $50M to Accelerate Product Innovation
* Black Hat Announces Sustainability Pledge
* Secure Code Warrior Ushers in Next Era in Developer Driven Security With $50M Series C Funding Round
* Introducing EncryptionSafe: A Free and Easy-to-Use Encryption App for Windows PC
* Facebook and Microsoft are the Most Impersonated Brands in Phishing Attacks
* Safe Security Acquires RiskLens
* Linux Hacker Exploits Researchers With Fake PoCs Posted to GitHub
* Cybersecurity Leaders Report Reduction in Disruptive Cyber Incidents With MSS/MDR Solutions

The Hacker News

* Cybercriminals Exploit Microsoft Word Vulnerabilities to Deploy LokiBot Malware
* CERT-UA Uncovers Gamaredon's Rapid Data Exfiltration Tactics Following Initial Compromise
* WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks
* Microsoft Bug Allowed Hackers to Breach Over Two Dozen Organizations via Forged Azure AD Tokens
* Critical Security Flaws Uncovered in Honeywell Experion DCS and QuickBlox Services
* Defend Against Insider Threats: Join this Webinar on SaaS Security Posture Management
* AIOS WordPress Plugin Faces Backlash for Storing User Passwords in Plaintext
* TeamTNT's Cloud Credential Stealing Campaign Now Targets Azure and Google Cloud
* New SOHO Router Botnet AVrecon Spreads to 70,000 Devices Across 20 Countries
* Zimbra Warns of Critical Zero-Day Flaw in Email Software Amid Active Exploitation
* PicassoLoader Malware Used in Ongoing Attacks on Ukraine and Poland
* TeamTNT's Silentbob Botnet Infecting 196 Hosts in Cloud Attack Campaign
* Fake PoC for Linux Kernel Vulnerability on GitHub Exposes Researchers to Malware
* Rockwell Automation ControlLogix Bugs Expose Industrial Systems to Remote Attacks
* U.S. Government Agencies' Emails Compromised in China-Backed Cyber Attack

Security Week

* In Other News: Security Firm Hit by Investor Lawsuit, Satellite Hacking, Cloud Attacks
* Zluri Raises $20 Million for SaaS Management Platform
* Industry Reactions to EU-US Data Privacy Framework: Feedback Friday
* Critical Cisco SD-WAN Vulnerability Leads to Information Leaks
* Secure Code Warrior Raises $50 Million to Help Developers Write Secure Code
* Hackers Target Reddit Alternative Lemmy via Zero-Day Vulnerability
* US Publishes Implementation Plan for National Cybersecurity Strategy
* Google Researchers Discover In-the-Wild Exploitation of Zimbra Zero-Day
* API Flaw in QuickBlox Framework Exposed PII of Millions of Users
* Cisco Shopping Spree Adds Oort ID Threat Detection Tech

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [LIVE DEMO] Are Your Users Making Risky Security Mistakes? Deliver Real-Time Coaching in Respons
* KnowBe4 Wins 2023 Top Workplaces for Technology Award
* Ransomware Crypto Payments Are on the Rise While the Rest of Crypto Crime is on the Decline
* Nearly One-Quarter of All Emails Are Considered to be Malicious
* Banking Detail Malvertising Attack Disguises Itself as a Foolproof USPS Google Ad
* [Discovered] An evil new AI disinformation attack called 'PoisonGPT'
* Tailgating Through Physical Security Using Social Engineering Tactics
* Two-Thirds of Ransomware Attacks Against Manufacturing Resulted in Encrypted Data
* Phishing Attacks Employing QR Codes Are Capturing User Credentials
* Launch Of New Meta Thread App Spawns Hundreds Of Spoof Domains

ISC2.org Blog

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

HackRead

* Tips to Choose The Best Web Hosting Service for Your Business
* Steps Involved In Penetration Testing And Their Methodology In Cybersecurity
* Google Removes Swing VPN Android App Exposed as DDoS Botnet
* Dark Web Domain of Genesis Market and Infrastructure Sold
* Fake GitHub Repos Caught Dropping Malware as PoCs AGAIN!
* WormGPT - The Malicious ChatGPT Alternative Empowering Cybercriminals
* Teenagers Face Trial for Hacking BT, Nvidia, Rockstar Games, Revolut, Uber

Koddos

* Tips to Choose The Best Web Hosting Service for Your Business
* Steps Involved In Penetration Testing And Their Methodology In Cybersecurity
* Google Removes Swing VPN Android App Exposed as DDoS Botnet
* Dark Web Domain of Genesis Market and Infrastructure Sold
* Fake GitHub Repos Caught Dropping Malware as PoCs AGAIN!
* WormGPT - The Malicious ChatGPT Alternative Empowering Cybercriminals
* Teenagers Face Trial for Hacking BT, Nvidia, Rockstar Games, Revolut, Uber

Naked Security

* Zimbra Collaboration Suite warning: Patch this 0-day right now (by hand)!
* S3 Ep143: Supercookie surveillance shenanigans
* Microsoft patches four zero-days, finally takes action against crimeware kernel drivers
* Apple silently pulls its latest zero-day update - what now?
* Urgent! Apple fixes critical zero-day hole in iPhones, iPads and Macs
* Serious Security: Rowhammer returns to gaslight your computer
* S3 Ep142: Putting the X in X-Ops
* Firefox 115 is out, says farewell to users of older Windows and Mac versions
* Ghostscript bug could allow rogue documents to run system commands
* WordPress plugin lets users become admins - Patch early, patch often!

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

IBM Security Intelligence

* BlotchyQuasar: X-Force Hive0129 targeting financial institutions in LATAM with a custom banking troja
* Crypto fraud in 2023: How can security teams fight
* Personal data vs. sensitive data: What is the difference?
* Are we doomed to make the same security mistakes with AI?
* CSC report: Space systems should be critical infrastructure
* Beware of the growing scourge of job recruitment scams
* SOAR and SIEM in 2023: Key trends and new changes
* How fraudsters redefine mobile banking account takeovers
* Cloud workload protection platforms: An essential shield
* Is open-source security a ticking cyber time bomb?

InfoWorld

* Build a chatbot with Google's PaLM API
* The biggest barrier to AI productivity is people
* Golang vulnerability checker flags Go vulnerabilities
* What's new in Rust 1.71
* Microsoft Semantic Kernel will support OpenAI plugins
* The engines of AI: Machine learning algorithms explained
* The new high-paying jobs in generative AI
* Visual Studio Code stabilizes Remote Tunnels to WSL
* How to use the is and as operators in C#
* Build custom actions for Power Automate for Windows

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.

Unfortunately, at the time of this report, the Capture the Flag (CTF Time) resource was not availible.

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

* Faraday 4.5.0
* Wireshark Analyzer 4.0.7
* jSQL Injection 0.87
* Zed Attack Proxy 2.13.0 Cross Platform Package
* OATH Toolkit 2.6.9
* jSQL Injection 0.86
* Zeek 6.0.0
* Capstone 5.0
* GNU Privacy Guard 2.4.3
* AIDE 0.18.5

Kali Linux Tutorials

* Vid2img-extract all frame from a given video
* 404 Frame - Infiltrating websites is now easy
* jupyter-kali
* Passwordless Authentication Should Become Mainstream by 2023
* Email2PhoneNumber: Obtain Phone Number via Email Address
* SOC-Multitool
* KubeStalk : Discovers Kubernetes Attack Surface From A Black-Box Perspective
* kalipak
* LazyBox
* Vichiti

GBHackers Analysis

* MITRE Releases Top 25 Most Dangerous Software Weaknesses
* AndroRAT - A Remote Access Trojan Compromise Android Devices and Inject Root Exploits
* Critical Vulnerability in Microsoft Azure Let Hackers Take Over the Complete Control of the Azure Acc
* SIM Swap Attack Let Hackers Port a Telephone Number to a New SIM to Hack WhatsApp & Bypass 2FA
* Massive Cyber Attack Across the World Against ISPs & Data Centres: More than 200,000 Cisco Switches H

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS DFIR Summit & Training 2023
* SANS Threat Analysis Rundown (STAR) with Katie Nickels
* SANS Threat Analysis Rundown | Katie Nickels
* Protecting the Cloud from Ransomware | Host: Ryan Chapman | June 20, 2023

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 - Silk - Hacker Karaoke
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge
* DEF CON 30 - Silk - DEF CON Memorial Interview

Hak5

* State DMV Data Stolen via MOVEit Vulnerabilities & Reddit's API Change Triggers Hackers - ThreatWire
* Microsoft Fined For Violating Children's Privacy - ThreatWire
* Amazon FINED For Privacy Violations - ThreatWire

The PC Security Channel [TPSC]

* How to tell if your PC is Hacked? Process Forensics
* Terminator Malware

Eli the Computer Guy

* Kemper Brown Jr CEO of Electronic Office (MSP - Managed Service Provider)
* Will AI DESTROY the WORLD?
* ChatGPT Token - What is a…
* Social Media is DIGITAL SYPHILIS

Security Now

* Rowhammer Indelible Fingerprinting - MOVEit SQLi flaw, China's OpenKylin v1, Firefox 115, Syncthing
* Operation Triangulation - DuckDuckBrowse, KasperskyOS Phone, Cyber Force, MOVEit

Troy Hunt

* Weekly Update 356

Intel Techniques: The Privacy, Security, & OSINT Show

* 303-iOS Privacy & Security
* 302-Self-Hosted 4: The Next Level

Proof of Concept (PoC) & Exploits

Packet Storm Security

* BloodBank 1.0 Cross Site Scripting
* Blogator 0.93 Cross Site Scripting
* Bigware Shop 2.3 Cross Site Scripting
* Bazaar Social Listing Shopping Web PHP Template 2.3.2 Cross Site Scripting
* pfSense Restore RRD Data Command Injection
* BloodBank 1.0 Insecure Direct Object Reference
* Bloly 1.3 Add Administrator
* BKMobile CMS 1.5.0 SQL Injection
* Blogator Script 0.93 Insecure Settings
* Blackboard 2.0.2 Database Disclosure
* Bigware-Shop CMS 2.1 Insecure Direct Object Reference
* BD-Schools LMS 1.0.2 Cross Site Scripting
* BBook 5.7 Shell Upload
* BBAM 1.1 Insecure Direct Object Reference
* Bazaar Social Listing Shopping Web PHP Template 2.3.2 Privilege Escalation
* Bayfront CMS 1.0 SQL Injection
* ARTISTRY LIMITED LMS 0.5 SQL Injection
* Vaidya-Mitra 1.0 SQL Injection
* WordPress User Registration 3.0.2 Arbitrary File Upload
* Frappe Framework 13.4.0 Remote Code Execution
* Spring Cloud 3.2.2 Remote Command Execution
* Banner RotatorCMS 1.0 Database Disclosure
* Avidi Media 2.0 Insecure Settings
* AtTestimonials CMS 1.2 Missing Authentication
* Atom CMS 2.0 Directory Traversal

CXSecurity

* pfSense Restore RRD Data Command Injection
* Bludit
* MOVEit SQL Injection
* Polycom BToE Connector 4.4.0.0 Buffer Overflow / Man-In-The-Middle
* WordPress Abandoned Cart Lite For WooCommerce 5.14.2 Authentication Bypass
* Oracle Weblogic PreAuth Remote Command Execution
* Instagram App 287.0.0.22.85 - Local Stack Buffer Overflow (DOS)

Proof of Concept (PoC) & Exploits

Exploit Database

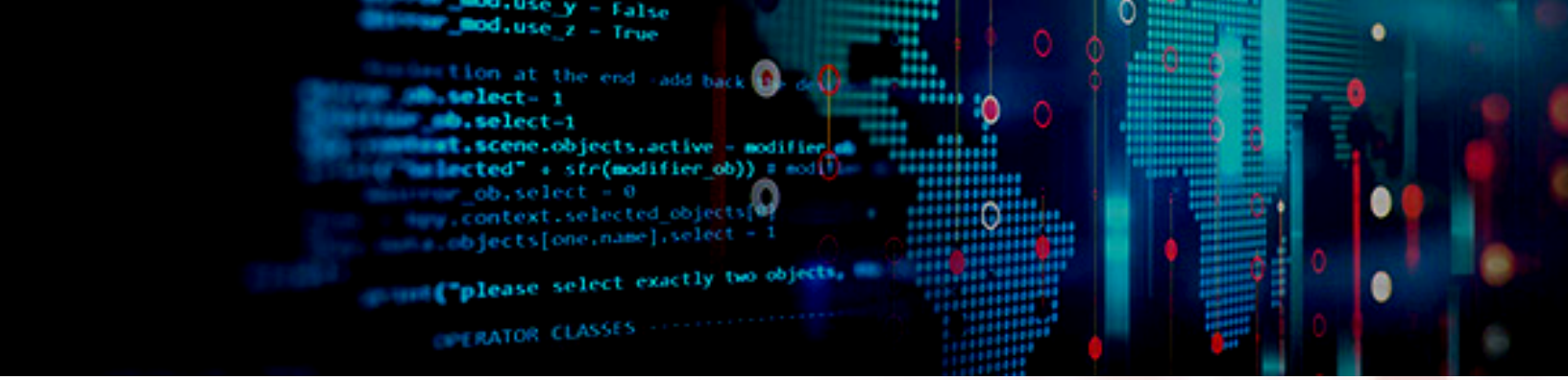
* [webapps] Pluck v4.7.18 - Remote Code Execution (RCE)
* [webapps] WinterCMS
* [webapps] Admidio v4.2.10 - Remote Code Execution (RCE)
* [webapps] Cisco UCS-IMC Supervisor 2.2.0.0 - Authentication Bypass
* [webapps] ProjeQtOr Project Management System v10.4.1 - Multiple XSS
* [webapps] News Portal v4.0 - SQL Injection (Unauthorized)
* [webapps] Icinga Web 2.10 - Authenticated Remote Code Execution
* [local] XAMPP 8.2.4 - Unquoted Path
* [local] Game Jackal Server v5 - Unquoted Service Path "GJServiceV5"
* [local] AVG Anti Spyware 7.5 - Unquoted Service Path "AVG Anti-Spyware Guard"
* [webapps] Ateme TITAN File 3.9 - SSRF File Enumeration
* [webapps] BuildaGate5library v5 - Reflected Cross-Site Scripting (XSS)
* [webapps] Frappe Framework (ERPNext) 13.4.0 - Remote Code Execution (Authenticated)
* [local] MiniTool Partition Wizard ShadowMaker v.12.7 - Unquoted Service Path "MTSchedulerService"
* [local] MiniTool Partition Wizard ShadowMaker v.12.7 - Unquoted Service Path "MTAgentService"
* [webapps] Spring Cloud 3.2.2 - Remote Command Execution (RCE)
* [webapps] Netlify CMS 2.10.192 - Stored Cross-Site Scripting (XSS)
* [remote] Windows 10 v21H1 - HTTP Protocol Stack Remote Code Execution
* [remote] Microsoft Outlook Microsoft 365 MSO (Version 2306 Build 16.0.16529.20100) 32-bit - Remote Co
* [webapps] Faculty Evaluation System v1.0 - SQL Injection
* [webapps] Piwigo v13.7.0 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Lost and Found Information System v1.0 - SQL Injection
* [webapps] Gila CMS 1.10.9 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Beauty Salon Management System v1.0 - SQLi
* [webapps] Car Rental Script 1.8 - 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*

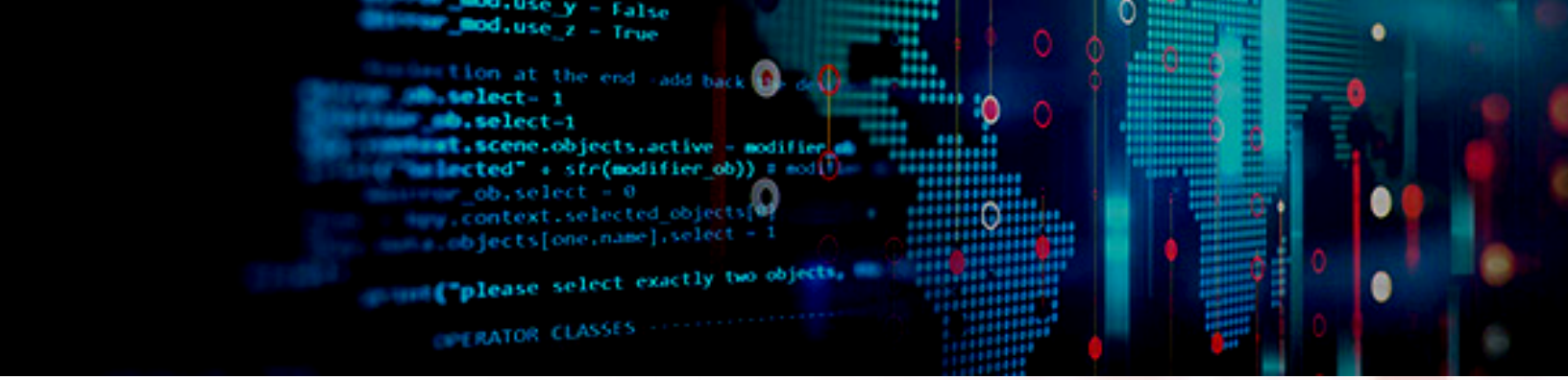
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://unifast.gov.ph/d3c0yph.html
https://unifast.gov.ph/d3c0yph.html notified by d3c0yph
https://kotawaringinbaratkab.go.id/heked.txt
https://kotawaringinbaratkab.go.id/heked.txt notified by KID2ZON3
http://dukcapil.tanjungbalaikota.go.id/read.txt
http://dukcapil.tanjungbalaikota.go.id/read.txt notified by Mr.L3RB1
https://nometnes.gov.lv/a.txt
https://nometnes.gov.lv/a.txt notified by UnM@SK
https://napa.gov.pk
https://napa.gov.pk notified by 0x1998
http://chittagongzoo.gov.bd/fanc.html
http://chittagongzoo.gov.bd/fanc.html notified by Red Cloud
http://alshabab.gov.eg/vbs.html
http://alshabab.gov.eg/vbs.html notified by vbsdz17
https://mesadeayuda.cuenca.gob.ec/pwned.txt
https://mesadeayuda.cuenca.gob.ec/pwned.txt notified by diparis
https://helpdesk.ines.gov.br/marketplace/dct.txt
https://helpdesk.ines.gov.br/marketplace/dct.txt notified by diparis
https://calg.ncr.dilg.gov.ph/km.txt
https://calg.ncr.dilg.gov.ph/km.txt notified by Black-Python
https://diskominfo.donggala.go.id/memekcroot.txt
https://diskominfo.donggala.go.id/memekcroot.txt notified by cirebonblackhat
https://archive.ogunstate.gov.ng/id.htm
https://archive.ogunstate.gov.ng/id.htm notified by Typical Idiot Security
https://observatorio.ssf.gov.co/id.htm
https://observatorio.ssf.gov.co/id.htm notified by Typical Idiot Security
https://rpmcl.nrc.gov.ng/id.htm
https://rpmcl.nrc.gov.ng/id.htm notified by Typical Idiot Security
https://cooperacion.stp.gov.py/id.htm
https://cooperacion.stp.gov.py/id.htm notified by Typical Idiot Security
https://seccan.sec.gov.ph/id.htm
https://seccan.sec.gov.ph/id.htm notified by Typical Idiot Security
https://census.statinja.gov.jm/id.htm
https://census.statinja.gov.jm/id.htm notified by Typical Idiot Security

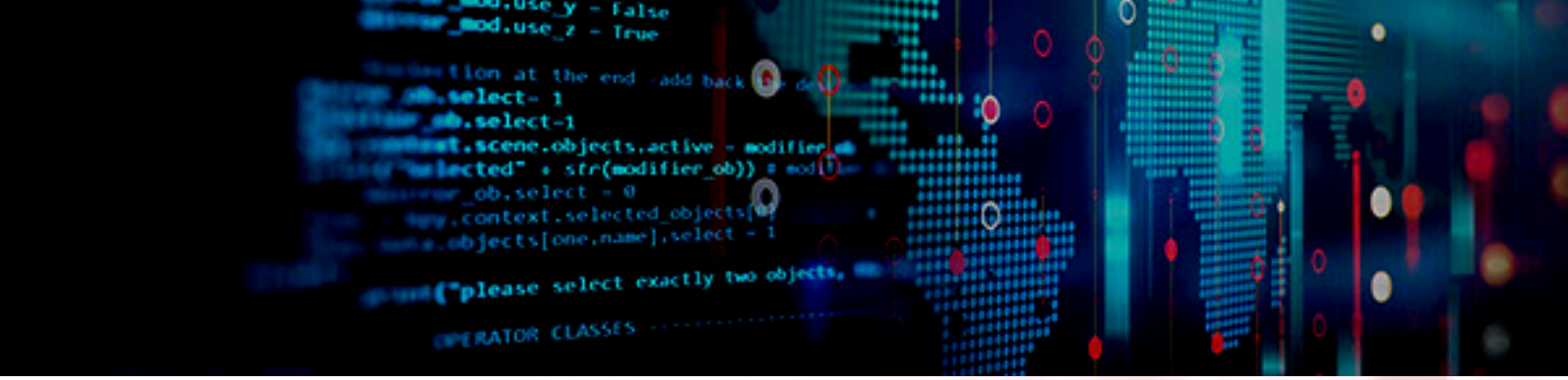


Dark Web News

Darknet Live

[Ross Ulbricht's Advisor "Variety Jones" Imprisoned]
[Washington Man Sentenced for Running a Drugs Vendor Account]
[A Welcome To Video User Sentenced to Federal Prison]
[Maltese Man Purchased Explosives and Poison on the Dark Web]

Dark Web Link



Trend Micro Anti-Malware Blog

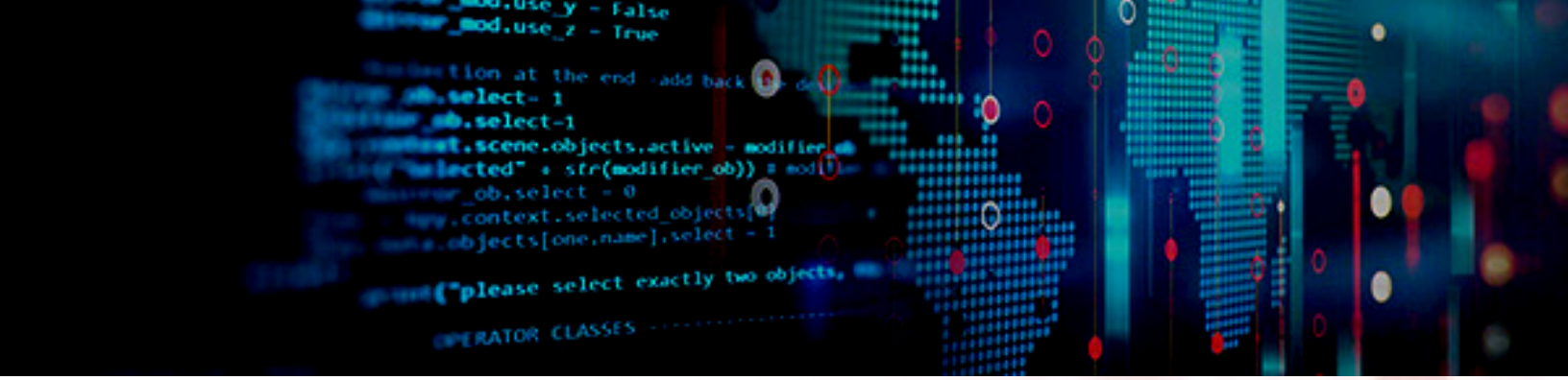
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* 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
* The Japanese Financial Services Attack Landscape
* PenTales: Old Vulns, New Tricks
* Old Blackmoon Trojan, NEW Monetization Approach
* SonicWall Recommends Urgent Patching for GMS and Analytics CVEs
* Patch Tuesday - July 2023
* CVE-2023-29298: Adobe ColdFusion Access Control Bypass
* What's New in Rapid7 Detection & Response: Q2 2023 in Review
* Metasploit Weekly Wrap-Up
* The Japanese Automotive Industry Attack Landscape



Advisories

US-Cert Alerts & bulletins

* CISA Adds Two Known Vulnerabilities to Catalog
* Cisco Releases Security Update for SD-WAN vManage API
* CISA Releases Nine Industrial Control Systems Advisories
* Juniper Releases Multiple Security Updates for Juno OS
* CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting O
* CISA Releases One Industrial Control Systems Advisory
* Mozilla Releases Security Update for Firefox and Firefox ESR
* Microsoft Releases July 2023 Security Updates
* Enhanced Monitoring to Detect APT Activity Targeting Outlook Online
* Increased Truebot Activity Infects U.S. and Canada Based Networks
* Vulnerability Summary for the Week of July 3, 2023
* Vulnerability Summary for the Week of June 26, 2023

Zero Day Initiative Advisories

ZDI-CAN-21287: 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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21675: D-Link
A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21664: D-Link
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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21299: 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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21492: D-Link
A CVSS score 6.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on:

2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21441: 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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21673: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21670: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21667: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21300: 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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21669: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21663: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21672: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21776: Microsoft

A CVSS score 4.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Nicholas Ange' was reported to the affected vendor on: 2023-07-14, 3 days ago. The vendor is given until 2023-11-11 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-21703: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21704: 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 of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21705: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21449: 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 'Anonymous' was reported to the affected vendor on: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21702: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21697: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21424: 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 'Anonymous' was reported to the affected vendor on: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21706: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21698: 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: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 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-21493: 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 'Anonymous' was reported to the affected vendor on: 2023-07-13, 4 days ago. The vendor is given until 2023-11-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-6229-1

Ubuntu Security Notice 6229-1 - It was discovered that LibTIFF was not properly handling variables used to perform memory management operations when processing an image through tiffcrop, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code. It was discovered that LibTIFF was not properly processing numerical values when dealing with little-endian input data, which could lead to the execution of an invalid operation. An attacker could possibly use this issue to cause a denial of service

Ubuntu Security Notice USN-6228-1

Ubuntu Security Notice 6228-1 - It was discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation when mounting certain images. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service. Wei Chen discovered that the InfiniBand RDMA communication manager implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-6227-1

Ubuntu Security Notice 6227-1 - Several security issues were discovered in the SpiderMonkey JavaScript library. If a user were tricked into opening malicious JavaScript applications or processing malformed data, a remote attacker could exploit a variety of issues related to JavaScript security, including denial of service attacks, and arbitrary code execution.

Ubuntu Security Notice USN-6226-1

Ubuntu Security Notice 6226-1 - It was discovered that SciPy did not properly manage memory operations during reference counting. An attacker could possibly use this issue to cause a denial of service. A use-after-free was discovered in SciPy when handling reference counts. An attacker could possibly use this to cause a denial of service. This issue only affected Ubuntu 20.04 LTS.

Red Hat Security Advisory 2023-4071-01

Red Hat Security Advisory 2023-4071-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4066-01

Red Hat Security Advisory 2023-4066-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6225-1

Ubuntu Security Notice 6225-1 - It was discovered that Knot Resolver did not correctly handle certain client options. A remote attacker could send requests to malicious domains and cause a denial of service.

Red Hat Security Advisory 2023-4062-01

Red Hat Security Advisory 2023-4062-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6224-1

Ubuntu Security Notice 6224-1 - It was discovered that the XFS file system implementation in the Linux kernel did not properly perform metadata validation when mounting certain images. An attacker could use this to specially craft a file system image that, when mounted, could cause a denial of service. Wei Chen discovered that the InfiniBand RDMA communication manager implementation in the Linux kernel contained an out-of-bounds read vulnerability. A local attacker could use this to cause a denial of service.

Red Hat Security Advisory 2023-4070-01

Red Hat Security Advisory 2023-4070-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4064-01

Red Hat Security Advisory 2023-4064-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This

update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6223-1

Ubuntu Security Notice 6223-1 - It was discovered that the TUN/TAP driver in the Linux kernel did not properly initialize socket data. A local attacker could use this to cause a denial of service. It was discovered that the Real-Time Scheduling Class implementation in the Linux kernel contained a type confusion vulnerability in some situations. A local attacker could use this to cause a denial of service.

Red Hat Security Advisory 2023-4058-01

Red Hat Security Advisory 2023-4058-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

Red Hat Security Advisory 2023-4065-01

Red Hat Security Advisory 2023-4065-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6222-1

Ubuntu Security Notice 6222-1 - Jiasheng Jiang discovered that the HSA Linux kernel driver for AMD Radeon GPU devices did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service. Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-6221-1

Ubuntu Security Notice 6221-1 - It was discovered that a race condition existed in the overlay file system implementation in the Linux kernel. A local attacker could use this to cause a denial of service. It was discovered that the virtual terminal device implementation in the Linux kernel contained a race condition in its ioctl handling that led to an out-of-bounds read vulnerability. A local attacker could possibly use this to expose sensitive information.

Red Hat Security Advisory 2023-4075-01

Red Hat Security Advisory 2023-4075-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4067-01

Red Hat Security Advisory 2023-4067-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4063-01

Red Hat Security Advisory 2023-4063-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-6216-1

Ubuntu Security Notice 6216-1 - It was discovered that lib3mf did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted 3MF file, a local attacker could possibly use this issue to cause applications using lib3mf to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2023-4072-01

Red Hat Security Advisory 2023-4072-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4073-01

Red Hat Security Advisory 2023-4073-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4069-01

Red Hat Security Advisory 2023-4069-01 - Mozilla Firefox is an open-source web browser, designed for

standards compliance, performance, and portability. This update upgrades Firefox to version 102.13.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-4074-01

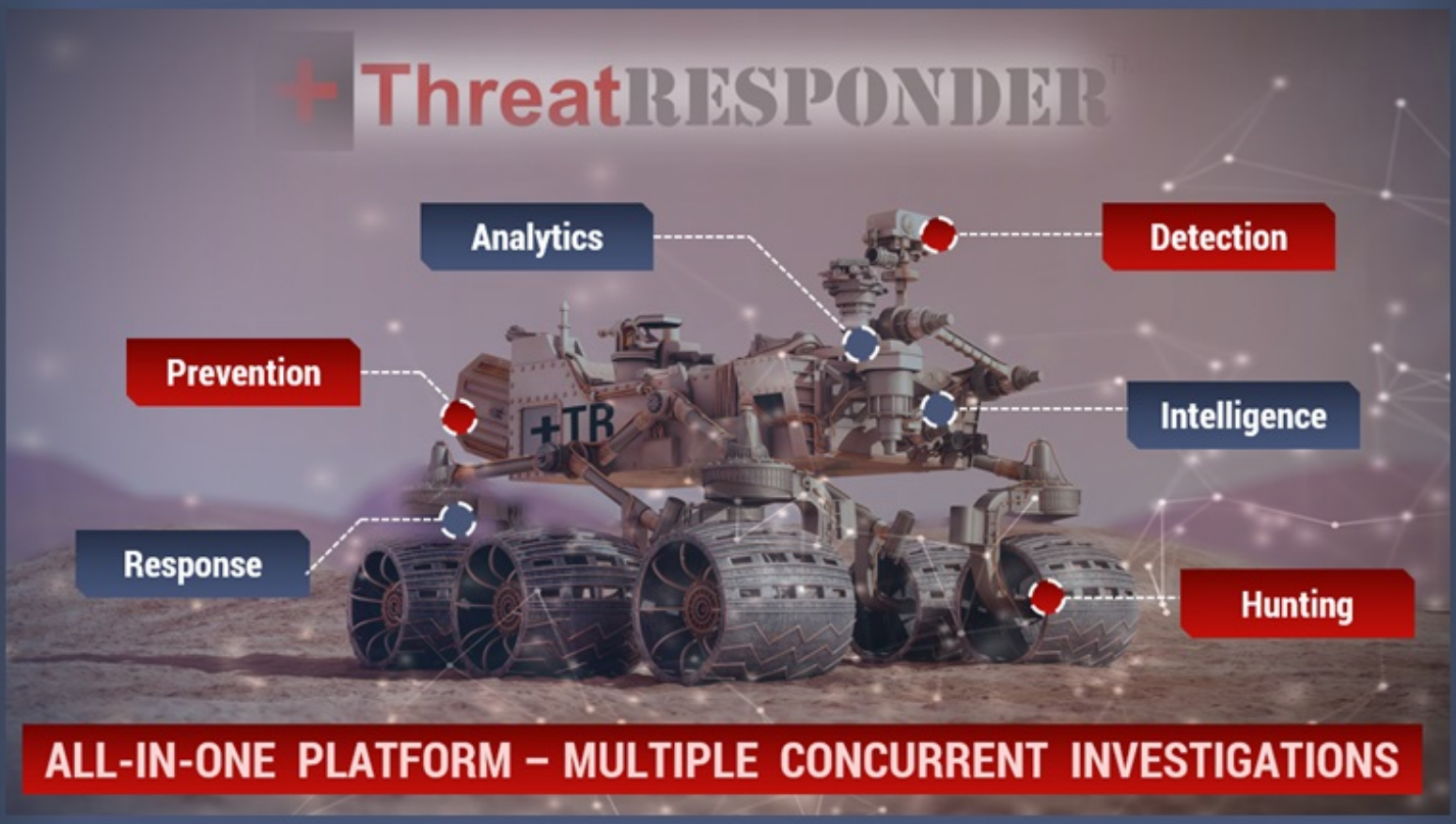
Red Hat Security Advisory 2023-4074-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.13.0. Issues addressed include a use-after-free vulnerability.

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



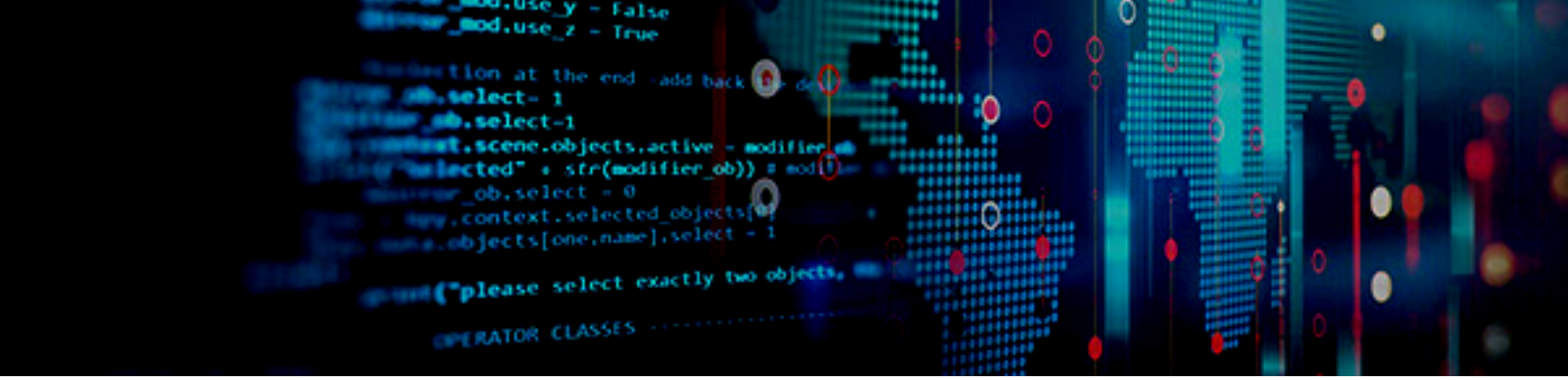
The Solution – ThreatResponder® Platform

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**

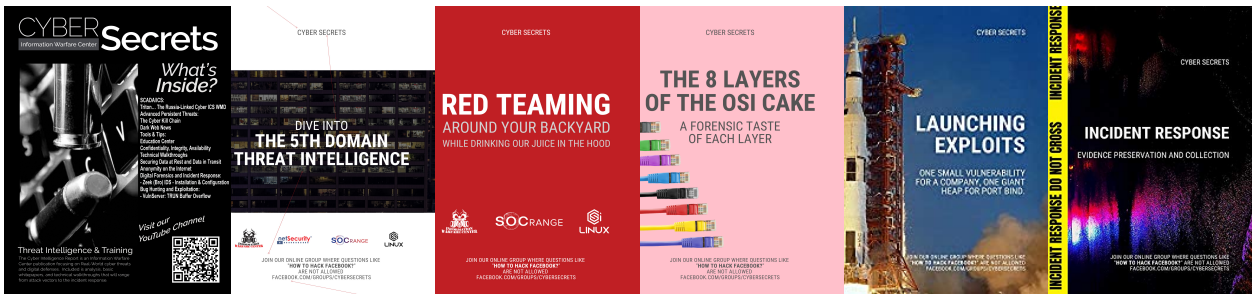
https://netsecurity.com



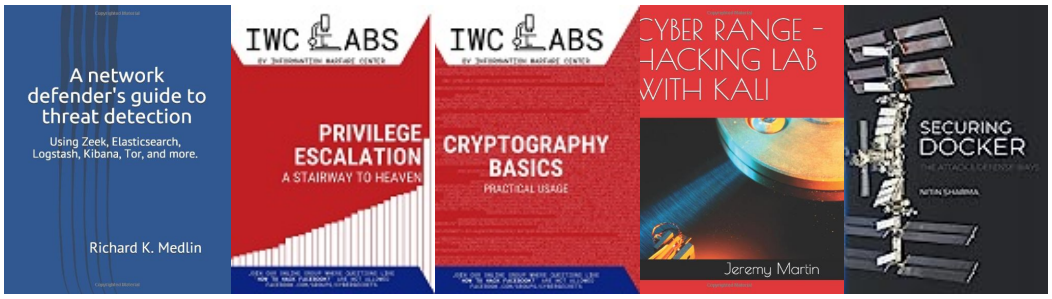
The Cyber Secrets publications on Amazon

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.



Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP