Oct-17-22

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®

October 17, 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

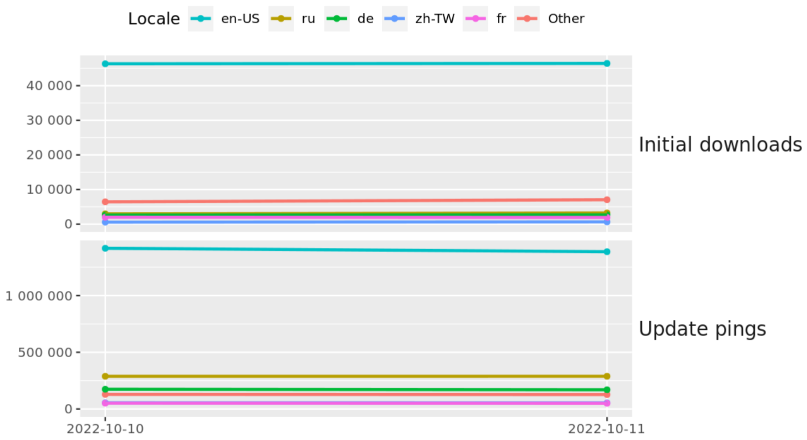
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* Equifax Surveilled 1,000 Remote Workers, Fired 24 Found Juggling Two Jobs
* Samsung Brings Blockchain Based Security To Smart Devices
* Shein Owner Zoetop Fined $1.9m Over Data Breach Response
* How Mudge Upended One Of The World's Most Influential Social Networks
* Data Of 380K Patients Compromised In Hack Of 13 Anesthesia Practices
* Insurer Medibank Hit By Targeted Cyberattack
* Financial Watchdogs Have An Interest In Trader Talk On WhatsApp
* Prison Inmate Accused Of Orchestrating $11M Fraud Using Cellphone
* How Wi-Fi Spy Drones Snooped On Financial Firm
* Bittrex Coughs Up $53m To End Claims Of US Sanctions Busting
* NASA's DART Spacecraft Successfully Moved An Asteroid
* Microsoft Patch Tuesday: 84 New Vulnerabilities
* Google Makes Major Play For Cloud Security Market
* iPhones Calling 911 From Owners' Pockets On Rollercoasters
* Fortinet Warns Of Critical Flaw In Its Security Appliance OSes, Admin Panels
* Meta Uncovers 400 Malicious Apps On Android And iOS
* Singtel Confirms Digital Burglary At Dialog Subsidiary
* Unpatched Zimbra Flaw Lets Hackers Backdoor Servers
* New macOS Vuln Lets Malicious Apps Bypass Security Checks
* Protests In Iran: State-Run Live TV Hacked By Protestors
* Biden Signs Order For EU - U.S. Data Privacy Framework
* 2K Warns Users Their Info Was Stolen Due To A Help Desk Breach
* Binance Says $100 Million Of Crypto Produced Out Of Thin Air By Hackers
* Feds Ink $26 Million Contract For Deception Platform For Defense
* NetWalker Ransomware Scumbag Jailed For 20 Years

Krebs on Security

* 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
* Botched Crypto Mugging Lands Three U.K. Men in Jail
* Say Hello to Crazy Thin 'Deep Insert' ATM Skimmers

LATEST NEWS

Dark Reading

* What Fast-Talkers Can Teach Us About Vetting Vendors
* Disinformation Attacks Threaten US Midterm Elections
* 4 Stakeholders Critical to Addressing the Cybersecurity Workforce Gap
* Imprivata Expands Its Integrated Digital Identity Platform to Defragment Identities Across Disparate
* Microsoft Secures Azure Enclaves With Hardware Guards
* Concerns Over Fortinet Flaw Mount; PoC Released, Exploit Activity Grows
* Apple's Constant Battles Against Zero-Day Exploits
* Fast Fashion Retailer Data Breach Draws $1.9M Fine
* Microsoft 365 Message Encryption Can Leak Sensitive Info
* Acuity Reports Increase in Cyber Liability Insurance Claims as Cybercrime Skyrockets
* Care and Feeding of the SOC's Most Powerful Tool: Your Brain
* Juice Technology Receives ISO Certification for Charging Station Cyber Security
* ControlMap Announces the Launch of the Trust Portal, Creating Transparency in Cybersecurity Complianc
* Quarter of Healthcare Ransomware Victims Forced to Halt Operations
* Armis Now Available on Google Cloud Marketplace
* Google Cloud Advances Partnerships with 20-Plus Software Companies Focused on Digital Sovereignty and
* HSBC and Silent Eight Expand Machine Learning Partnership
* Nexusguard Research Shows Total Number of DDoS Attacks Increased during First Half of 2022 While Maxi
* Resistant AI and ComplyAdvantage Launch AI Transaction Monitoring Solution To Combat Fraud and Money
* Newly Introduced HackerOne Assets Goes Beyond Attack Surface Management To Close Security Gaps

The Hacker News

* Black Basta Ransomware Hackers Infiltrates Networks via Qakbot to Deploy Brute Ratel C4
* Researchers Say Microsoft Office 365 Uses Broken Email Encryption to Secure Messages
* Why Crypto Winter is No Excuse to Let Your Cyber Defenses Falter
* New Prestige Ransomware Targeting Polish and Ukrainian Organizations
* Zimbra Releases Patch for Actively Exploited Vulnerability in its Collaboration Suite
* INTERPOL-led Operation Takes Down 'Black Axe' Cyber Crime Organization
* Indian Energy Company Tata Power's IT Infrastructure Hit By Cyber Attack
* Researchers Detail Windows Zero-Day Vulnerability Patched Last Month
* New Chinese Cyberespionage Group Targeting IT Service Providers and Telcos
* New PHP Version of Ducktail Malware Hijacking Facebook Business Accounts
* How To Build a Career as a Freelance Cybersecurity Analyst - From Scratch
* Mirai Botnet Hits Wynncraft Minecraft Server with 2.5 Tbps DDoS Attack
* PoC Exploit Released for Critical Fortinet Auth Bypass Bug Under Active Attacks
* New Chinese Malware Attack Framework Targets Windows, macOS, and Linux Systems
* New Timing Attack Against NPM Registry API Could Expose Private Packages

LATEST NEWS

Security Week

* Retail Giant Woolworths Discloses Data Breach Impacting 2.2 Million MyDeal Customers
* New 'Prestige' Ransomware Targets Transportation Industry in Ukraine, Poland
* Fortinet Admits Many Devices Still Unprotected Against Exploited Vulnerability
* 75 Arrested in Crackdown on West-African Cybercrime Gangs
* New 'Black Lotus' UEFI Rootkit Provides APT-Level Capabilities to Cybercriminals
* Cybersecurity M&A Roundup for October 1-15, 2022
* Flaw in Microsoft OME Could Lead to Leakage of Encrypted Data
* Timing Attacks Can Be Used to Check for Existence of Private NPM Packages
* IronVest Emerges From Stealth Mode With $23 Million in Seed Funding
* New 'Alchimist' Attack Framework Targets Windows, Linux, macOS
* Seven 'Creepy' Backdoors Used by Lebanese Cyberspy Group in Israel Attacks
* BAE Releases New Cybersecurity System for F-16 Fighter Aircraft
* PoC Published for Fortinet Vulnerability as Mass Exploitation Attempts Begin
* Austria's Kurz Sets up Cyber Firm With Ex-NSO Chief
* DataGrail Raises $45 Million for Data Privacy Platform
* Mirai Botnet Launched 2.5 Tbps DDoS Attack Against Minecraft Server
* New Chinese Cyberespionage Group WIP19 Targets Telcos, IT Service Providers
* Google Brings Passkey Support to Android and Chrome
* Palo Alto Networks, Aruba Patch Severe Vulnerabilities
* Chinese Cyberspies Targeting US State Legislature
* Anticipation and Action: What's Next in SOC Modernization
* Vista Equity Partners to Acquire Security Awareness Training Firm KnowBe4 for $4.6B
* Immersive Labs Raises $66 Million for Cyber Workforce Resilience Platform
* Malwarebytes Launches MDR Solution for SMBs
* Chrome 106 Update Patches Several High-Severity Vulnerabilities
* QBot Malware Infects Over 800 Corporate Users in New, Ongoing Campaign

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Sloppy but Dangerous: Fake Ransomware
* Cyberattacks are the biggest risk to the UK financial system - Bank of England research
* New Phishing Campaign Uses Office Docs to Install Cobalt Strike Beacon
* Cyber-Zombie Apocalypse: Ransomware Gangs Continue to Come Back from the Dead
* German Hackers Arrested for Stealing â‚¬4 Million in 7-Month Banking Phishing Scams
* Small Business Grants as Phishbait
* Scams, Scams, Everywhere!
* A New Phishing-as-a-Service Kit
* 79 Million Malicious Domains Flagged in the First Half of 2022
* Three-Quarters of Ethical Hackers Can Collect and (Potentially) Exfiltrate Data in 10 Hours or Less

ISC2.org Blog

* #ISC2Congress 2022: Highlighting the Need for Collaborative Defense
* #ISC2Congress 2022: Ian Bremmer - Is Technology the New World Order?
* No work experience? Don't let that stop you from pursuing a career in cybersecurity
* #ISC2CONGRESS 2022: Panel: Why Apprenticeships Matter
* #ISC2Congress 2022: Effective Cybersecurity Takes Collaboration

HackRead

* Dutch Police Tricked Deadbolt Ransomware Gang Into Sharing Decryption Keys
* 6 Best Ways to Make a Collaborative PowerPoint Presentation
* How to make decentralized apps: Modern subtleties of development process management
* Rising Bot Attacks - Why is Your Organization Struggling to Deal with Them?
* Encrypted Email Service ProtonMail Now Supports Physical Security Keys
* Linux, Windows and macOS Hit By New "Alchimist" Attack Framework
* How web data is leading US cybersecurity to unreached possibilities

Koddos

* Dutch Police Tricked Deadbolt Ransomware Gang Into Sharing Decryption Keys
* 6 Best Ways to Make a Collaborative PowerPoint Presentation
* How to make decentralized apps: Modern subtleties of development process management
* Rising Bot Attacks - Why is Your Organization Struggling to Deal with Them?
* Encrypted Email Service ProtonMail Now Supports Physical Security Keys
* Linux, Windows and macOS Hit By New "Alchimist" Attack Framework
* How web data is leading US cybersecurity to unreached possibilities

LATEST NEWS

Naked Security

* Serious Security: Microsoft Office 365 attacked over feeble encryption
* S3 Ep104: Should hospital ransomware attackers be locked up for life? [Audio + Text]
* Patch Tuesday in brief - one 0-day fixed, but no patches for Exchange!
* Move over Patch Tuesday - it's Ada Lovelace Day!
* Mystery iPhone update patches against iOS 16 mail crash-attack
* Serious Security: OAuth 2 and why Microsoft is finally forcing you into it
* WhatsApp goes after Chinese password scammers via US court
* S3 Ep103: Scammers in the Slammer (and other stories) [Audio + Text]
* Former Uber CSO convicted of covering up megabreach back in 2016
* NetWalker ransomware affiliate sentenced to 20 years by Florida court

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 cloud has a people problem
* The best open source software of 2022
* Get ready for the metaverse
* Java needs sequenced collections, OpenJDK proposal says
* Get used to cloud vendor lock-in
* 12 top-notch libraries for C++ programming
* What is Kotlin? The Java alternative explained
* Ant Group lists OceanBase on AWS Marketplace to increase reach
* Use model validation in minimal APIs in ASP.NET Core 6
* Natural language processing with Apache OpenNLP

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

* The quantum state of Linux kernel garbage collection CVE-2021-0920 (Part I)
* 2022 0-day In-the-Wild Exploitation&hellip;so far

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.

* 3rd stage MetaRed CTF Mexico|Anuies-TIC 2022
* Jade CTF
* EyesOpen CTF
* Cryptoverse CTF 2022
* TsukuCTF 2022
* Hack The Boo
* Phoenix CTF
* FE-CTF 2022: Cyber Demon
* Hack.lu CTF 2022
* BlueHens CTF 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

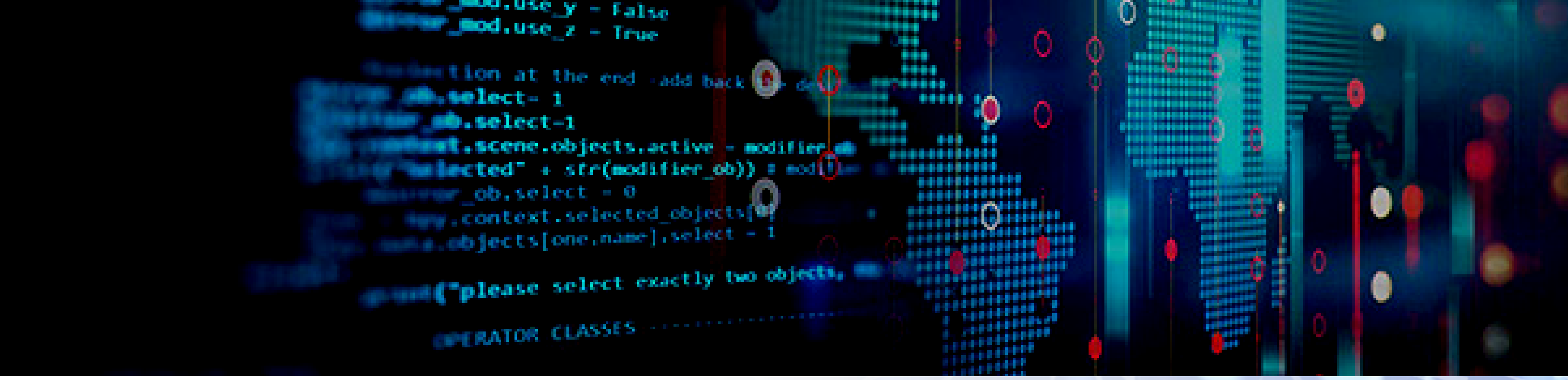
* GNU Privacy Guard 2.3.8
* GNU Privacy Guard 2.2.40
* American Fuzzy Lop plus plus 4.04c
* OpenSSL Toolkit 3.0.6
* OpenSSL Toolkit 1.1.1r
* cryptmount Filesystem Manager 6.1.0
* Wireshark Analyzer 4.0.0
* OpenSSH 9.1p1
* TestSSL 3.0.8
* SIPPTS 3.2

Kali Linux Tutorials

* Monkey365 - Tool For Security Consultants Microsoft 365
* HSTP - Simple Hyper Service Transfer Protocol On Networks
* EvilnoVNC - Ready To Go Phishing Platform
* AoratosWin : A Tool That Removes Traces Of Executed Applications On Windows OS
* Cloudfox - Automating Situational Awareness For Cloud Penetration Tests
* Arsenal - Recon Tool Installer
* Erlik 2 : Vulnerable Flask App
* Utkuici - Nessus Automation
* Java-Remote-Class-Loader : Tool To Send Java Bytecode Victims To Load & Execute
* Bayanay - Python Wardriving Tool

GBHackers Analysis

* Tips to Avoid a Home Security System Hack
* State-Sponsored Hackers Used MS Exchange 0-Day Bugs to Attack At least 10 Orgs
* BIND DNS Software High-Severity Flaws Let Hackers Remotely Trigger the Attack
* RCE Bug in ZOHO Products Let Hackers Execute Arbitrary Code Remotely
* Critical Magento Vulnerability Let Unauthenticated Attackers to Execute Code



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 - Bill Graydon - Defeating Moving Elements in High Security Keys
* DEF CON 30 - Sick Codes - Hacking the Farm = Breaking Badly into Agricultural Devices
* DEF CON 30 - RedAlert ICS CTF
* DEF CON 30 - Blue Team Village

Hak5

* This is How Hackers Would Track You | Retia
* Live Hacking Q&A with Kody and Michael
* Chaos Malware Targets Windows and Linux + Giveaway Winner Announcement! - ThreatWire

The PC Security Channel [TPSC]

* Most Secure Browser? Chrome vs Firefox vs Edge
* Windows 11 Superlite: No Bloatware and Telemetry

Eli the Computer Guy

* I'm not here... Don't mind me... just testing...
* Face Tracking Camera on Servo Motors with OpenCV, Raspberry Pi 4 and Python
* OpenCV with Python - Printing Coordinates of Face on Video
* Easy OpenCV with Python on a Mac - Nothing to do with LOTR

Security Now

* Source Port Randomization - Targeted Malware, Uber CSO Guilty
* Poisoning Akamai - Turnstile vs CAPTCHA, Microsoft Teams Under Attack

Troy Hunt

* Weekly Update 317

Intel Techniques: The Privacy, Security, & OSINT Show

* 281-The Obsession Of Extreme Privacy
* 280-The Future Of Extreme Privacy

Proof of Concept (PoC) & Exploits

Packet Storm Security

* MiniDVBLinux 5.4 Arbitrary File Read
* WordPress Photo Gallery 1.8.0 Cross Site Scripting
* MiniDVBLinux 5.4 Remote Root Command Execution
* WiFi File Transfer 1.0.8 Cross Site Scripting
* Backdoor.Win32.Redkod.d MVID-2022-0649 Hardcoded Credential
* MiniDVBLinux 5.4 Remote Root Command Injection
* pfSense pfBlockerNG 2.1.4_26 Shell Upload
* Spring Cloud Gateway 3.1.0 Remote Code Execution
* Webile 1.0.1 Directory Traversal
* MiniDVBLinux 5.4 Unauthenticated Stream Disclosure
* Backdoor.Win32.DarkSky.23 MVID-2022-0648 Buffer Overflow
* MiniDVBLinux 5.4 Change Root Password
* MiniDVBLinux 5.4 SVDRP Control
* MiniDVBLinux 5.4 Configuration Download
* Joomla Vik Appointments 1.7.3 Cross Site Scripting
* MapTool 1.11.5 Cross Site Scripting
* MapTool 1.11.5 Denial Of Service
* Windows Kernel Registry Subkey Lists Integer Overflow
* WordPress ImageMagick-Engine 1.7.4 Remote Code Execution
* Stripe Green Downloads 2.03 Cross Site Scripting
* Garage Management System 1.0 Cross Site Scripting
* Vicidial 2.14-783a Cross Site Scripting
* Knap Advanced PHP Login 3.1.3 Cross Site Scripting
* Joomla OSG Courts Reservation 1.4.9 SQL Injection
* Intelbras WiFiber 120AC inMesh 1.1-220216 Command Injection

CXSecurity

* 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
* Remote Mouse 4.110 Remote Code Execution
* qdPM 9.1 Authenticated Shell Upload
* Veritas Backup Exec Agent Remote Code Execution
* Netfilter nft_set_elem_init Heap Overflow Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

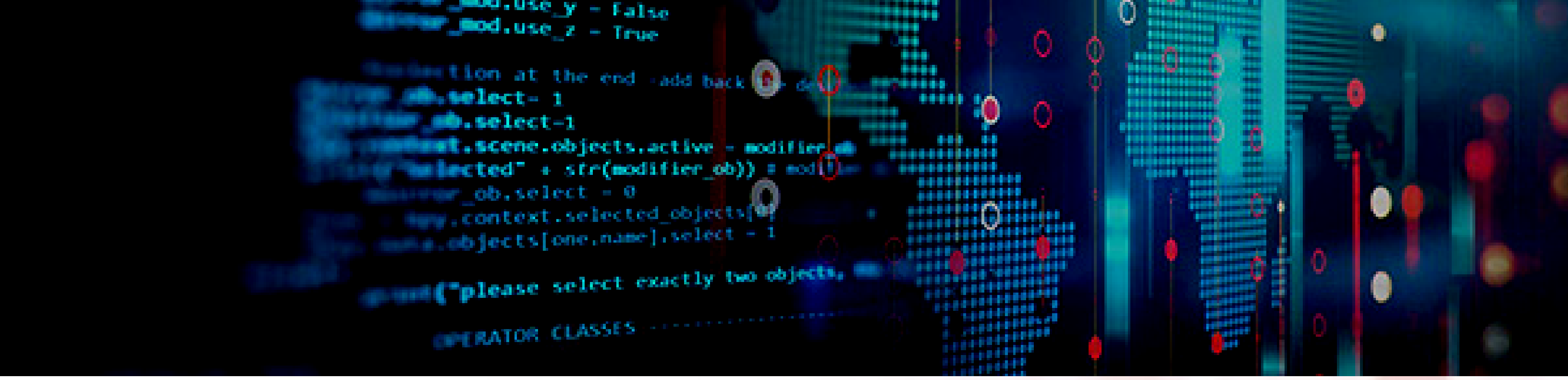
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] 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
* [remote] uftpd 2.10 - Directory Traversal (Authenticated)

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
```

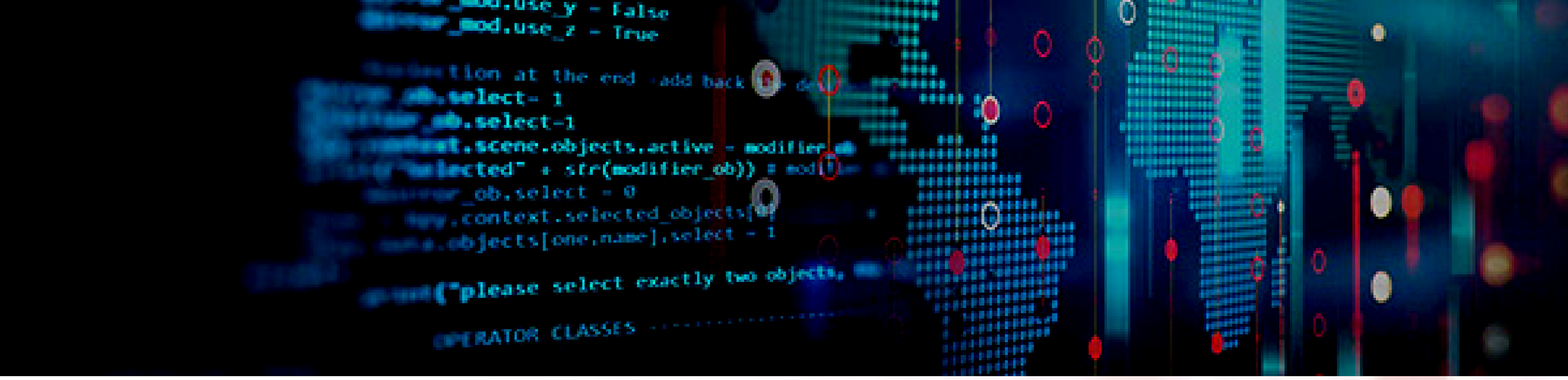
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://sumedangkab.go.id/root.php
https://sumedangkab.go.id/root.php notified by Black_X12
http://cardique.gov.co/d.htm
http://cardique.gov.co/d.htm notified by Bla3k_D3vil
https://pn-demak.go.id/logo.php
https://pn-demak.go.id/logo.php notified by KatakBeracun
https://ppp.gov.bf/SpammingTools.html
https://ppp.gov.bf/SpammingTools.html notified by VOLDIGOAD1999
http://susana.pn-putussibau.go.id/license.txt
http://susana.pn-putussibau.go.id/license.txt notified by tegal9etar
http://siroma.pn-putussibau.go.id/license.txt
http://siroma.pn-putussibau.go.id/license.txt notified by tegal9etar
http://sibantu.pn-putussibau.go.id/license.txt
http://sibantu.pn-putussibau.go.id/license.txt notified by tegal9etar
http://perpustakaan.pn-putussibau.go.id/license.txt
http://perpustakaan.pn-putussibau.go.id/license.txt notified by tegal9etar
http://wianglocal.go.th/m6.htm
http://wianglocal.go.th/m6.htm notified by magelang6etar
http://kaokum.go.th/m6.htm
http://kaokum.go.th/m6.htm notified by magelang6etar
https://dispenda.sintang.go.id/anc.html
https://dispenda.sintang.go.id/anc.html notified by anarchic.info
https://bappeda.sintang.go.id/anc.html
https://bappeda.sintang.go.id/anc.html notified by anarchic.info
http://sintang.go.id/anc.html
http://sintang.go.id/anc.html notified by anarchic.info
http://www.potosi.gob.bo/anc.html
http://www.potosi.gob.bo/anc.html notified by anarchic.info
http://niss.gov.lk/license.txt
http://niss.gov.lk/license.txt notified by tegal9etar
https://pn-putussibau.go.id/license.txt
https://pn-putussibau.go.id/license.txt notified by tegal9etar
https://tilang.pn-indramayu.go.id/readme.html
https://tilang.pn-indramayu.go.id/readme.html notified by Xwizx404


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;

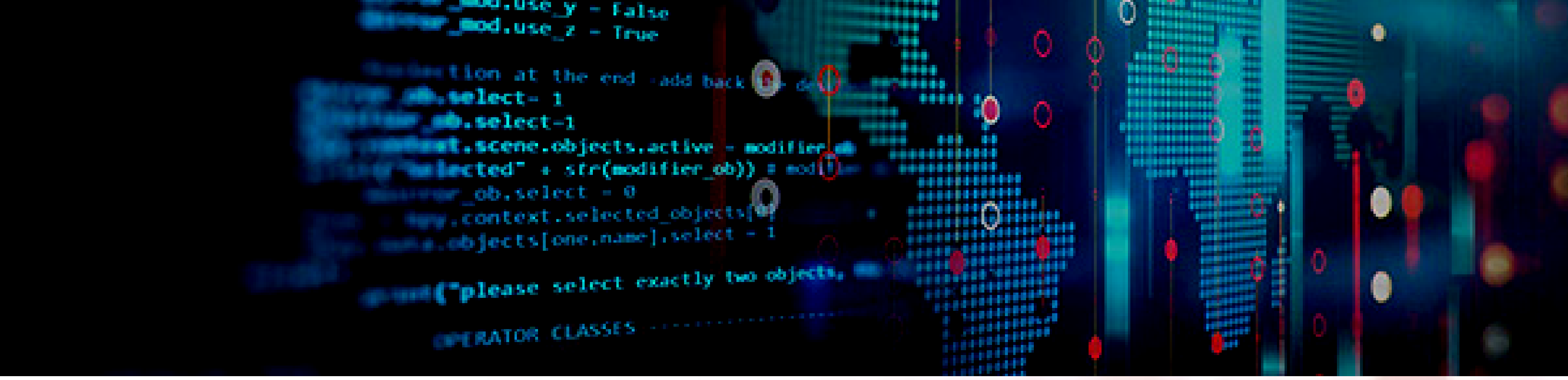
Binance   The training program is led by world-class practitioners from the Binance Investigations team, which employs security experts and former law enforcement agents, including analysts and operatives who had helped take down some of the world's largest criminal platforms, such as Silk Road and Hydra.   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

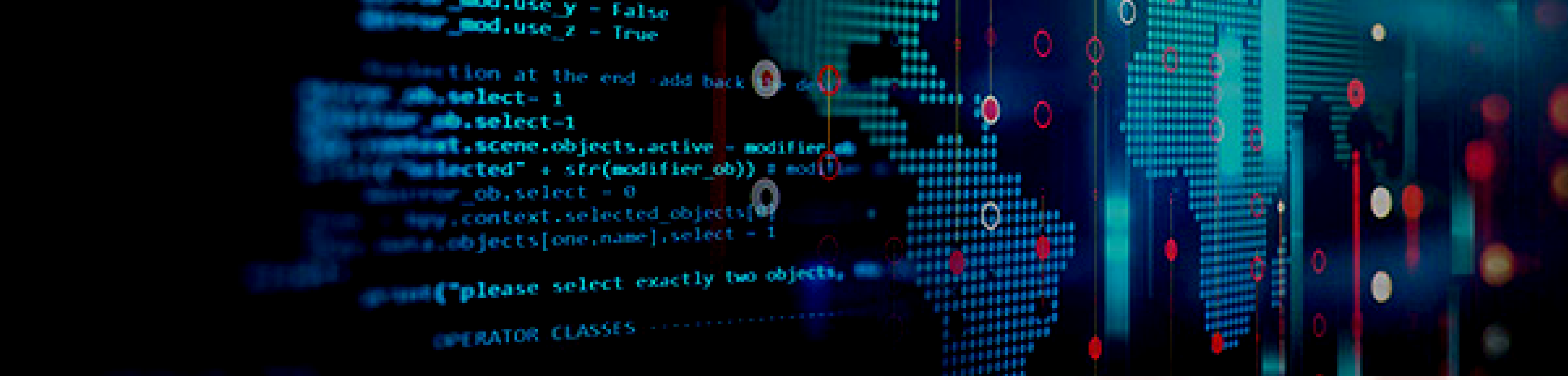
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* Addressing the Evolving Attack Surface Part 1: Modern Challenges
* Metasploit Wrap-Up
* Cloud IAM Done Right: How LPA Helps Significantly Reduce Cloud Risk
* A SIEM With a Pen Tester's Eye: How Offensive Security Helps Shape InsightIDR
* The Intelligent Listing: Cybersecurity Job Descriptions That Deliver
* We're Challenging Convention. Rapid7 Recognized in the 2022 GartnerÂ® Magic Quadrantâ„¢ for SIEM.
* [Security Nation] James Kettle of PortSwigger on Advancing Web-Attack Research
* Real-Time Risk Mitigation in Google Cloud Platform
* Patch Tuesday - October 2022
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Releases RedEye: Red Team Campaign Visualization and Reporting Tool
* CISA Releases Twenty-Five Industrial Control Systems Advisories
* Adobe Releases Security Updates for Multiple Products
* Microsoft Releases October 2022 Security Updates
* CISA Has Added One Known Exploited Vulnerability to Catalog
* CISA Releases Three Industrial Control Systems Advisories
* FBI and CISA Publish a PSA on Information Manipulation Tactics for 2022 Midterm Elections
* Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors
* AA22-279A: Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors
* AA22-277A: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial
* Vulnerability Summary for the Week of October 3, 2022
* Vulnerability Summary for the Week of September 26, 2022

Zero Day Initiative Advisories

ZDI-CAN-19133: Microsoft
A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19110: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-18647: Microsoft
A CVSS score 3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L) severity vulnerability discovered by 'insu of 78ResearchLab' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19123: 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: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19132: Microsoft
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: 2022-10-13, 4 days ago. The vendor is

given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19127: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19129: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19130: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19125: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19128: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19124: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19120: 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: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19126: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19101: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19104: 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: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19109: Unity Technologies

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-10-13, 4 days ago. The vendor is given until 2023-02-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19121: 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: 2022-10-12, 5 days ago. The vendor is given until 2023-02-09 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-18598: 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 'khangkito - Tran Van Khang (VinCSS)' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-18920: Delta Electronics

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-18753: 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 'Anonymous' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-18906: VBASE

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-18601: 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 'khangkito - Tran Van Khang (VinCSS)' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-18907: VBASE

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 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-19084: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-10-06, 11 days ago. The vendor is given until 2023-02-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5682-1

Ubuntu Security Notice 5682-1 - It was discovered that the BPF verifier in the Linux kernel did not properly handle internal data structures. A local attacker could use this to expose sensitive information. It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Gentoo Linux Security Advisory 202210-08

Gentoo Linux Security Advisory 202210-8 - Multiple vulnerabilities have been discovered in Tcpreplay, the worst of which could result in denial of service. Versions less than 4.4.2 are affected.

RRX IOB LP 1.0 DNS Cache Snooping

RRX IOB LP version 1.0 suffers from a DNS cache snooping vulnerability.

Ubuntu Security Notice USN-5680-1

Ubuntu Security Notice 5680-1 - It was discovered that gThumb did not properly managed memory when processing certain image files. If a user were tricked into opening a specially crafted JPEG file, an attacker could possibly use this issue to cause gThumb to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that gThumb did not properly handled certain malformed image files. If a user were tricked into opening a specially crafted JPEG file, an attacker could possibly use this issue to cause gThumb to crash, resulting in a denial of service.

Gentoo Linux Security Advisory 202210-07

Gentoo Linux Security Advisory 202210-7 - A vulnerability has been found in Deluge which could result in XSS. Versions less than 2.1.1 are affected.

Gentoo Linux Security Advisory 202210-06

Gentoo Linux Security Advisory 202210-6 - Multiple vulnerabilities have been discovered in libvirt, the worst of which could result in denial of service. Versions less than 8.2.0 are affected.

Gentoo Linux Security Advisory 202210-05

Gentoo Linux Security Advisory 202210-5 - Multiple vulnerabilities have been discovered in virglrenderer, the worst of which could result in remote code execution. Versions less than 0.10.1 are affected.

Ubuntu Security Notice USN-5683-1

Ubuntu Security Notice 5683-1 - It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of- bounds write. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Selim Enes Karaduman discovered that a race condition existed in the General notification queue implementation of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5676-1

Ubuntu Security Notice 5676-1 - Alexander Lakhin discovered that PostgreSQL incorrectly handled the security restricted operation sandbox when a privileged user is maintaining another user's objects. An attacker having permission to create non-temp objects can use this issue to execute arbitrary commands as the superuser.

Ubuntu Security Notice USN-5679-1

Ubuntu Security Notice 5679-1 - It was discovered that the SUNRPC RDMA protocol implementation in the Linux kernel did not properly calculate the header size of a RPC message payload. A local attacker could use this to expose sensitive information. Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information.

Gentoo Linux Security Advisory 202210-04

Gentoo Linux Security Advisory 202210-4 - Multiple vulnerabilities have been discovered in Wireshark, the worst of which could result in denial of service. Versions less than 3.6.8 are affected.

Red Hat Security Advisory 2022-6954-01

Red Hat Security Advisory 2022-6954-01 - Red Hat Advanced Cluster Management for Kubernetes 2.5.3

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

Ubuntu Security Notice USN-5678-1

Ubuntu Security Notice 5678-1 - It was discovered that the SUNRPC RDMA protocol implementation in the Linux kernel did not properly calculate the header size of a RPC message payload. A local attacker could use this to expose sensitive information. Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information.

Gentoo Linux Security Advisory 202210-03

Gentoo Linux Security Advisory 202210-3 - Multiple vulnerabilities have been discovered in libxml2, the worst of which could result in arbitrary code execution. Versions less than 2.10.2 are affected.

Ubuntu Security Notice USN-5677-1

Ubuntu Security Notice 5677-1 - It was discovered that the BPF verifier in the Linux kernel did not properly handle internal data structures. A local attacker could use this to expose sensitive information. It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

SAP Manufacturing Execution Core 15.3 Path Traversal

SAP Manufacturing Execution Core versions 15.1 through 15.3 suffer from a path traversal vulnerability.

Ubuntu Security Notice USN-5675-1

Ubuntu Security Notice 5675-1 - Isaac Boukris and Andrew Bartlett discovered that Heimdal's KDC was not properly performing checksum algorithm verifications in the S4U2Self extension module. An attacker could possibly use this issue to perform a machine-in-the-middle attack and request S4U2Self tickets for any user known by the application. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. It was discovered that Heimdal was not properly handling the verification of key exchanges when an anonymous PKINIT was being used. An attacker could possibly use this issue to perform a machine-in-the-middle attack and expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS.

Gentoo Linux Security Advisory 202210-02

Gentoo Linux Security Advisory 202210-2 - Multiple vulnerabilities have been discovered in OpenSSL, the worst of which could result in denial of service. Versions less than 1.1.1q are affected.

Gentoo Linux Security Advisory 202210-01

Gentoo Linux Security Advisory 202210-1 - Multiple vulnerabilities have been discovered in Open Asset Import Library, the worst of which could result in denial of service. Versions less than 5.2.2 are affected.

Ubuntu Security Notice USN-5674-1

Ubuntu Security Notice 5674-1 - It was discovered that XML Security Library incorrectly handled certain input documents. An attacker could possibly use this issue to obtain sensitive information or cause a denial of service.

Apple Music Android Application 3.10.2 Man-In-The-Middle

Apple Music Android Application versions 3.8.0 through 3.10.2 suffer from a man-in-the-middle vulnerability.

Apple Security Advisory 2022-10-10-1

Apple Security Advisory 2022-10-10-1 - iOS 16.0.3 addresses a denial of service vulnerability.

Red Hat Security Advisory 2022-6941-01

Red Hat Security Advisory 2022-6941-01 - This release of Red Hat build of Quarkus 2.7.6.SP1 includes security updates, bug fixes, and enhancements. For more information, see the release notes page listed in the References section. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5673-1

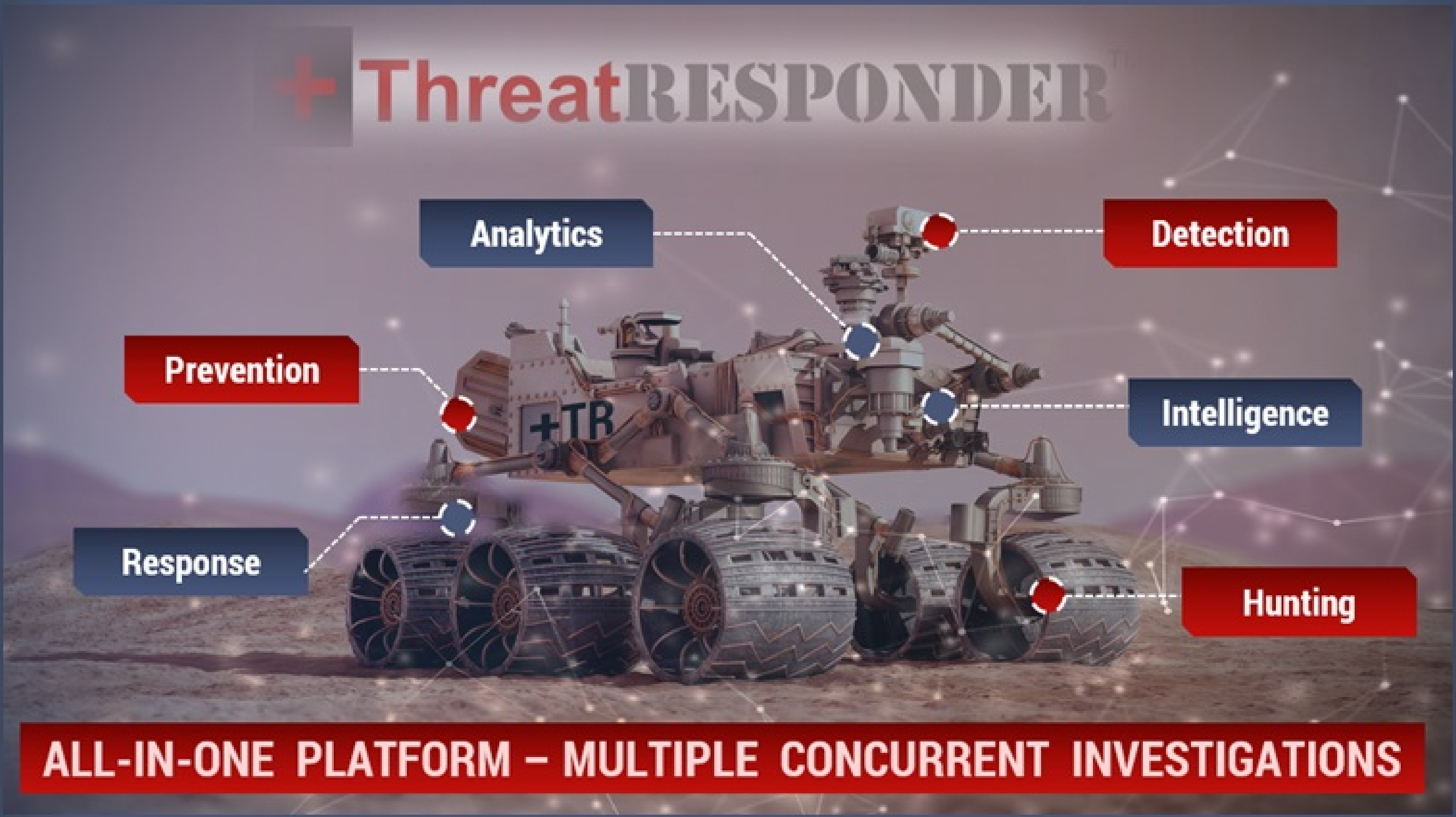
Ubuntu Security Notice 5673-1 - It was discovered that unzip did not properly handle unicode strings under certain circumstances. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that unzip did not properly perform bounds checking while converting wide strings to local strings. If a user were tricked into opening a specially crafted zip file, an attacker could possibly use this issue to cause unzip to crash, resulting in a denial of service, or possibly execute arbitrary code.

Are You...

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

Do DFIR Investigations Better

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



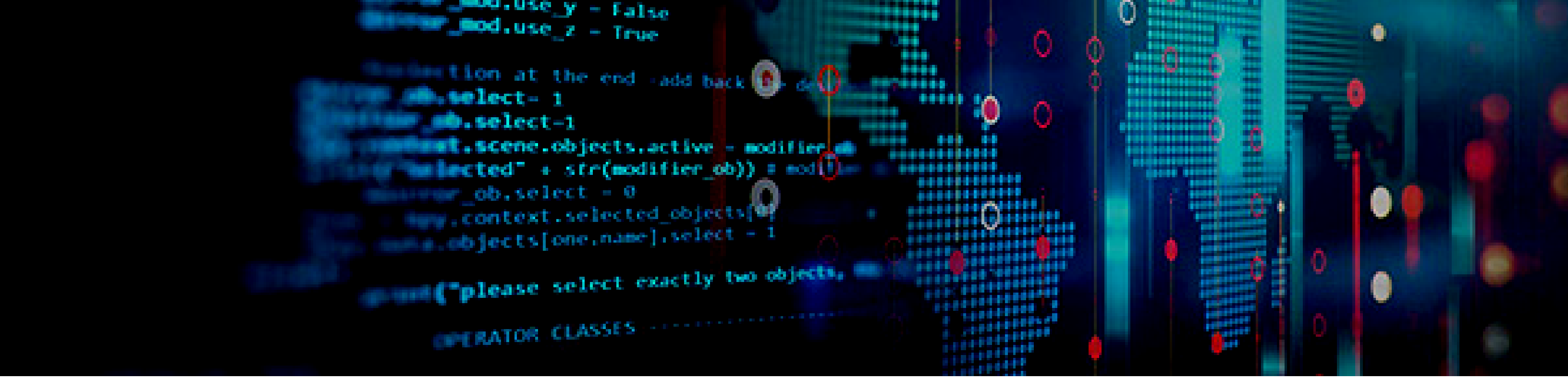
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com



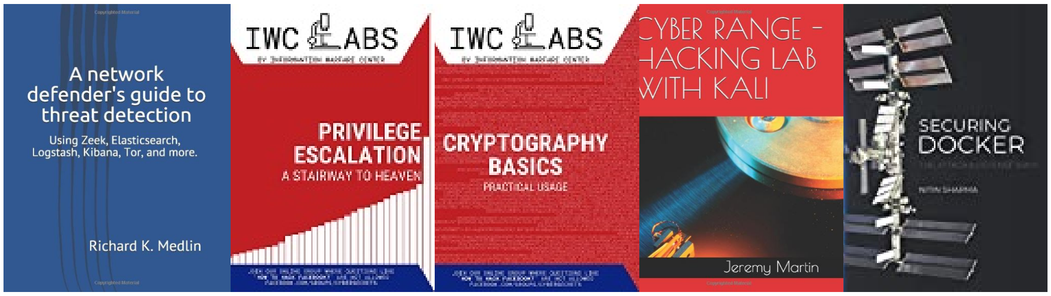
The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

CYBER Secrets
What's Inside?
Threat Intelligence & Training
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION

Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin
IWC LABS
PRIVILEGE ESCALATION
A STAIRWAY TO HEAVEN
IWC LABS
CRYPTOGRAPHY BASICS
PRACTICAL USAGE
CYBER RANGE - HACKING LAB WITH KALI
Jeremy Martin
SECURING DOCKER

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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP