Nov-07-22

CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

November 7, 2022

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

Summary

Internet Storm Center Infocon Status

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

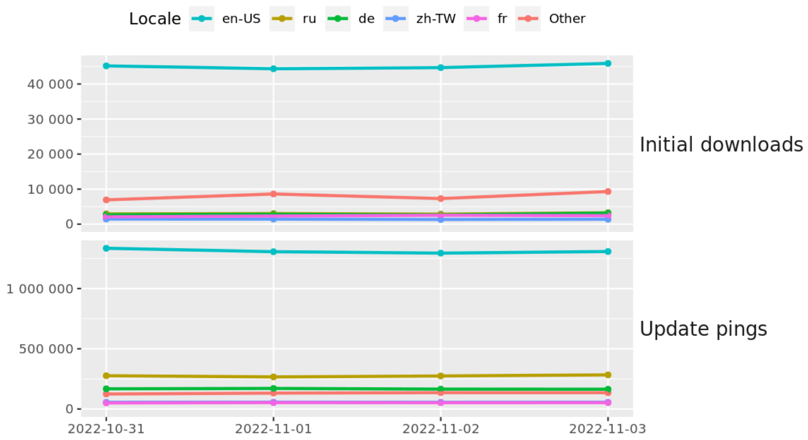
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

Tor Browser downloads and updates by locale



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

* In-Car VR Arrives For New Audis Courtesy Of Holoride
* Why Egypt Became One Of The Biggest Chokepoints For Internet Cables
* OPERA1ER Hackers Steal Over $11 Million From Banks And Telcos
* More Than 250 US News Sites Inject Malware In Possible Supply Chain Attack
* Ukraine War, Geopolitics Fuelling Cybersecurity Attacks
* US Treasury Thwarts DDoS Attack From Russian Killnet Group
* Researchers Discover Link In Tooling Between FIN7 And Black Basta Ransomware Group
* Royal Mail Customer Data Leak Shutters Online Click And Drop
* Your Boss Is Spying On You. The NLRB Might Stop It.
* Former Apple Worker Pleads Guilty To $17m Mail And Wire Fraud Charges
* Ritz Cracker Giant Settles Bust-Up With Insurer Over $100m+ NotPetya Cleanup
* 130 Private Dropbox Github Repos Copied After Phishing Attack
* OpenSSL Downgrades Horror Bug After Week Of Panic, Hype
* Twitter Restricts Staff From Policing Content Violations Ahead Of US Midterms
* U.S. FCC Commissioner Visits Taiwan To Discuss Cybersecurity
* Unofficial Fix Released For Windows Ransomware Enabling Bug
* German Cops Arrest Student Suspected Of Running Dark Web Souk
* Pandemic Relief Fraud Has Congress Eyeing Digital IDs
* IT Defenders Race To Scope Out The Threat Ahead Of OpenSSL Patch Release
* Inside A US Military Cyber Team's Defense Of Ukraine
* Europe Prepares To Rewrite The Rules Of The Internet
* Thawing Permafrost Exposes Old Pathogens And New Hosts
* Cyber Officials From 37 Countries, 13 Companies To Meet On Ransomware In Washington
* Bed Bath And Beyond Reviewing Possible Data Breach
* Burgeoning Cranefly Hacking Group Has A New Intel Gathering Tool

Krebs on Security

* LinkedIn Adds Verified Emails, Profile Creation Dates
* Hacker Charged With Extorting Online Psychotherapy Service
* Accused 'Raccoon' Malware Developer Fled Ukraine After Russian Invasion
* Battle with Bots Prompts Mass Purge of Amazon, Apple Employee Accounts on LinkedIn
* How Card Skimming Disproportionally Affects Those Most In Need
* Anti-Money Laundering Service AMLBot Cleans House
* Microsoft Patch Tuesday, October 2022 Edition
* Report: Big U.S. Banks Are Stiffing Account Takeover Victims
* Glut of Fake LinkedIn Profiles Pits HR Against the Bots
* Microsoft: Two New 0-Day Flaws in Exchange Server

LATEST NEWS

Dark Reading

The Hacker News

* Robin Banks Phishing Service for Cybercriminals Returns with Russian Server
* Researchers Uncover 29 Malicious PyPI Packages Targeted Developers with W4SP Stealer
* Microsoft Warns of Uptick in Hackers Leveraging Publicly-Disclosed 0-Day Vulnerabilities
* Researchers Detail New Malware Campaign Targeting Indian Government Employees
* Your OT Is No Longer Isolated: Act Fast to Protect It
* CISA Warns of Critical Vulnerabilities in 3 Industrial Control System Software
* Researchers Find Links b/w Black Basta Ransomware and FIN7 Hackers
* Why Identity & Access Management Governance is a Core Part of Your SaaS Security
* OPERA1ER APT Hackers Targeted Dozens of Financial Organizations in Africa
* Hackers Using Rogue Versions of KeePass and SolarWinds Software to Distribute RomCom RAT
* New TikTok Privacy Policy Confirms Chinese Staff Can Access European Users' Data
* Multiple Vulnerabilities Reported in Checkmk IT Infrastructure Monitoring Software
* These Android Apps with a Million Play Store Installations Redirect Users to Malicious Sites
* Inside Raccoon Stealer V2
* Experts Warn of SandStrike Android Spyware Infecting Devices via Malicious VPN App

LATEST NEWS

Security Week

* Surveillance 'Existential' Danger of Tech: Signal Boss
* Video: ESG - CISO's Guide to an Emerging Risk Cornerstone
* Apple Rolls Out Xcode Update Patching Git Vulnerabilities
* Cloud-Native Application Security Firm Apiiro Raises $100 Million
* Ransomware Group Threatens to Leak Data Stolen From Car Parts Giant Continental
* Black Basta Ransomware Linked to FIN7 Cybercrime Group
* Red Cross Eyes Digital Emblem for Cyberspace Protection
* Binary Defense Raises $36 Million for MDR Platform
* Cyberattack Causes Trains to Stop in Denmark
* Offense Gets the Glory, but Defense Wins the Game
* Microsoft Extends Aid for Ukraine's Wartime Tech Innovation
* Cisco Patches High-Severity Bugs in Email, Identity, Web Security Products
* Webinar Today: ESG - CISO's Guide to an Emerging Risk Cornerstone
* Splunk Patches 9 High-Severity Vulnerabilities in Enterprise Product
* French-Speaking Cybercrime Group Stole Millions From Banks
* Checkmk Vulnerabilities Can Be Chained for Remote Code Execution
* Over 250 US News Websites Deliver Malware via Supply Chain Attack
* Fortinet Patches 6 High-Severity Vulnerabilities
* US Charges 8 People Over Cybercrime, Tax Fraud Scheme
* Religious Minority Persecuted in Iran Targeted With Sophisticated Android Spyware
* US Electric Cooperatives Awarded $15 Million to Expand ICS Security Capabilities
* CISA Urges Organizations to Implement Phishing-Resistant MFA
* Hackers Stole Source Code, Personal Data From Dropbox Following Phishing Attack
* Microsoft Patches Azure Cosmos DB Flaw Leading to Remote Code Execution
* Anxiously Awaited OpenSSL Vulnerability's Severity Downgraded From Critical to High
* Tailoring Security Training to Specific Kinds of Threats

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* DHL Tops the List of Most Impersonated Brand in Phishing Attacks
* New LinkedIn-Impersonated Phishing Attack Uses Bad Sign-In Attempts to Harvest Credentials
* Number Matching Push-Based MFA Is Only Half the Solution
* KnowBe4 Wins 2022 "Best Software" Awards From TrustRadius in Multiple Categories
* Phishing for Feds: Credential-Harvesting Attacks Found in New Study
* FBI: Watch Out for Student Loan Forgiveness Scams!
* CheckPoint Warns of Black Basta Ransomware as the Number of Victim Organizations Increases by 59%
* CISA Warns of Daxin Team Ransomware Group Targeting the Healthcare and Public Health Sector via VPNs
* Hacking Biometrics: If You Thought Your Fingerprints Were Safe, Think Again!
* Phishing Resistant MFA Does Not Mean Un-Phishable

ISC2.org Blog

* LATEST CYBERTHREATS AND ADVISORIES - November 4, 2022
* Elevating Diverse Voices: (ISC)&sup2; Announces Five Key DEI Partnerships
* Building the Next Generation of Security and Privacy Professionals
* Effective Cybersecurity Board Reporting
* #CybersecurityAwarenessMonth Mentorship Interview Series: Part 3 - Reverse Mentorship

HackRead

* Hackers Abusing Microsoft Dynamics 365 Customer Voice to Steal Credentials
* AS Roma's Paulo Dybala is the new face of Web3 soccer game MonkeyLeague
* 4 Major Benefits of Next Gen SIEM
* Privacy Protocol Elusiv Raises $3.5 Million in Seed Funding
* Blokhaus Announced Launching of New Open-Source NFT Tool Minterpress
* SandStrike Spyware Infecting Android Devices through VPN Apps
* OpenSSL Released Patch for High-Severity Vulnerability Detected Last Week

Koddos

* Hackers Abusing Microsoft Dynamics 365 Customer Voice to Steal Credentials
* AS Roma's Paulo Dybala is the new face of Web3 soccer game MonkeyLeague
* 4 Major Benefits of Next Gen SIEM
* Privacy Protocol Elusiv Raises $3.5 Million in Seed Funding
* Blokhaus Announced Launching of New Open-Source NFT Tool Minterpress
* SandStrike Spyware Infecting Android Devices through VPN Apps
* OpenSSL Released Patch for High-Severity Vulnerability Detected Last Week

LATEST NEWS

Naked Security

* Twitter Blue Badge email scams - Don't fall for them!
* The OpenSSL security update story - how can you tell what needs fixing?
* S3 Ep107: Eight months to kick out the crooks and you think that's GOOD? [Audio + Text]
* OpenSSL patches are out - CRITICAL bug downgraded to HIGH, but patch anyway!
* SHA-3 code execution bug patched in PHP - check your version!
* Psychotherapy extortion suspect: arrest warrant issued
* Chrome issues urgent zero-day fix - update now!
* Updates to Apple's zero-day update story - iPhone and iPad users read this!
* S3 Ep106: Facial recognition without consent - should it be banned?
* Online ticketing company "See" pwned for 2.5 years by attackers

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

Unfortunately, at the time of this report, the IBM Security Intelligence Blog resource was not availible.

InfoWorld

* Qualys previews TotalCloud FlexScan for multicloud security management
* OpenJDK considers async stack traces for Java
* IBM bolsters BI offerings with Business Analytics Enterprise suite
* The cloud is downturn-proof-maybe
* How to use the in, out, and ref keywords in .NET Core
* Intro to virtual threads: A new approach to Java concurrency
* New TypeScript operator finds coding mistakes
* Microsoft Java introduces compiler optimization
* Grafana Labs' Phlare, Faro to simplify profiling, app observability
* Azul detects Java vulnerabilities in production apps

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

* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021
* Is It Worth Public Speaking?

Google Zero Day Project

* A Very Powerful Clipboard: Analysis of a Samsung in-the-wild exploit chain
* Gregor Samsa: Exploiting Java's XML Signature Verification

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.

* 4th stage MetaRed CTF Per&uacute; 2022
* HK Cyber Security New Generation CTF Challenge 2022
* ISITDTU CTF 2022 Quals
* SECCON CTF 2022 Quals
* RuCTF Finals 2022
* BlackHat MEA CTF Final 2022
* CTF After Dark - Fall 2022
* m0leCon CTF 2022
* Square CTF 2022
* Digital Overdose 2022 Autumn CTF

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

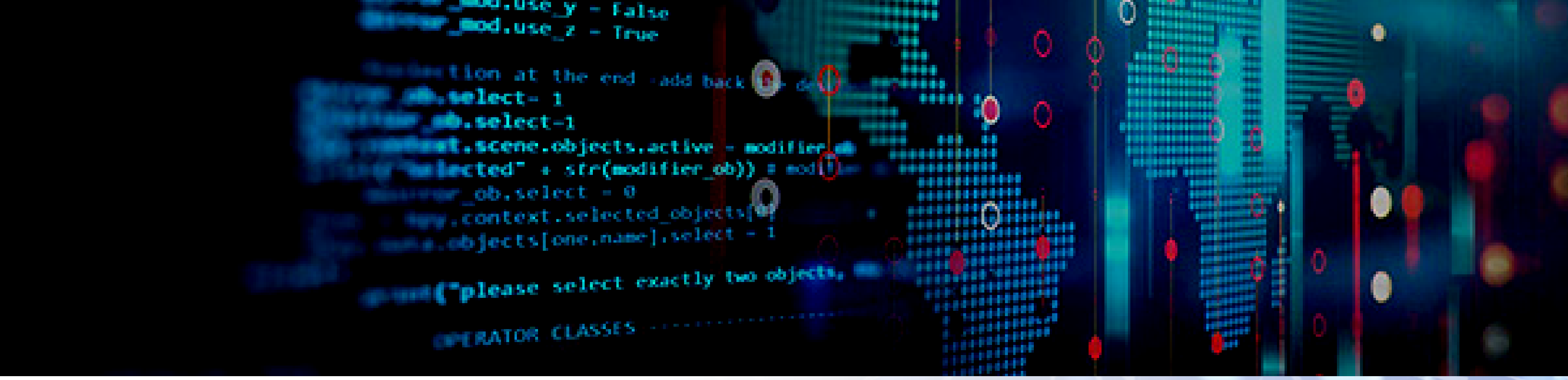
* OpenSSL Toolkit 3.0.7
* OpenSSL Toolkit 1.1.1s
* Faraday 4.2.0
* Proxmark3 4.15864 Custom Firmware
* Zed Attack Proxy 2.12.0 Cross Platform Package
* GNUnet P2P Framework 0.18.0
* Wireshark Analyzer 4.0.1
* nfstream 6.5.3
* MutableSecurity 0.4.0
* Falco 0.33.0

Kali Linux Tutorials

* Mangle : Tool That Manipulates Aspects Of Compiled Executables (.Exe Or DLL) To Avoid Detection From
* Shomon : Shodan Monitoring Integration For TheHive
* Usbsas : Tool And Framework For Securely Reading Untrusted USB Mass Storage Devices
* MHDDoS : DDoS Attack Script With 56 Methods
* PartyLoud : A Simple Tool To Generate Fake Web Browsing And Mitigate Tracking
* How to Install and Run Rust on Linux
* PenguinTrace : Tool To Show How Code Runs At The Hardware Level
* xnLinkFinder : A Python Tool Used To Discover Endpoints And Potential Parameters
* JSubFinder : Searches Webpages For Javascript To Find Hidden Subdomains & Secrets
* God Genesis : Payload Capable Bypass All The Known Antiviruses And Endpoints

GBHackers Analysis

* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input
* Tips to Avoid a Home Security System Hack



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown (STAR)
* SANS Threat Analysis Rundown (STAR)
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown

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

* Microsoft Discloses Unpatched (Officially) Zero Day - ThreatWire
* Live Hacking Q&A with Kody and Michael
* IoT Nutrition labels TBA 2023 - ThreatWire

The PC Security Channel [TPSC]

* Bonzi Buddy: Friendliest Malware
* Is your PC hacked? RAM Forensics with Volatility

Eli the Computer Guy

* TWITTER ADVERTISER BOYCOTT - Elon Musk Threatens to go "Thermonuclear"
* TWITTER LAYOFFS - Elon Musk Fires HALF of EMPLOYEES
* The RECESSION HAS STARTED
* Nancy Pelosi's Husband Attacked in House - Failure of Security Technology

Security Now

* After 20 years in GCHQ - Stranger Strings, PayPal passkeys, new TCP/IP RCE in Windows
* Data Breach Responsibility - Firefox 106, KataOS and Sparrow, banking malware, CVSS 9.8 update

Troy Hunt

* Weekly Update 320

Intel Techniques: The Privacy, Security, & OSINT Show

* 283-Announcements, Updates, & News
* 282-Major OSINT Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* WebKit HTMLSelectElement Use-After-Free
* Senayan Library Management System 9.5.0 SQL Injection
* Automated Tank Gauge (ATG) Remote Configuration Disclosure
* Apache CouchDB Erlang Remote Code Execution
* FLIR AX8 1.46.16 Remote Command Injection
* Webmin 1.984 File Manager Remote Code Execution
* Packet Storm New Exploits For October, 2022
* Leeloo Multipath Authorization Bypass / Symlink Attack
* Simple Cold Storage Management System 1.0 SQL Injection
* Train Scheduler App 1.0 Insecure Direct Object Reference
* wolfSSL Buffer Overflow
* Ecommerce CodeIgniter Bootstrap 1.0 Cross Site Scripting
* Siemens APOGEE PXC / TALON TC Authentication Bypass
* Vagrant Synced Folder Vagrantfile Breakout
* Dinstar FXO Analog VoIP Gateway DAG2000-16O Cross Site Scripting
* ERP Sankhya 4.13.x Cross Site Scripting
* GLPI 10.0.2 Command Injection
* ZKTeco ZEM500-510-560-760 / ZEM600-800 / ZEM720 / ZMM Missing Authentication
* Backdoor.Win32.Psychward.10 MVID-2022-0651 Remote Command Execution
* Email-Worm.Win32.Kipis.c MVID-2022-0652 File Write / Code Execution
* Pega Platform 8.7.3 Remote Code Execution
* Backdoor.Win32.Delf.arh MVID-2022-0650 Authentication Bypass
* Zimbra Collaboration Suite TAR Path Traversal
* Chrome AccountSelectionBubbleView::OnAccountImageFetched Heap Use-After-Free
* Cisco Jabber XMPP Stanza Smuggling

CXSecurity

* Automated Tank Gauge (ATG) Remote Configuration Disclosure
* Apache CouchDB Erlang Remote Code Execution
* FLIR AX8 1.46.16 Remote Command Injection meta
* Webmin 1.984 File Manager Remote Code Execution
* Siemens APOGEE PXC / TALON TC Authentication Bypass
* AVS Audio Converter 10.3 Stack Overflow
* MiniDVBLinux 5.4 Arbitrary File Read

Proof of Concept (PoC) & Exploits

Exploit Database

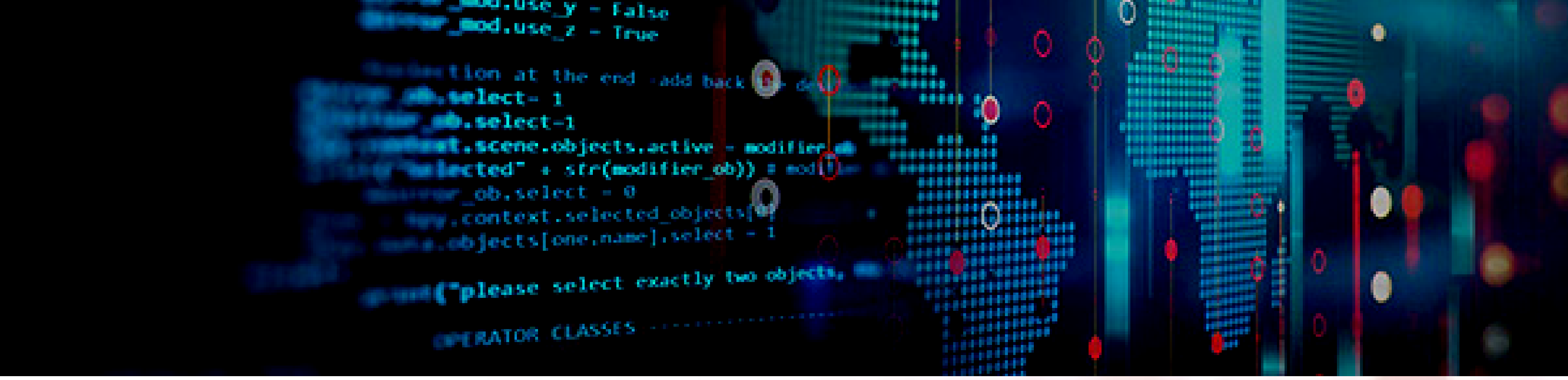
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (RCE) (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - Stored Cross-Site Scripting (XSS)
* [webapps] Sophos XG115w Firewall 17.0.10 MR-10 - Authentication Bypass
* [remote] PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)
* [webapps] ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)
* [webapps] Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Prestashop blockwishlist module 2.1.0 - SQLi

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
```

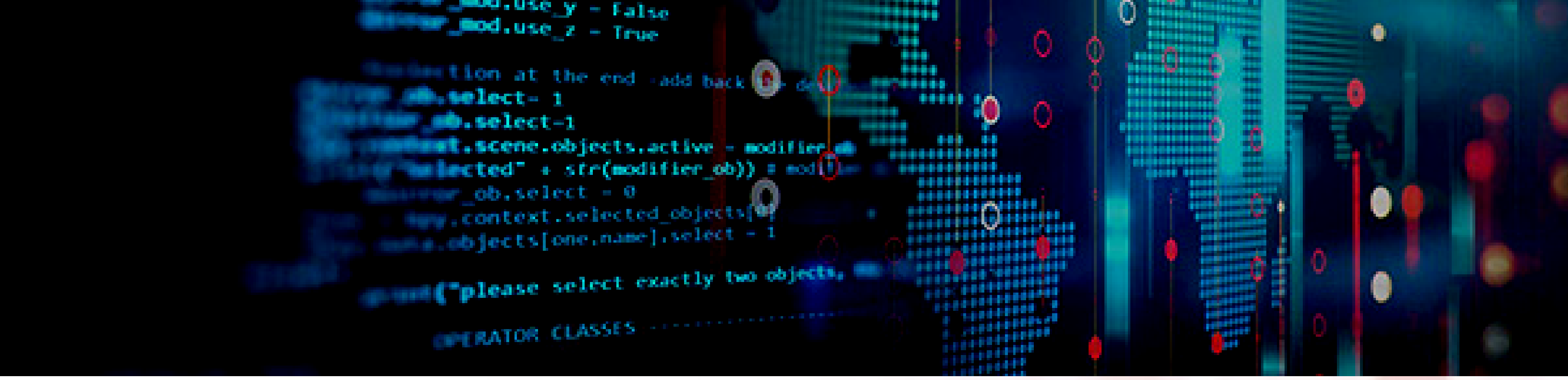
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://mhpa.gov.bt/R.html
http://mhpa.gov.bt/R.html notified by RUBIYAT
http://lansakae.go.th
http://lansakae.go.th notified by Mendung_Ireng
https://kpese.gov.pk/-.php
https://kpese.gov.pk/-.php notified by Throvinus
https://pn-pasarwajo.go.id/readme.html
https://pn-pasarwajo.go.id/readme.html notified by F3RGUSO
https://skwdaqua.gov.ph/pwnslaught.txt
https://skwdaqua.gov.ph/pwnslaught.txt notified by pwnslaught
https://gnhc.gov.bt/info.php
https://gnhc.gov.bt/info.php notified by UnM@SK
http://conocer.gob.mx/CR4P5.txt
http://conocer.gob.mx/CR4P5.txt notified by Mr.CR4P5
http://reddesaludabancay.gob.pe/license.txt
http://reddesaludabancay.gob.pe/license.txt notified by tegal9etar
https://hyppadec.gov.ng/wp-config-sample.php
https://hyppadec.gov.ng/wp-config-sample.php notified by 0xEv1lS0UL
https://kec-bekasiutara.bekasikota.go.id/0x.htm
https://kec-bekasiutara.bekasikota.go.id/0x.htm notified by UnM@SK
https://setda.bekasikota.go.id/0x.htm
https://setda.bekasikota.go.id/0x.htm notified by UnM@SK
https://kec-rawalumbu.bekasikota.go.id/0x.htm
https://kec-rawalumbu.bekasikota.go.id/0x.htm notified by UnM@SK
https://disdukcapil.bekasikota.go.id/0x.htm
https://disdukcapil.bekasikota.go.id/0x.htm notified by UnM@SK
https://kec-bantargebang.bekasikota.go.id/0x.htm
https://kec-bantargebang.bekasikota.go.id/0x.htm notified by UnM@SK
https://satpolpp.bekasikota.go.id/0x.htm
https://satpolpp.bekasikota.go.id/0x.htm notified by UnM@SK
https://kec-pondokmelati.bekasikota.go.id/0x.htm
https://kec-pondokmelati.bekasikota.go.id/0x.htm notified by UnM@SK
https://dkukm.bekasikota.go.id/0x.htm
https://dkukm.bekasikota.go.id/0x.htm notified by UnM@SK

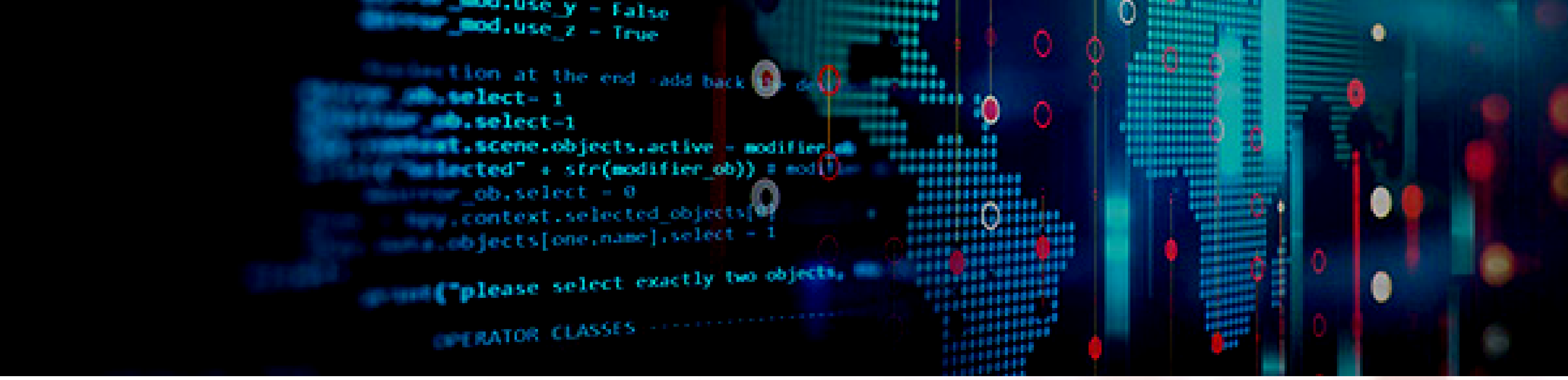


Dark Web News

Darknet Live

Illinois Man Sentenced for Buying 900 Grams of MDMA
Florida Man Convicted of Using Crypto Mixers to Evade Taxes
US Government Calls for More Cryptocurrency Regulation
Binance Announces Law Enforcement Training Program

Dark Web Link



Trend Micro Anti-Malware Blog

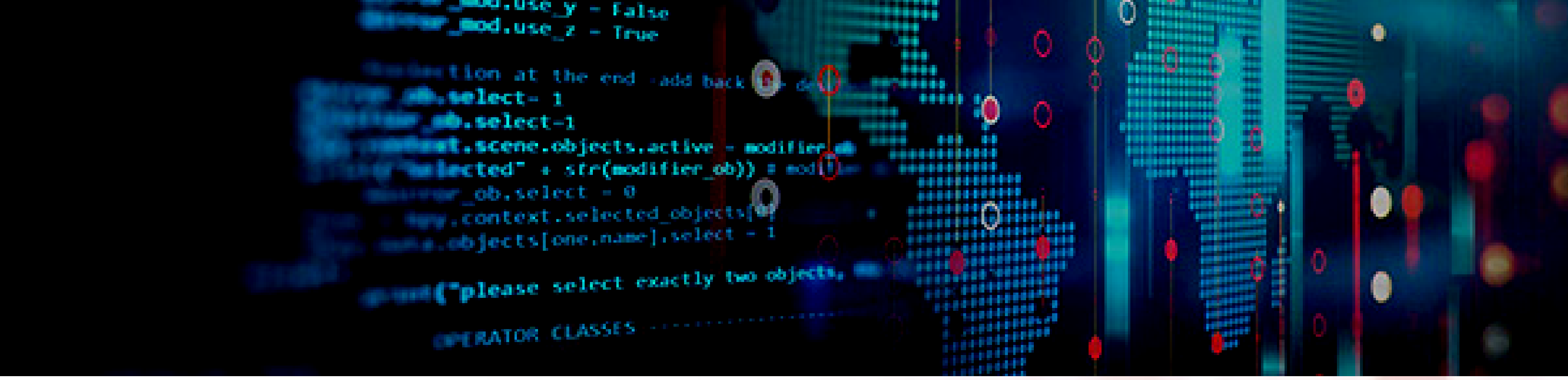
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Rapid7's Impact from Apache Commons Text Vulnerability (CVE-2022-42889)
* Go Inside Rapid7 MDR: Timelines and Tick Tocks
* Common questions when evolving your VM program
* Hands-On IoT Hacking: Rapid7 at DEF CON 30 IoT Village, Pt. 3
* CVE-2022-3786 and CVE-2022-3602: Two High-Severity Buffer Overflow Vulnerabilities in OpenSSL Fixed
* 7 Rapid Questions with Toshio Honda, Sr. Security Solutions Engineer
* Metasploit Weekly Wrap-UP
* From Churn to Cherry on Top: How to Foster Talent in a Cybersecurity Skills Gap
* CVE-2021-39144: VMware Cloud Foundation Unauthenticated Remote Code Execution



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for Multiple Products
* Apple Releases Security Update for Xcode
* CISA Releases Three Industrial Control Systems Advisories
* OpenSSL Releases Security Update
* CISA Upgrades to TLP 2.0
* CISA Releases One Industrial Control Systems Advisory
* CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication
* CISA Has Added One Known Exploited Vulnerability to Catalog
* AA22-294A: #StopRansomware: Daixin Team
* AA22-279A: Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors
* Vulnerability Summary for the Week of October 24, 2022
* Vulnerability Summary for the Week of October 17, 2022

Zero Day Initiative Advisories

ZDI-CAN-19411: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19385: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19387: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-18848: Trend Micro
A CVSS score 8.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L) severity vulnerability discovered by 'Elias Martinez (filenotfound - https://www.linkedin.com/in/eli-martinez07/)' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19384: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is

given until 2023-03-04 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-19383: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19382: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19391: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19413: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19393: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19240: 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 'Ashfaq Ansari and Krishnakant Patil - HackSys Inc' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19390: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19412: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19410: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19389: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19386: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-19388: 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: 2022-11-04, 3 days ago. The vendor is given until 2023-03-04 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-18933: 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 'Alexandre Adamski of Impalabs' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-18964: Parallels

A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'kn32' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-19187: Parallels

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'kn32' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-19103: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-19095: KeySight

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Steven Seeley (mr_me) of Source Incite' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-18896: Microsoft

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 'Eduardo Braun Prado' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 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-19303: 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 'hades_kito' was reported to the affected vendor on: 2022-11-03, 4 days ago. The vendor is given until 2023-03-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Red Hat Security Advisory 2022-7410-01

Red Hat Security Advisory 2022-7410-01 - Red Hat Single Sign-On 7.6 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.6.1 on RHEL 8 serves as a replacement for Red Hat Single Sign-On 7.6.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include HTTP request smuggling, code execution, cross site scripting, and denial of service vulnerabilities.

Red Hat Security Advisory 2022-7409-01

Red Hat Security Advisory 2022-7409-01 - Red Hat Single Sign-On 7.6 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.6.1 on RHEL 7 serves as a replacement for Red Hat Single Sign-On 7.6.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include HTTP request smuggling, code execution, cross site scripting, and denial of service vulnerabilities.

Red Hat Security Advisory 2022-7417-01

Red Hat Security Advisory 2022-7417-01 - Red Hat Single Sign-On 7.6 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.6.1 serves as a replacement for Red Hat Single Sign-On 7.6.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include HTTP request smuggling, code execution, cross site scripting, and denial of service vulnerabilities.

Red Hat Security Advisory 2022-7407-01

Red Hat Security Advisory 2022-7407-01 - Service Binding Operator 1.3.1 is now available for OpenShift Developer Tools and Services for OCP 4.9 +.

Red Hat Security Advisory 2022-7411-01

Red Hat Security Advisory 2022-7411-01 - Red Hat Single Sign-On 7.6 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.6.1 on RHEL 9 serves as a replacement for Red Hat Single Sign-On 7.6.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include HTTP request smuggling, code execution, cross site scripting, and denial of service vulnerabilities.

Ubuntu Security Notice USN-5712-1

Ubuntu Security Notice 5712-1 - It was discovered that SQLite did not properly handle large string inputs in certain circumstances. An attacker could possibly use this issue to cause a denial of service or arbitrary code execution.

Ubuntu Security Notice USN-5713-1

Ubuntu Security Notice 5713-1 - Devin Jeanpierre discovered that Python incorrectly handled sockets when the multiprocessing module was being used. A local attacker could possibly use this issue to execute arbitrary code and escalate privileges.

Ubuntu Security Notice USN-5711-2

Ubuntu Security Notice 5711-2 - USN-5711-1 fixed a vulnerability in NTFS-3G. This update provides the corresponding update for Ubuntu 14.04 ESM Ubuntu 16.04 ESM. Yuchen Zeng and Eduardo Vela discovered that NTFS-3G incorrectly validated certain NTFS metadata. A local attacker could possibly use this issue to gain privileges.

Red Hat Security Advisory 2022-7216-01

Red Hat Security Advisory 2022-7216-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.9.51. Issues addressed include code execution and memory leak vulnerabilities.

Red Hat Security Advisory 2022-7384-01

Red Hat Security Advisory 2022-7384-01 - The ubi9/openssl image provides provides an openssl command-line tool for using the various functions of the OpenSSL crypto library. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2022-7323-01

Red Hat Security Advisory 2022-7323-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-7338-01

Red Hat Security Advisory 2022-7338-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include code execution, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-7329-01

Red Hat Security Advisory 2022-7329-01 - The lua packages provide support for Lua, a powerful light-weight programming language designed for extending applications. Lua is also frequently used as a general-purpose, stand-alone language. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2022-7343-01

Red Hat Security Advisory 2022-7343-01 - The pcs packages provide a command-line configuration system for the Pacemaker and Corosync utilities. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-7318-01

Red Hat Security Advisory 2022-7318-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-7313-01

Red Hat Security Advisory 2022-7313-01 - Red Hat Advanced Cluster Management for Kubernetes 2.6.2 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. Issues addressed include denial of service and remote SQL injection vulnerabilities.

Red Hat Security Advisory 2022-7330-01

Red Hat Security Advisory 2022-7330-01 - 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 privilege escalation and use-after-free vulnerabilities.

Debian Security Advisory 5269-1

Debian Linux Security Advisory 5269-1 - Nicky Mouha discovered a buffer overflow in the sha3 module of PyPy, a fast, compliant alternative implementation of the Python language.

Red Hat Security Advisory 2022-7319-01

Red Hat Security Advisory 2022-7319-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-7344-01

Red Hat Security Advisory 2022-7344-01 - 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 privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-7314-01

Red Hat Security Advisory 2022-7314-01 - The zlib packages provide a general-purpose lossless data compression library that is used by many different programs. Issues addressed include buffer over-read and buffer overflow vulnerabilities.

Red Hat Security Advisory 2022-7326-01

Red Hat Security Advisory 2022-7326-01 - The Public Key Infrastructure Core contains fundamental packages required by Red Hat Certificate System.

Red Hat Security Advisory 2022-7340-01

Red Hat Security Advisory 2022-7340-01 - The php-pear package contains the PHP Extension and Application Repository, a framework and distribution system for reusable PHP components. Issues addressed include file overwrite and traversal vulnerabilities.

Red Hat Security Advisory 2022-7337-01

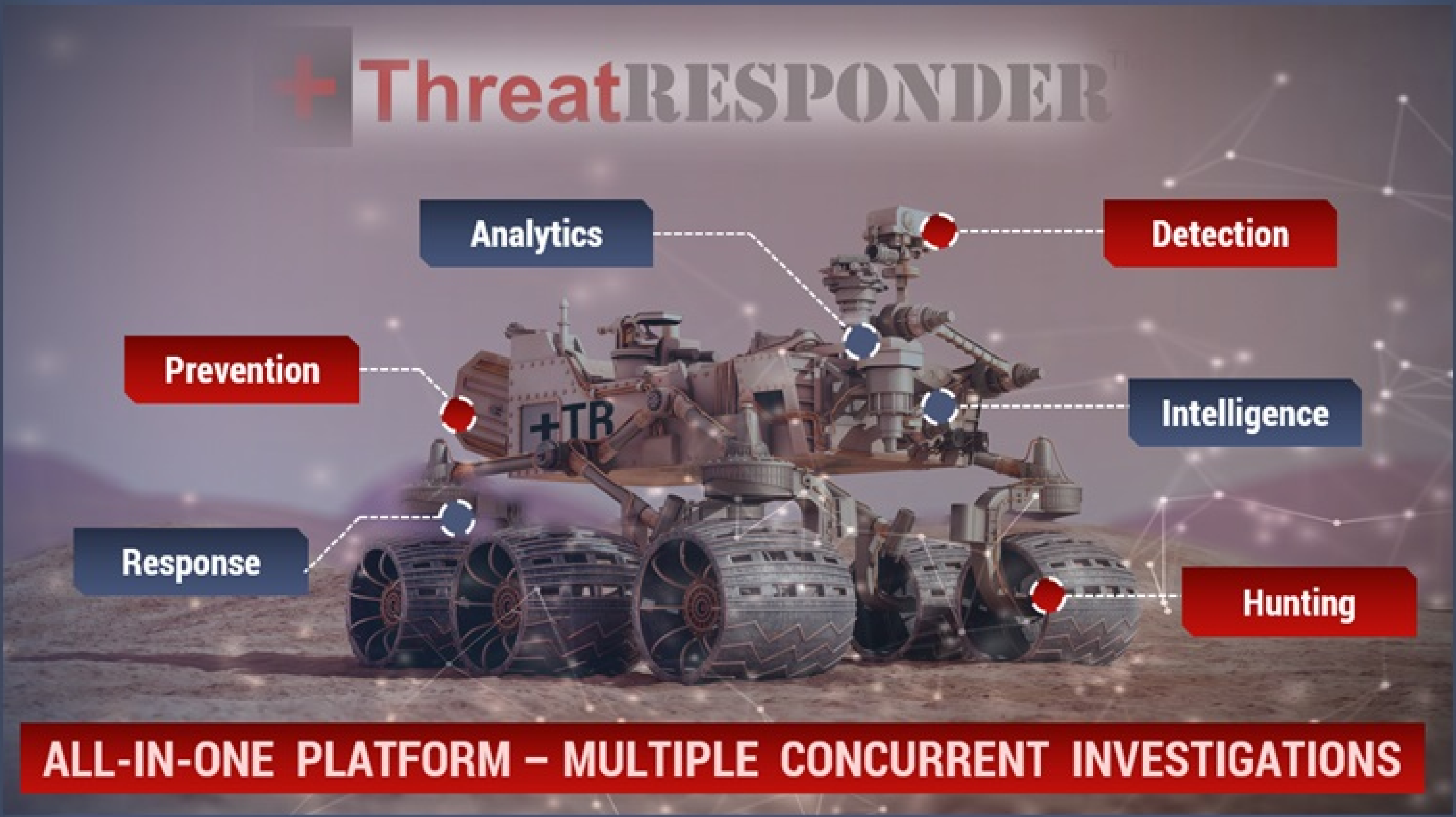
Red Hat Security Advisory 2022-7337-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include code execution, privilege escalation, and use-after-free vulnerabilities.

Are You…

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

Do DFIR Investigations Better

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



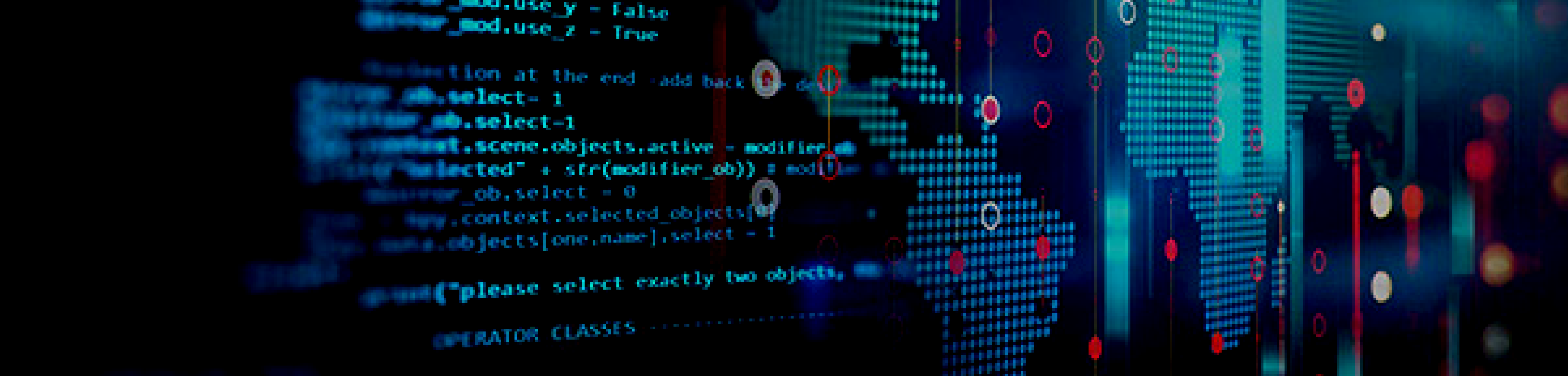
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

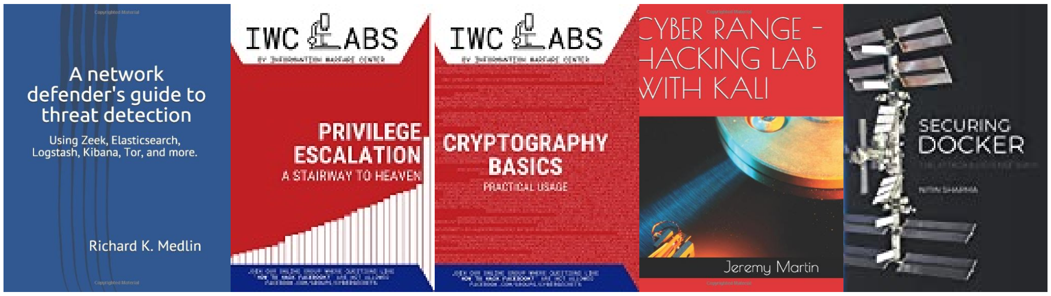

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier
"elected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

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