Oct-31-22

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

October 31, 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

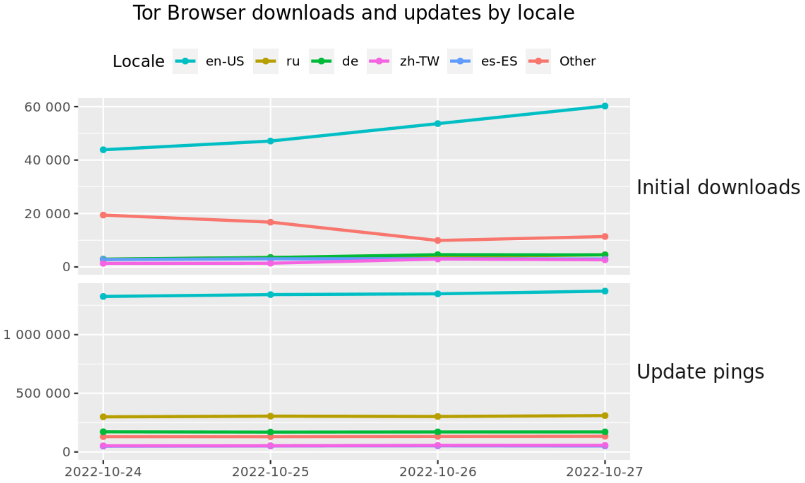
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* 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
* Biden Now Wants To Toughen Up Chemical Sector Cybersecurity
* Meet The Windows Servers That Have Been Fueling Massive DDoSes For Months
* What Does The Fox Hack? Breaking Down The Anonymous Fox F-Automatical Script
* Ukrainian Running Malware Service Amassed 50M Credentials
* Cisco AnyConnect Windows Client Under Active Attack
* Pro-China Crew Ramps Up Disinfo Ahead Of US Midterms
* High Severity Vulnerability In GitHub Was Susceptible To Repo Jacking
* APAC Faces 2.1M Shortage In Cybersecurity Professionals
* PayPal Ditches Passwords, At Least On Apple Devices
* Researchers Uncover Cryptojacking Campaign Targeting Docker, Kubernetes Cloud Servers
* Medibank's Data Breach Diagnosis Keeps Getting Worse
* Apple Releases Patch For iPhone And iPad Zero Day
* DHL Named Most-Spoofed Brand In Phishing
* Payment Terminal Malware Steals $3.3m Worth Of Credit Card Numbers
* Senator Pushes Zuckerberg On How Facebook Collects Health Information
* FBI Warns Ransomware Group Targeting Poorly Protected VPN Servers
* US Charges Alleged Chinese Spies In Telecoms Probe Case
* Google Says Slap Some GUAC On Your Software Supply Chain
* BlackByte Ransomware Slinger Twists The Knife With Data Stealer

Krebs on Security

* 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
* Fake CISO Profiles on LinkedIn Target Fortune 500s
* Accused Russian RSOCKS Botmaster Arrested, Requests Extradition to U.S.
* SIM Swapper Abducted, Beaten, Held for $200k Ransom

LATEST NEWS

Dark Reading

The Hacker News

* Fodcha DDoS Botnet Resurfaces with New Capabilities
* Tips for Choosing a Pentesting Company
* Unofficial Patch Released for New Actively Exploited Windows MotW Vulnerability
* Samsung Galaxy Store Bug Could've Let Hackers Secretly Install Apps on Targeted Devices
* GitHub Repojacking Bug Could've Allowed Attackers to Takeover Other Users' Repositories
* Twilio Reveals Another Breach from the Same Hackers Behind the August Hack
* High-Severity Flaws in Juniper Junos OS Affect Enterprise Networking Devices
* These Dropper Apps On Play Store Targeting Over 200 Banking and Cryptocurrency Wallets
* Cloud Security Made Simple in New Guidebook For Lean Teams
* Researchers Uncover Stealthy Techniques Used by Cranefly Espionage Hackers
* Implementing Defense in Depth to Prevent and Mitigate Cyber Attacks
* Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability
* Raspberry Robin Operators Selling Cybercriminals Access to Thousands of Endpoints
* British Hacker Charged for Operating "The Real Deal" Dark Web Marketplace
* Researchers Expose Over 80 ShadowPad Malware C2 Servers

LATEST NEWS

Security Week

* Deepfakes - Significant or Hyped Threat?
* White House Invites Dozens of Nations for Ransomware Summit
* Label Giant Multi-Color Corporation Discloses Data Breach
* VMware Warns of Exploit for Recent NSX-V Vulnerability
* How to Prepare for New SEC Cybersecurity Disclosure Requirements
* Critical ConnectWise Vulnerability Affects Thousands of Internet-Exposed Servers
* Copper Giant Aurubis Shuts Down Systems Due to Cyberattack
* Calls for UK to Probe Reported Hacking of Liz Truss's Phone
* Indianapolis Low-Income Housing Agency Hit by Ransomware
* Twilio Says Employees Targeted in Separate Smishing, Vishing Attacks
* DHS Develops Baseline Cybersecurity Goals for Critical Infrastructure
* Apple Paid Out $20 Million via Bug Bounty Program
* Google Releases Emergency Chrome 107 Update to Patch Actively Exploited Zero-Day
* Slovak, Polish Parliaments Hit by Cyberattacks
* New York Post 'Hacked' in Tweets Calling for Assassination of Biden, Lawmakers
* Asset Risk Management Firm Sepio Raises $22 Million in Series B Funding
* Versa Networks Raises $120 Million in Pre-IPO Funding Round
* GitHub Account Renaming Could Have Led to Supply Chain Attacks
* See Tickets Customer Payment Card Data Stolen by Web Skimmer
* Windows Event Log Vulnerabilities Could Be Exploited to Blind Security Products
* White House Adds Chemical Sector to ICS Cybersecurity Initiative
* Industrial Ransomware Attacks: New Groups Emerge, Manufacturing Pays Highest Ransom
* VMware Patches Critical Vulnerability in End-of-Life Product
* Drizly Agrees to Tighten Data Security After Alleged Breach
* Leveraging Managed Services to Optimize Your Threat Intelligence Program During an Economic Downturn
* Spyderbat Raises $10 Million for Cloud and Container Security Platform

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Australia's Lacking Cybersecurity Workforce Results to a Influx in Attacks
* [WARNING] Micro Transactions Lead to a Drained Bank Account
* LinkedIn Phishing Attack Bypassed Email Filters Because it Passed Both SPF and DMARC Auth
* [EYE OPENER] Phishing Attacks 61% Up Over 2021. A Whopping 255 Million Attacks This Year So Far
* The Number of Vulnerabilities Associated with Ransomware Grows 426% Over Three Years
* Ransomware Attacks Via RDP Drop Significantly as Phishing Continues to Dominate
* Over Two-Thirds of Organizations Have No Ransomware-Specific Incident Response Playbook
* Your KnowBe4 Fresh Content Updates from October 2022
* Stolen Devices and Phishing
* [APPLY TODAY] Security Awareness Training Eligible for $185 Million DHS Cybersecurity Grant Opportuni

ISC2.org Blog

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

HackRead

* Why and how cyber security should be taken seriously
* New Dropper Apps on Play Store Targeting Banking and Crypto Wallets
* Researchers hack SpaceX Starlink satellite signal for GPS alternative
* GitHub fixes critical vulnerability that exposed repositories to attackers
* Chrome Extensions Harboring Dormant Colors Malware Infect Over a Million PCs
* See Tickets data breach went undetected for 2.5 years
* New Cryptojacking Campaign Kiss-a-dog Targeting Docker and Kubernetes

Koddos

* Why and how cyber security should be taken seriously
* New Dropper Apps on Play Store Targeting Banking and Crypto Wallets
* Researchers hack SpaceX Starlink satellite signal for GPS alternative
* GitHub fixes critical vulnerability that exposed repositories to attackers
* Chrome Extensions Harboring Dormant Colors Malware Infect Over a Million PCs
* See Tickets data breach went undetected for 2.5 years
* New Cryptojacking Campaign Kiss-a-dog Targeting Docker and Kubernetes

LATEST NEWS

Naked Security

* 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
* Clearview AI image-scraping face recognition service hit with â‚¬20m fine in France
* Apple megaupdate: Ventura out, iOS and iPad kernel zero-day - act now!
* Serious Security: How randomly (or not) can you shuffle cards?
* When cops hack back: Dutch police fleece DEADBOLT criminals (legally!)
* S3 Ep105: WONTFIX! The MS Office cryptofail that "isn't a security flaw" [Audio + Text]
* Women in Cryptology - USPS celebrates WW2 codebreakers

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

* The 7 Rs of cloud app modernization
* Some rain in the clouds
* 9 dark secrets of the federated web
* Deno runtime backs inlay hints for coding
* Oracle aligns GraalVM development with Java development
* 3 primo cloud gigs in 2023
* What is the JVM? Introducing the Java virtual machine
* Next.js 13 hones routing, layouts, rendering
* How to use BitArray in .NET 7
* Vaadin CEO: Developers are the architects of the future

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

* RC4 Is Still Considered Harmful
* The quantum state of Linux kernel garbage collection CVE-2021-0920 (Part I)

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.

* EKOPARTY CTF 2022
* WiCSME CTF 2022
* *POSTPONED* KalmarCTF 2022
* BuckeyeCTF 2022
* N1CTF 2022
* LakeCTF Finals
* p4ctf 2022
* Bambi CTF #7
* 4th stage MetaRed CTF Per&uacute; 2022
* HK Cyber Security New Generation CTF Challenge 2022

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

* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1
* Napping: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

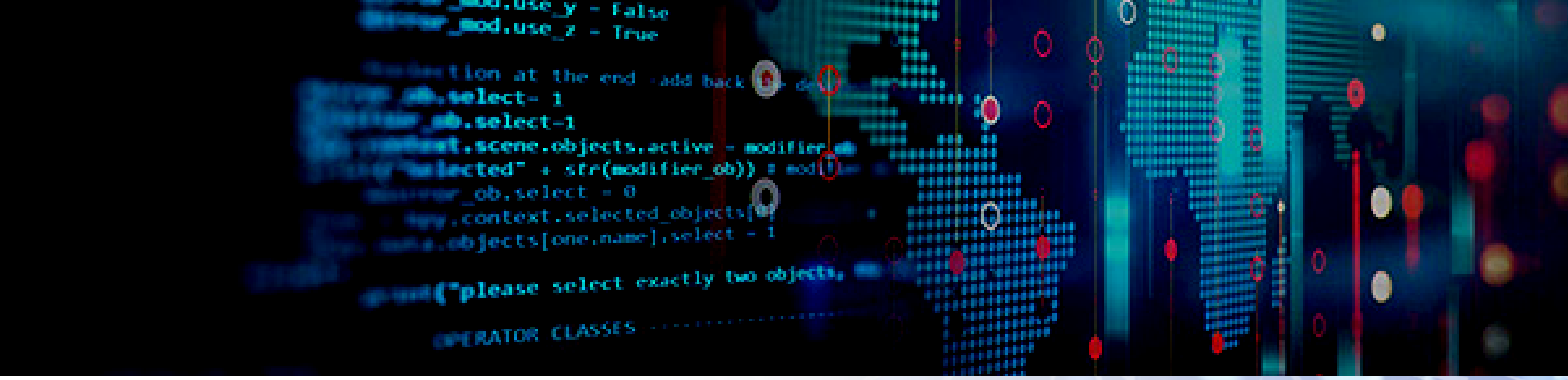
* Faraday 4.2.0
* Proxmark3 4.15864 Custom Firmware
* Zed Attack Proxy 2.12.0 Cross Platform Package
* GNUnet P2P Framework 0.18.0
* Wireshark Analyzer 4.0.1
* nfstream 6.5.3
* MutableSecurity 0.4.0
* Falco 0.33.0
* GNU Privacy Guard 2.3.8
* GNU Privacy Guard 2.2.40

Kali Linux Tutorials

* 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
* Matano : The Open-Source Security Lake Platform For AWS

GBHackers Analysis

* 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
* State-Sponsored Hackers Used MS Exchange 0-Day Bugs to Attack At least 10 Orgs



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown
* The Godfather of Forensics: How to Leverage Your "Year One" to Get an Offer You Cannot Refuse

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

* Live Hacking Q&A with Kody and Michael
* IoT Nutrition labels TBA 2023 - ThreatWire
* OMG Plug Elite

The PC Security Channel [TPSC]

* Is your PC hacked? RAM Forensics with Volatility
* GTA 6 Ransomware

Eli the Computer Guy

* YOUTUBE IS DEAD (Long Live YouTube)
* This bot will hunt... Louis Rossmann (paid for by paid off friends of big tech)
* Training Robots to hunt Louis Rossmann
* Training Terminator to Target LOUIS ROSSMANN (paid for by friends of apple)

Security Now

* Data Breach Responsibility - Firefox 106, KataOS and Sparrow, banking malware, CVSS 9.8 update
* Password Change Automation - Windows Update RSS, malicious kernal drivers, Signal SMS/MMS, ZimaBoard

Troy Hunt

* Weekly Update 319

Intel Techniques: The Privacy, Security, & OSINT Show

* 282-Major OSINT Updates

* 281-The Obsession Of Extreme Privacy

Proof of Concept (PoC) & Exploits

Packet Storm Security

* 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
* Chrome offline_items_collection::OfflineContentAggregator::OnItemRemoved Heap Buffer Overflow
* Fortinet FortiOS / FortiProxy / FortiSwitchManager Authentication Bypass
* Zimbra Privilege Escalation
* AVS Audio Converter 10.3 Stack Overflow
* MiniDVBLinux 5.4 Arbitrary File Read
* WordPress Photo Gallery 1.8.0 Cross Site Scripting
* MiniDVBLinux 5.4 Remote Root Command Execution

CXSecurity

* Siemens APOGEE PXC / TALON TC Authentication Bypass
* AVS Audio Converter 10.3 Stack Overflow
* MiniDVBLinux 5.4 Arbitrary File Read
* Mobile Mouse 3.6.0.4 Remote Code Execution (RCE)
* MiniDVBLinux 5.4 Remote Root Command Injection
* pfSense pfBlockerNG 2.1.4_26 Shell Upload
* Ubuntu 22.04.1 X64 Desktop Enlightenment 0.25.3-1 Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

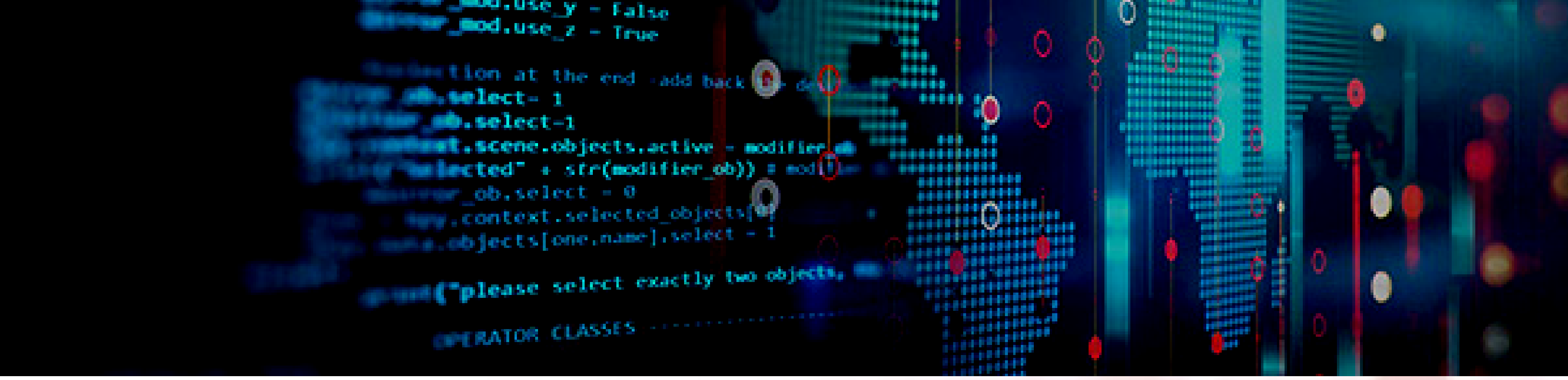
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [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

https://pn-lubuklinggau.go.id/license.txt

https://pn-lubuklinggau.go.id/license.txt notified by tegal9etar

https://sipp.pn-mandailingnatal.go.id/license.txt

https://sipp.pn-mandailingnatal.go.id/license.txt notified by tegal9etar

http://www.municipiodeyotoco.gov.co/kurd.html

http://www.municipiodeyotoco.gov.co/kurd.html notified by 0x1998

https://esperanza.gov.ar/3inawe.php

https://esperanza.gov.ar/3inawe.php notified by Einawe Hacker

https://tiwintza.gob.ec/kurd.html

https://tiwintza.gob.ec/kurd.html notified by 0x1998

https://sonsonantioquia.gov.co/kurd.html

https://sonsonantioquia.gov.co/kurd.html notified by 0x1998

https://gadmsmb.gob.ec/kurd.html

https://gadmsmb.gob.ec/kurd.html notified by 0x1998

https://munisanjorge.gob.gt/kz.html

https://munisanjorge.gob.gt/kz.html notified by Mr.Kro0oz.305

http://munisandiego.gob.gt/kz.html

http://munisandiego.gob.gt/kz.html notified by Mr.Kro0oz.305

https://muniimperial.gob.pe/kz.html

https://muniimperial.gob.pe/kz.html notified by Mr.Kro0oz.305

http://municabanaszacapa.gob.gt/kz.html

http://municabanaszacapa.gob.gt/kz.html notified by Mr.Kro0oz.305

https://munihuite.gob.gt/kz.html

https://munihuite.gob.gt/kz.html notified by Mr.Kro0oz.305

http://municipalidaddeusumatlan.gob.gt/kz.html

http://municipalidaddeusumatlan.gob.gt/kz.html notified by Mr.Kro0oz.305

http://muniteculutan.gob.gt/kz.html

http://muniteculutan.gob.gt/kz.html notified by Mr.Kro0oz.305

https://balochistan.gob.pk/license.txt

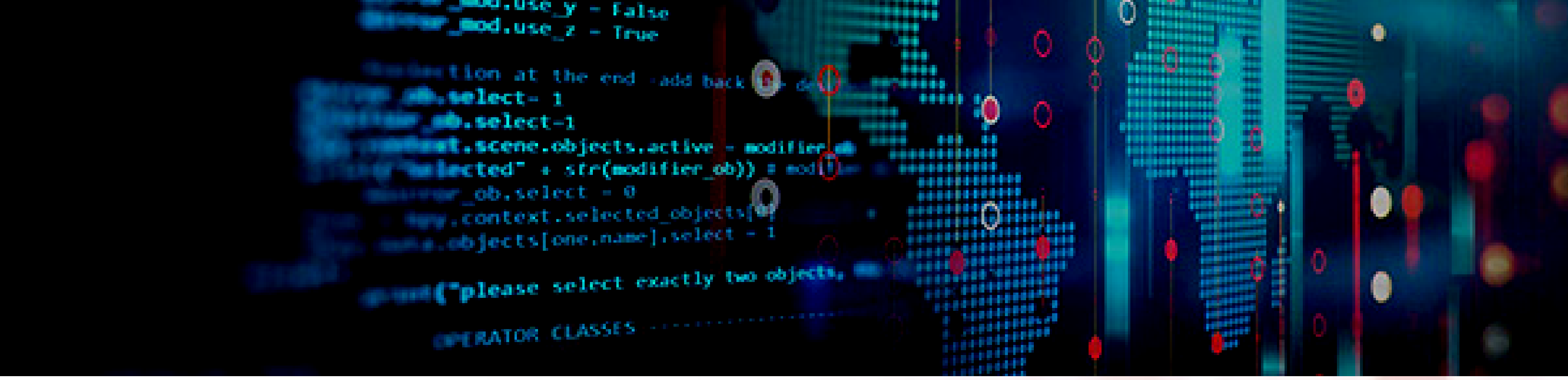
https://balochistan.gob.pk/license.txt notified by tegal9etar

https://www.finance.gob.pk/licenza.txt

https://www.finance.gob.pk/licenza.txt notified by tegal9etar

https://dinkes.demakkab.go.id/readme.html

https://dinkes.demakkab.go.id/readme.html notified by AnonSec Team


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_ob
lected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Dark Web News

Darknet Live

Florida Man Convicted of Using Crypto Mixers to Evade Taxes

A Florida man admitted using "sophisticated online techniques&rdquo; to conceal more than $1 million in cryptocurrency from the IRS. Ethan Thomas Trainor pleaded guilty to attempted tax evasion. According to information revealed in court and a proffer statement, Trainor sold hacked online accounts on darkweb markets in exchange for cryptocurrency. He used mixers in an attempt to obscure the source of the funds. Trainor then underreported his earnings to the IRS by filing tax returns that underrepresented his earnings. For example, according to a criminal information, Trainor filed a tax return in 2015 that was short by $181,933. As a result, the filing resulted in a "loss&rdquo; to the federal government of $40,846. The underreported amounts Trainor admitted that he filed similar tax returns multiple times, resulting in a total "loss&rdquo; to the federal government of $238,894. From the proffer statement: "Ethan TRAINOR bought and sold hacked online account login (usemames and passwonis) for movie streaming websites such as Netflix, pornography websites, Spotify, Major Sports websites, laming websites, and Uber accounts through various dark net markets. TRAINOR illegally obtained these usemames and passwords using various methods, from hacking the accounts himself to buying the hacked usernames and passwords. These darknet markets that TRAINOR operated on are specifically designed to facilitate illegal commerce and provide anonymity through user concealment and by employing numerous financial obfuscation techniques. Agents were able to successfully trace the virtual flow of cryptocurrency proceeds from TRAINOR's sales on various blockchains to numerous mixing and cash-out services.&rdquo; Very serious IRS-CI agents in training There is virtually no information on how investigators tracked Trainor's activities. Perhaps they flagged him for tax evasion and worked backward from there. He faces up to five years in prison and is scheduled to be sentenced in December. Non-Payment of Federal Income Tax on Cryptocurrency Earnings Leads to Conviction for South Florida Resident | www.justice.gov, archive.is, archive.org Statement The last thing you see (via darknetlive.com at https://darknetlive.com/post/florida-man-convicted-of-attempted-tax-evasion/)

US Government Calls for More Cryptocurrency Regulation

Once again, the federal government is calling for more cryptocurrency rules and regulations. The Financial Stability Oversight Council released a report on Digital Asset Financial Stability Risks and Regulation. The report is a response to Section 6 of President Biden's Executive Order 14067 on "Ensuring Responsible Development of Digital Assets.&rdquo; The Council is one of many government bodies with reports calling for the same thing: regulation directed at cryptocurrency. Financial stability risks Crypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulation, including enforcement of the existing regulatory structure. The scale of crypto-asset activities has increased significantly in recent years. Although interconnections with the traditional financial system are currently relatively limited, they could potentially increase rapidly. Participants in the crypto-asset ecosystem and the traditional financial system have explored or created a variety of interconnections. Notable sources of potential interconnections include traditional assets held as part of stablecoin activities. Cryptoasset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access cryptoasset activities, including through certain traditional money services businesses. Some characteristics of crypto-asset activities have acutely amplified instability within the crypto-asset ecosystem.   Many crypto-asset activities lack basic risk controls to protect against run risk or to help ensure that leverage is not excessive. Crypto-asset prices appear to be primarily driven by speculation rather than grounded in current fundamental economic use cases, and prices have repeatedly recorded significant and broad declines. Many crypto-asset firms or activities have sizable interconnections with crypto-asset entities that have risky business profiles and opaque capital and liquidity positions. In addition, despite the distributed nature of crypto-asset systems, operational risks may arise from the concentration of key services or from vulnerabilities related to distributed ledger technology.   These vulnerabilities are partly attributable to the choices made by market participants, including crypto-asset issuers and platforms, to not implement or refuse to implement appropriate risk controls, arrange for effective governance, or take other available steps that would address the financial stability risks of their activities. __ Correlations between Bitcoin Prices and Equity Prices   Enforcement of the existing regulatory structure _ Many nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated. Firms often emphasize money services business regulation, though such regulation is largely focused on anti-money laundering controls or consumer protection requirements and does not provide a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities that may be undertaken, for example, by a trading platform or stablecoin issuer. While some firms in the crypto-asset ecosystem have attempted to avoid the existing regulatory system, other firms have engaged with the existing regulatory system by obtaining trust charters or special state-level crypto-asset-specific charters or licenses.   Compliance with and enforcement of the existing regulatory structure is a key step in addressing financial stability risks. For example, certain crypto-asset platforms may be listing securities but are not in compliance with exchange or broker-dealer registration requirements. In addition, certain crypto-asset issuers have offered and sold crypto-assets in violation of federal and state securities laws, because the offering and sale were not registered or conducted pursuant to an available exemption. Regulators have taken enforcement actions over the past several years to address many additional instances of non-compliance with existing rules and regulations, including illegally offered crypto-asset derivatives products, false statements about stablecoin assets, and many episodes of fraud and market manipulation. In addition, false and misleading statements, made directly or by implication, concerning availability of federal deposit insurance for a given product, are violations of the law, and have given customers the impression that they are protected by the government safety net when they are not. Further, misrepresentations by crypto-asset firms about how they are regulated have also confused consumers and investors regarding whether a given crypto-asset product is regulated to the same extent as other financial products.   Regulatory Gaps _ Though the existing regulatory system covers large parts of the crypto-asset ecosystem, this report identifies three gaps in the regulation of crypto-asset activities in the United States. First, the spot markets for crypto-assets that are not securities are subject to limited direct federal regulation. As a result, those markets may not feature robust rules and regulations designed to ensure orderly and transparent trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly. Second, crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage. Some crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, and no single regulator may have visibility into the risks across the entire business. Third, a number of crypto-asset trading platforms have proposed offering retail customers direct access to markets by vertically integrating the services provided by intermediaries such as broker-dealers or futures commission merchants. Financial stability and investor protection implications may arise from retail investors' exposure to certain practices commonly proposed by vertically integrated trading platforms, such as automated liquidation.   Recommendations _ The Council notes that large parts of the crypto-asset ecosystem are covered by the existing regulatory structure. In applying these existing authorities, the Council recommends that its members take into consideration a set of principles and emphasizes the importance of continued enforcement of existing rules and regulations.   To address regulatory gaps, the Council recommends: the passage of legislation providing for rulemaking authority for federal financial regulators over the spot market for crypto-assets that are not securities; steps to address regulatory arbitrage including coordination, legislation regarding risks posed by stablecoins, legislation relating to regulators' authorities to have visibility into, and otherwise supervise, the activities of all of the affiliates and subsidiaries of cryptoasset entities, and appropriate service provider regulation; and study of potential vertical integration by crypto-asset firms.   Finally, the Council recommends bolstering its members' capacities related to data and to the analysis, monitoring, supervision, and regulation of crypto-asset activities. The Council appears to be targeting legitimate concerns, such as companies committing securities fraud. Of course, securities fraud is already illegal. The full report can be viewed here. (via darknetlive.com at https://darknetlive.com/post/government-calls-for-more-cryptocurrency-regulation/)

Binance Announces Law Enforcement Training Program

The cryptocurrency exchange Binance announced the launch of a law enforcement training program. Binance, like most other cryptocurrency exchanges and blockchain analytics companies, employs former federal law enforcement officers. These former feds work closely with current feds in many ways, including information sharing and "training programs.&rdquo; The press release: Over the past year, the Binance Investigations team has conducted and participated in more than 30 workshops on countering cyber and financial crime, engaging law enforcement officers in Argentina, Brazil, Canada, France, Germany, Israel, Netherlands, Philippines, Sweden, South Korea, and the UK, among others.   "As more regulators, public law enforcement agencies, and private sector stakeholders look closely at crypto, we are seeing an increased demand for training to help educate on and combat crypto crimes,&rdquo; said Tigran Gambaryan, Global Head of Intelligence and Investigations at Binance. "To meet that demand, we have bolstered our team to conduct more training and work hand-in-hand with regulators across the globe.&rdquo;

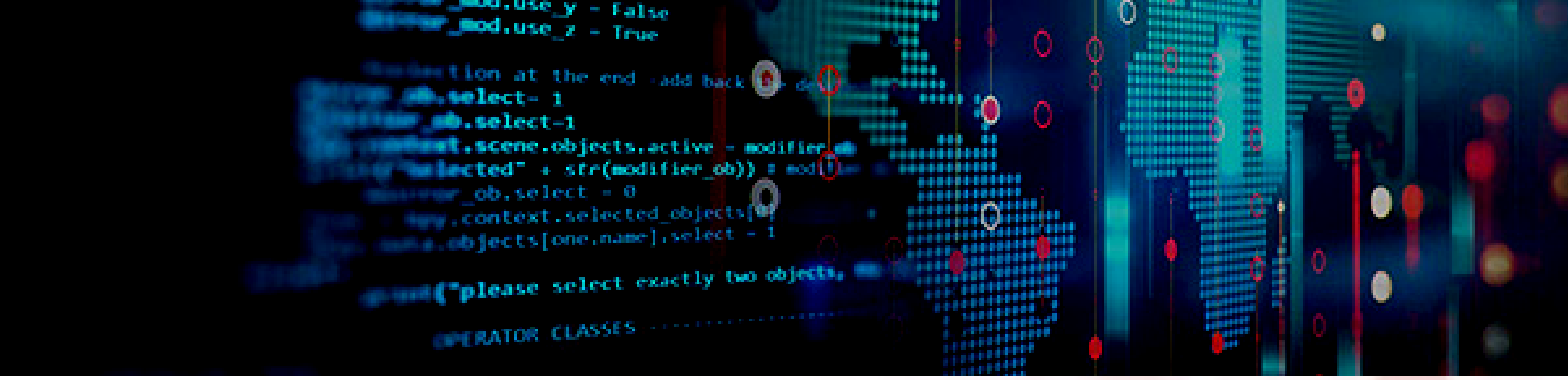
Binance   The training program is led by world-class practitioners from the Binance Investigations team, which employs security experts and former law enforcement agents, including analysts and operatives who had helped take down some of the world's largest criminal platforms, such as Silk Road and Hydra.   The standard one-day training program includes in-person workshops on the fundamental concepts of blockchain and crypto assets, as well as insight into the evolving legal and regulatory environment they operate in. Binance's anti-money laundering (AML) policies and the investigative methods developed by the company to detect and prevent criminal behavior are also discussed in detail.   As a result of deploying robust compliance and AML programs, Binance has recently secured approvals and registrations in France, Italy, and Spain, among others, making the exchange one of the few crypto companies to accomplish this within G7 countries.   "Protecting users is our number one priority at Binance. We work hand-in-hand with law enforcement to track and trace suspected accounts and fraudulent activities, contributing to the fight against terrorism financing, ransomware, human trafficking, child pornography, and financial crimes," said Gambaryan, a former special agent of the Internal Revenue Service&mdash;Criminal Investigation (IRS-CI) Cyber Crimes Unit.   Since November 2021, the Binance Investigations team has responded to more than 27,000 law enforcement requests with an average of three days response time, which is faster than any traditional financial institution.   "Binance is known among law enforcement to have a fast response system, unmatched by any traditional financial institution,&rdquo; said Gambaryan.   Amid Growing Demand, Binance Boosts its Global Law Enforcement Training Program | www.binance.com, archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/binance-announces-new-law-enforcement-training-program/)

US Government Working on AI-Powered Stylometry Technology

The Intelligence Advanced Research Projects Activity (IARPA) is working on a program that will use "artificial intelligence technologies capable of attributing authorship.&rdquo; Put another way: the government is creating a program that uses artificial intelligence to identify or fingerprint anonymous authors. IARPA is the research and development arm of the Office of the Director of National Intelligence (ODNI).

Office of the Director of National Intelligence   "Each of the selected performers brings a unique, novel, and compelling approach to the HIATUS challenge,&rdquo; said program manager Dr. Tim McKinnon. "We have a strong chance of meeting our goals, delivering much-needed capabilities to the Intelligence Community, and substantially expanding our understanding of variation in human language using the latest advances in computational linguistics and deep learning.&rdquo; The DNI press release: "WASHINGTON, D.C. - The Intelligence Advanced Research Projects Activity (IARPA), the research and development arm of the Office of the Director of National Intelligence, today announced the launch of a program that seeks to engineer novel artificial intelligence technologies capable of attributing authorship and protecting authors' privacy.&rdquo;   "The Human Interpretable Attribution of Text Using Underlying Structure (HIATUS) program represents the Intelligence Community's latest research effort to advance human language technology. The resulting innovations could have far-reaching impacts, with the potential to counter foreign malign influence activities; identify counterintelligence risks; and help safeguard authors who could be endangered if their writing is connected to them.&rdquo;   The program's goals are to create technologies that: Perform multilingual authorship attribution by identifying stylistic features &mdash; such as word choice, sentence phrasing, organization of information &mdash; that help determine who authored a given text. Protect the author's privacy by modifying linguistic patterns that indicate the author's identity. Implement explainable AI techniques that provide novice users an understanding, trust, and verification as to why a particular text is attributable to a specific author or why a particular revision will preserve an author's privacy.   "Through a competitive Broad Agency Announcement, IARPA awarded HIATUS research contracts to the following lead organizations, which together bring more than 20 academic institutions, non-profits, and businesses into the program: Charles River Analytics, Inc. Leidos, Inc. Raytheon BBN SRI International University of Pennsylvania University of Southern California   "The HIATUS test and evaluation team consists of Lawrence Livermore National Labs, Pacific Northwest National Labs, and the University of Maryland Applied Research Laboratory for Intelligence and Security.&rdquo;   \   IARPA Kicks off Research Into Linguistic Fingerprint Technology | www.dni.gov, archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/dni-funding-stylometry-project/)

Dark Web Link



Trend Micro Anti-Malware Blog

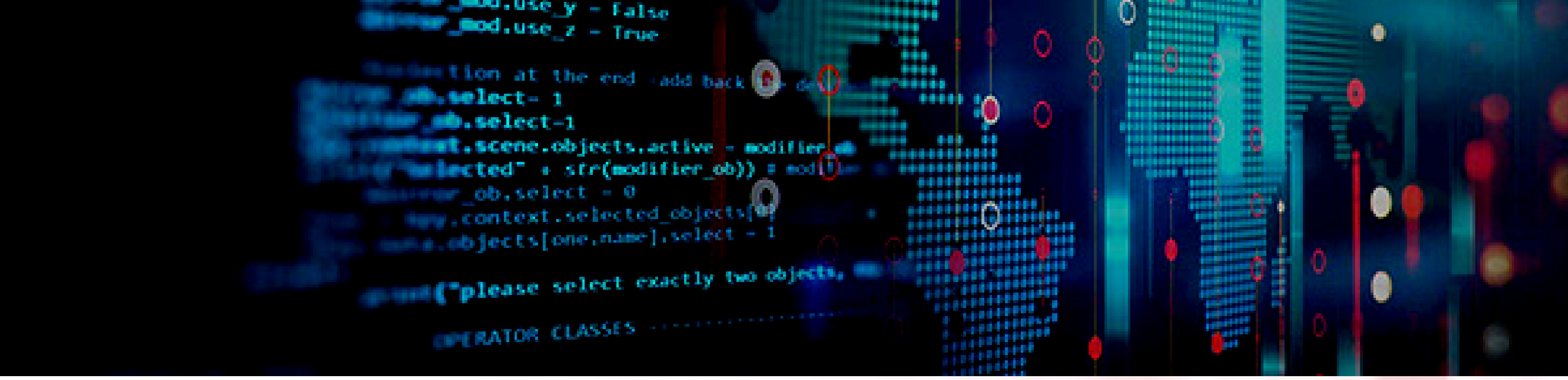
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* 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
* [Security Nation] Jeremi Gosney on the Psychology of Password Hygiene
* Hands-On IoT Hacking: Rapid7 at DEF CON 30 IoT Village, Pt. 2
* Adapting existing VM programs to regain control
* Metasploit Weekly Wrap-Up
* New Research: We're Still Terrible at Passwords; Making it Easy for Attackers
* [The Lost Bots] S02E05: The real magic in the Magic Quadrant


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

Advisories

US-Cert Alerts & bulletins

* [CISA Has Added One Known Exploited Vulnerability to Catalog]
* [Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies]
* [VMware Releases Security Updates]
* [CISA Releases Four Industrial Control Systems Advisories]
* [Apple Releases Security Updates for Multiple Products]
* [Samba Releases Security Updates]
* [CISA Has Added One Known Exploited Vulnerability to Catalog&#8239;&#8239;&#8239;]
* [CISA Releases Eight Industrial Control Systems Advisories]
* [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 17, 2022]
* [Vulnerability Summary for the Week of October 10, 2022]

Zero Day Initiative Advisories

ZDI-CAN-19053: Delta Electronics
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19277: Delta Electronics
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19279: Delta Electronics
A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19280: Delta Electronics
A CVSS score 7.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19276: Delta Electronics
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days

ago. The vendor is given until 2023-02-28 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-18590: Fortinet

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Ting' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19286: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19287: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19307: Microsoft

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19285: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19284: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19291: 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: 2022-10-31, 0 days ago. The vendor is given until 2023-02-28 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-19354: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19323: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19352: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19300: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19295: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19309: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19310: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19312: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19296: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19299: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19324: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 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-19297: 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: 2022-10-28, 3 days ago. The vendor is given until 2023-02-25 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Debian Security Advisory 5267-1
Debian Linux Security Advisory 5267-1 - Nicky Mouha discovered a buffer overflow in 'sha3', a Python library for the SHA-3 hashing functions.
Gentoo Linux Security Advisory 202210-32
Gentoo Linux Security Advisory 202210-32 - An integer overflow has been found in hiredis which could result in arbitrary code execution. Versions less than 1.0.1 are affected.
Debian Security Advisory 5266-1
Debian Linux Security Advisory 5266-1 - A heap use-after-free vulnerability after overeager destruction of a shared DTD in the XML_ExternalEntityParserCreate function in Expat, an XML parsing C library, may result in denial of service or potentially the execution of arbitrary code.
Apple Security Advisory 2022-10-27-15
Apple Security Advisory 2022-10-27-15 - Safari 16.1 addresses code execution, spoofing, and use-after-free vulnerabilities.
Gentoo Linux Security Advisory 202210-31
Gentoo Linux Security Advisory 202210-31 - Multiple vulnerabilities have been discovered in OpenEXR, the worst of which could result in arbitrary code execution. Versions less than 3.1.5 are affected.
Debian Security Advisory 5265-1
Debian Linux Security Advisory 5265-1 - Several security vulnerabilities have been discovered in the Tomcat servlet and JSP engine.
Apple Security Advisory 2022-10-27-14
Apple Security Advisory 2022-10-27-14 - Safari 16 addresses buffer overflow, code execution, out of bounds read, and spoofing vulnerabilities.
Gentoo Linux Security Advisory 202210-30
Gentoo Linux Security Advisory 202210-30 - Multiple vulnerabilities have been discovered in the Xorg Server and XWayland, the worst of which can result in remote code execution. Versions less than 21.1.4 are affected.
Red Hat Security Advisory 2022-7261-01
Red Hat Security Advisory 2022-7261-01 - OpenShift API for Data Protection enables you to back up and restore application resources, persistent volume data, and internal container images to external backup storage. OADP enables both file system-based and snapshot-based backups for persistent volumes. Issues addressed include a denial of service vulnerability.
Apple Security Advisory 2022-10-27-13
Apple Security Advisory 2022-10-27-13 - watchOS 9 addresses buffer overflow, bypass, code execution, out of bounds read, out of bounds write, spoofing, and use-after-free vulnerabilities.
Gentoo Linux Security Advisory 202210-29
Gentoo Linux Security Advisory 202210-29 - Multiple vulnerabilities have been discovered in Net-SNMP, the worst of which could result in denial of service. Versions less than 5.9.2 are affected.
Apple Security Advisory 2022-10-27-12
Apple Security Advisory 2022-10-27-12 - watchOS 9.1 addresses code execution, out of bounds write, and spoofing vulnerabilities.
Debian Security Advisory 5264-1
Debian Linux Security Advisory 5264-1 - It was discovered that Apache Batik, a SVG library for Java, allowed attackers to run arbitrary Java code by processing a malicious SVG file.
Red Hat Security Advisory 2022-7257-01
Red Hat Security Advisory 2022-7257-01 - A minor version update is now available for Red Hat Camel K that includes CVE fixes in the base images. Details are linked in the References section.
Gentoo Linux Security Advisory 202210-28
Gentoo Linux Security Advisory 202210-28 - A vulnerability has been discovered in exif which could result in denial of service. Versions less than 0.6.22 are affected.

Gentoo Linux Security Advisory 202210-27

Gentoo Linux Security Advisory 202210-27 - A vulnerability has been discovered in open-vm-tools which could allow for local privilege escalation. Versions less than 12.1.0 are affected.

Red Hat Security Advisory 2022-7191-01

Red Hat Security Advisory 2022-7191-01 - The device-mapper-multipath packages provide tools that use the device-mapper multipath kernel module to manage multipath devices. Issues addressed include a bypass vulnerability.

Apple Security Advisory 2022-10-27-11

Apple Security Advisory 2022-10-27-11 - tvOS 16 addresses buffer overflow, code execution, out of bounds read, out of bounds write, spoofing, and use-after-free vulnerabilities.

Gentoo Linux Security Advisory 202210-26

Gentoo Linux Security Advisory 202210-26 - A TOCTOU race has been discovered in Shadow, which could result in the unauthorized modification of files. Versions less than 4.12.2 are affected.

Gentoo Linux Security Advisory 202210-25

Gentoo Linux Security Advisory 202210-25 - Multiple vulnerabilities have been discovered in ISC BIND, the worst of which could result in denial of service. Versions less than 9.16.33 are affected.

Apple Security Advisory 2022-10-27-10

Apple Security Advisory 2022-10-27-10 - tvOS 16.1 addresses code execution, out of bounds write, and spoofing vulnerabilities.

Apple Security Advisory 2022-10-27-9

Apple Security Advisory 2022-10-27-9 - macOS Big Sur 11.7 addresses buffer overflow, bypass, code execution, out of bounds write, and use-after-free vulnerabilities.

Gentoo Linux Security Advisory 202210-24

Gentoo Linux Security Advisory 202210-24 - Multiple vulnerabilities have been found in FreeRDP, the worst of which could result in remote code execution. Versions less than 2.8.1 are affected.

Gentoo Linux Security Advisory 202210-23

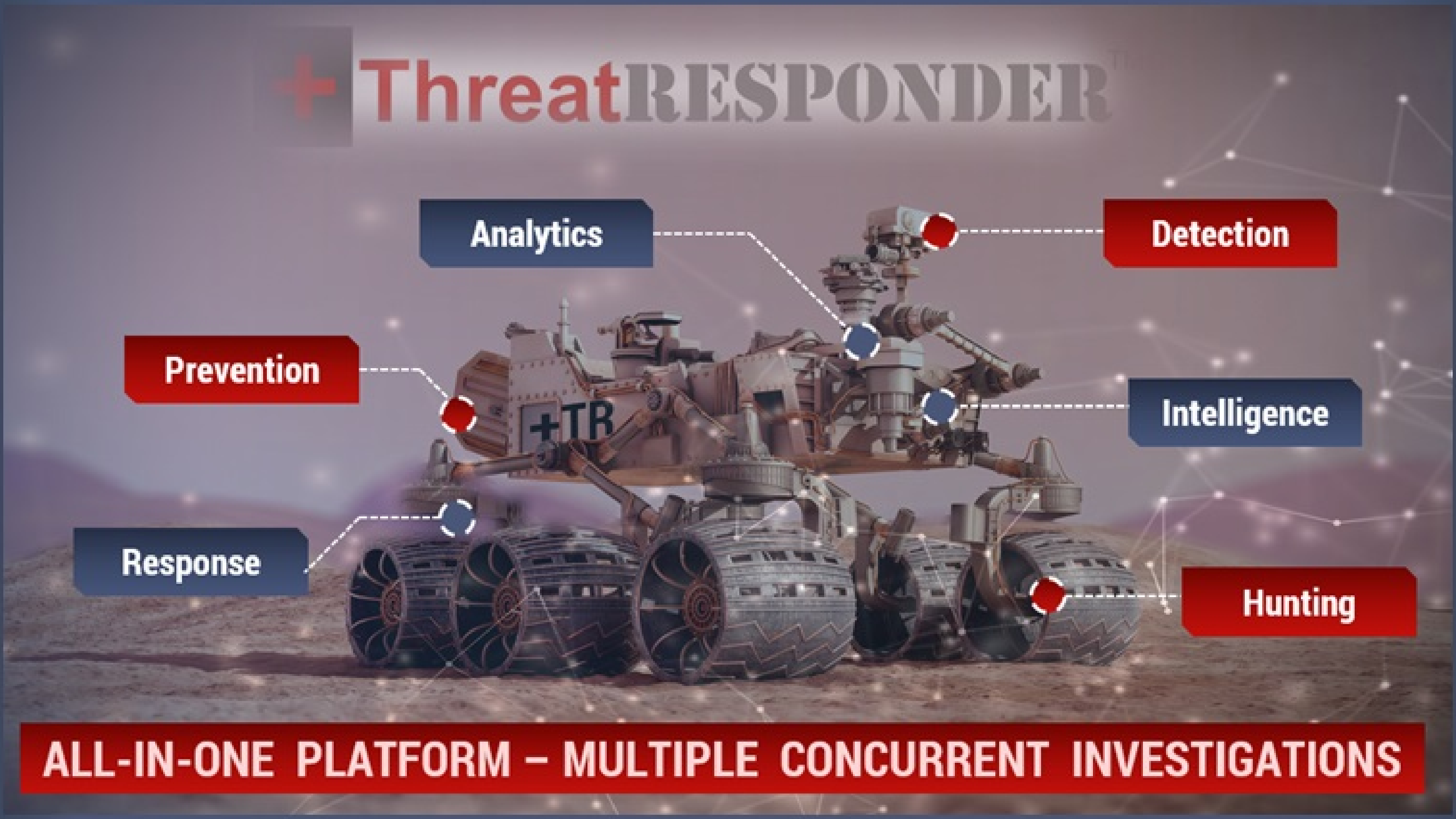
Gentoo Linux Security Advisory 202210-23 - An integer overflow vulnerability has been found in libksba which could result in remote code execution. Versions less than 1.6.2 are affected.

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



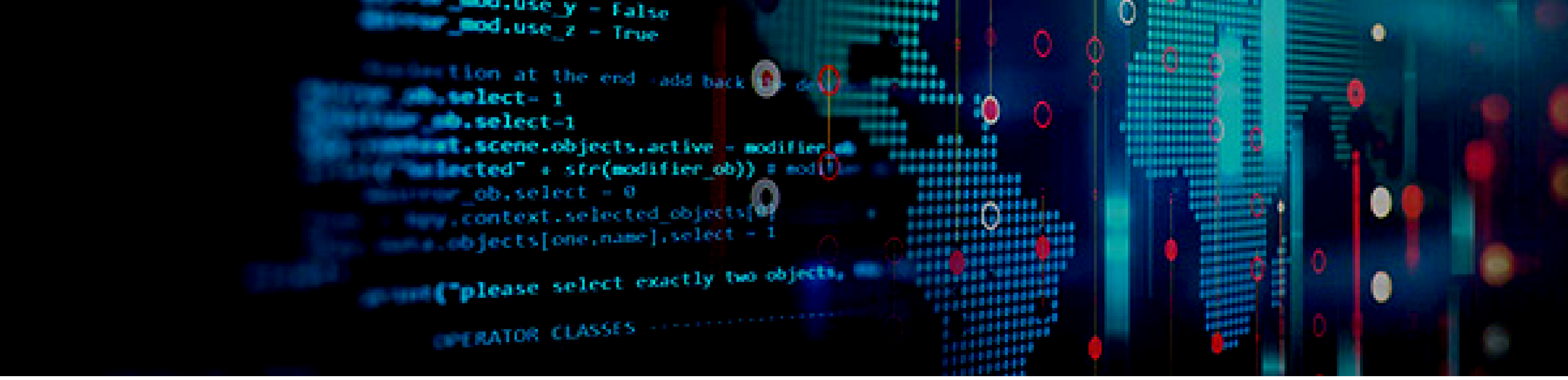
The Solution – ThreatResponder® Platform

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

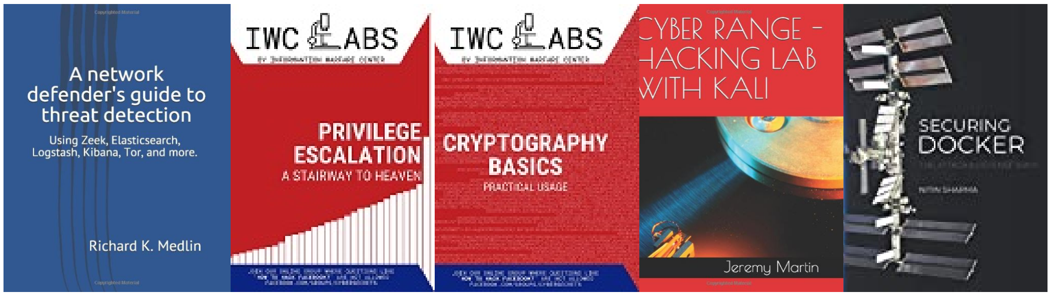


The Cyber Secrets publications on Amazon

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

Si LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP