Jun-19-23

CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

June 19, 2023

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

Summary

Internet Storm Center Infocon Status

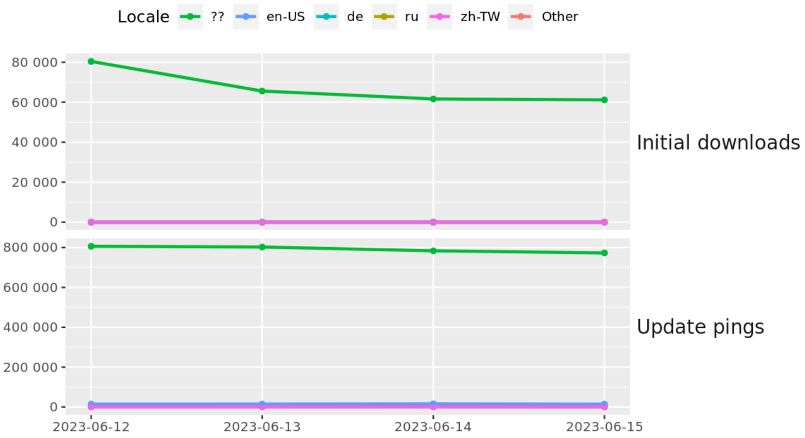
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

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

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

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

* Progress Software Rushes To Patch Another MOVEit SQL Vulnerability
* Intel To Start Shipping A Quantum Processor
* Hacker Gang Clop Publishes Victim Names On Dark Web
* Feds Arrest, Charge Russian National In Arizona For LockBit Attacks
* US Government Agencies Hit In Global Cyber Attack
* Barracuda Zero Day Attacks Attributed To Chinese Cyberespionage Group
* XSS Vulnerabilities In Azure Led To Unauthorized Access In User Sessions
* Is The US Trying To Kill Crypto?
* Russia Hackers Unleash New USB-Based Malware On Ukraine's Military
* LockBit Victims In The US Alone Paid Over $90m In Ransoms Since 2020
* Hackers Can Steal Cryptographic Keys By Video Recording Power LEDs 60 Feet Away
* MSSQL Makes Up 93% Of All Activity On Honeypots Across 10 DBs
* Fortinet Warns Customers Of Possible Zero Day Exploited In Limited Attacks
* Chinese Spies Caught Exploiting VMware ESXi Zero Day
* U.S. Intelligence Has Amassed Sensitive And Intimate Data On Nearly Everyone
* Online Muggers Make Serious Moves On Unpatched Microsoft Bugs
* Progress Software Issues New Critical Fix For MOVEit Transfer App
* Nvidia's AI Software Tricked Into Leaking Data
* FBI: FISA Section 702 Absolutely Critical To Spy On, Err, Protect Americans
* Ransomware Gang Clop Prepped Zero Day MOVEit Attacks In 2021
* Robinhood Markets Removes Three Crypto Tokens
* Netflix Sign-Ups Jump As Password Crackdown Kicks Off
* Google Changes Email Authentication After Spoof Shows A Bad Delivery For UPS
* Dozens Of Popular Minecraft Mods Found Infected With Fracturiser Malware
* VMware Discloses Trio Of High Severity Bugs In Network Monitoring Tool

Krebs on Security

* CISA Order Highlights Persistent Risk at Network Edge
* Microsoft Patch Tuesday, June 2023 Edition
* Barracuda Urges Replacing - Not Patching - Its Email Security Gateways
* Service Rents Email Addresses for Account Signups
* Ask Fitis, the Bear: Real Crooks Sign Their Malware
* Discord Admins Hacked by Malicious Bookmarks
* Phishing Domains Tanked After Meta Sued Freenom
* Interview With a Crypto Scam Investment Spammer
* Russian Hacker "Wazawaka" Indicted for Ransomware
* Re-Victimization from Police-Auctioned Cell Phones

LATEST NEWS

Dark Reading

* Getting Over the DNS Security Awareness Gap
* Security LeadHER Wraps Groundbreaking Inaugural Conference for Women in Security
* The Infrastructure Security Engineer Is a Unicorn Among Thoroughbreds
* Killnet Threatens Imminent SWIFT, World Banking Attacks
* Third MOVEit Transfer Vulnerability Disclosed by Progress Software
* Dodgy Microlending Apps Stalk MEA Users, Highlighting Cyber Maturity Gaps
* Attackers Create Synthetic Security Researchers to Steal IP
* Cybercrime Doesn't Take a Vacation
* HashiCorp Expands PAM, Secrets Management Capabilities
* How Do I Protect My API Keys From Appearing in Search Results?
* Coalition Releases Security Vulnerability Exploit Scoring System
* Keytos Uncovers 15,000 Vulnerable Subdomains per Month in Azure Using Cryptographic Certificates
* Action1 Announces $20M Investment in Its Patch Management Platform
* LockBit Affiliate Arrested, as Extortion Totals Reach $91M Since 2020
* Thales Proposes to Acquire Tesserent, Expanding its Global Cybersecurity Leadership
* Vulcan Cyber Is a Launch Partner for Wiz Integrations (WIN) Platform
* Critical Barracuda ESG Zero-Day Linked to Novel Chinese APT
* Free Training's Role in Cybersecurity
* Angola Marks Technology Advancements With Cybersecurity Academy Plans
* 'Shampoo' ChromeLoader Variant Difficult to Wash Out

The Hacker News

* State-Backed Hackers Employ Advanced Methods to Target Middle Eastern and African Governments
* Microsoft Blames Massive DDoS Attack for Azure, Outlook, and OneDrive Disruptions
* From Cryptojacking to DDoS Attacks: Diicot Expands Tactics with Cayosin Botnet
* ChamelDoH: New Linux Backdoor Utilizing DNS-over-HTTPS Tunneling for Covert CnC
* Activities in the Cybercrime Underground Require a New Approach to Cybersecurity
* 20-Year-Old Russian LockBit Ransomware Affiliate Arrested in Arizona
* Third Flaw Uncovered in MOVEit Transfer App Amidst Cl0p Ransomware Mass Attack
* Ransomware Hackers and Scammers Utilizing Cloud Mining to Launder Cryptocurrency
* Chinese UNC4841 Group Exploits Zero-Day Flaw in Barracuda Email Security Gateway
* Vidar Malware Using New Tactics to Evade Detection and Anonymize Activities
* Warning: GravityRAT Android Trojan Steals WhatsApp Backups and Deletes Files
* New Research: 6% of Employees Paste Sensitive Data into GenAI tools as ChatGPT
* New Supply Chain Attack Exploits Abandoned S3 Buckets to Distribute Malicious Binaries
* New Report Reveals Shuckworm's Long-Running Intrusions on Ukrainian Organizations
* Microsoft Warns of New Russian State-Sponsored Hacker Group with Destructive Intent

LATEST NEWS

Security Week

* Microsoft Says Early June Disruptions to Outlook, Cloud Platform, Were Cyberattacks
* In Other News: Linux Kernel Exploits, Update on BEC Losses, Cybersecurity Awareness Act
* Russian National Arrested, Charged in US Over Role in LockBit Ransomware Attacks
* Russian Hackers Using USB-Spreading Malware in Attacks on Ukrainian Government, Military
* Ransomware Group Starts Naming Victims of MOVEit Zero-Day Attacks
* CISA, NSA Share Guidance on Hardening Baseboard Management Controllers
* Content Moderation Tech Startup Trust Lab Snags $15M Investment
* OT Security Firm Shift5 Adds $33 Million in Funding
* XSS Vulnerabilities in Azure Led to Unauthorized Access to User Sessions
* Barracuda Zero-Day Attacks Attributed to Chinese Cyberespionage Group

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Breakdown of an Impersonation Attack: Using IPFS and Personalization to Improve Attack Success
* UK Attacker Responsible for a Literal "Man-in-the-Middle" Ransomware Attack is Finally Brought to Jus
* New Survey Shows 40% of People Searching for a Job Encountered a Scam
* [INFOGRAPHIC] KnowBe4's SecurityCoach: Top 10 Risky Behaviors
* Takeaways From a Threat Intelligence Specialist on Artificial Intelligence Being a 'Double-Edged Swor
* France Accuses Russia of Spoofing Foreign Ministry Website in 'Typosquatting' Campaign
* Cybercriminals Spoof German Media Anga Com Conference in New Phishing Campaign
* 85% of Organizations Have Experienced At Least One Ransomware Attack in the Last Year
* State-Based Cyber Attacks Continue to Be a Thorn in the Cyber Insurer's Side
* Microsoft Describes a Sophisticated Phishing Campaign that Targeted Several Financial Organizations

ISC2.org Blog

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

HackRead

* Soap2day Shuts Down Permanently - Free Legal and Paid Alternatives
* Warning: Fake GitHub Repos Delivering Malware as PoCs
* 5 Classic Games to Play in 2023
* New Diicot Threat Group Targets SSH Servers with Brute-Force Malware
* Unreleased Music Stolen and Sold on Dark Web: Hacker Fined
* Microsoft sued for alleged misuse of stolen Dark Web credentials
* Setting Strong and Unique Passwords: The First Line of Defense for PS5 Security

Koddos

* Soap2day Shuts Down Permanently - Free Legal and Paid Alternatives
* Warning: Fake GitHub Repos Delivering Malware as PoCs
* 5 Classic Games to Play in 2023
* New Diicot Threat Group Targets SSH Servers with Brute-Force Malware
* Unreleased Music Stolen and Sold on Dark Web: Hacker Fined
* Microsoft sued for alleged misuse of stolen Dark Web credentials
* Setting Strong and Unique Passwords: The First Line of Defense for PS5 Security

LATEST NEWS

Naked Security

* MOVEit mayhem 3: "Disable HTTP and HTTPS traffic immediately"
* S3 Ep139: Are password rules like running through rain?
* Patch Tuesday fixes 4 critical RCE bugs, and a bunch of Office holes
* Gozi banking malware "IT chief" finally jailed after more than 10 years
* History revisited: US DOJ unseals Mt. Gox cybercrime charges
* More MOVEit mitigations: new patches published for further protection
* Thoughts on scheduled password changes (don't call them rotations!)
* S3 Ep138: I like to MOVEit, MOVEit
* Firefox 114 is out: No 0-days, but one fascinating "teachable moment" bug
* Chrome and Edge zero-day: "This exploit is in the wild", so check your versions now

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

LATEST NEWS

IBM Security Intelligence

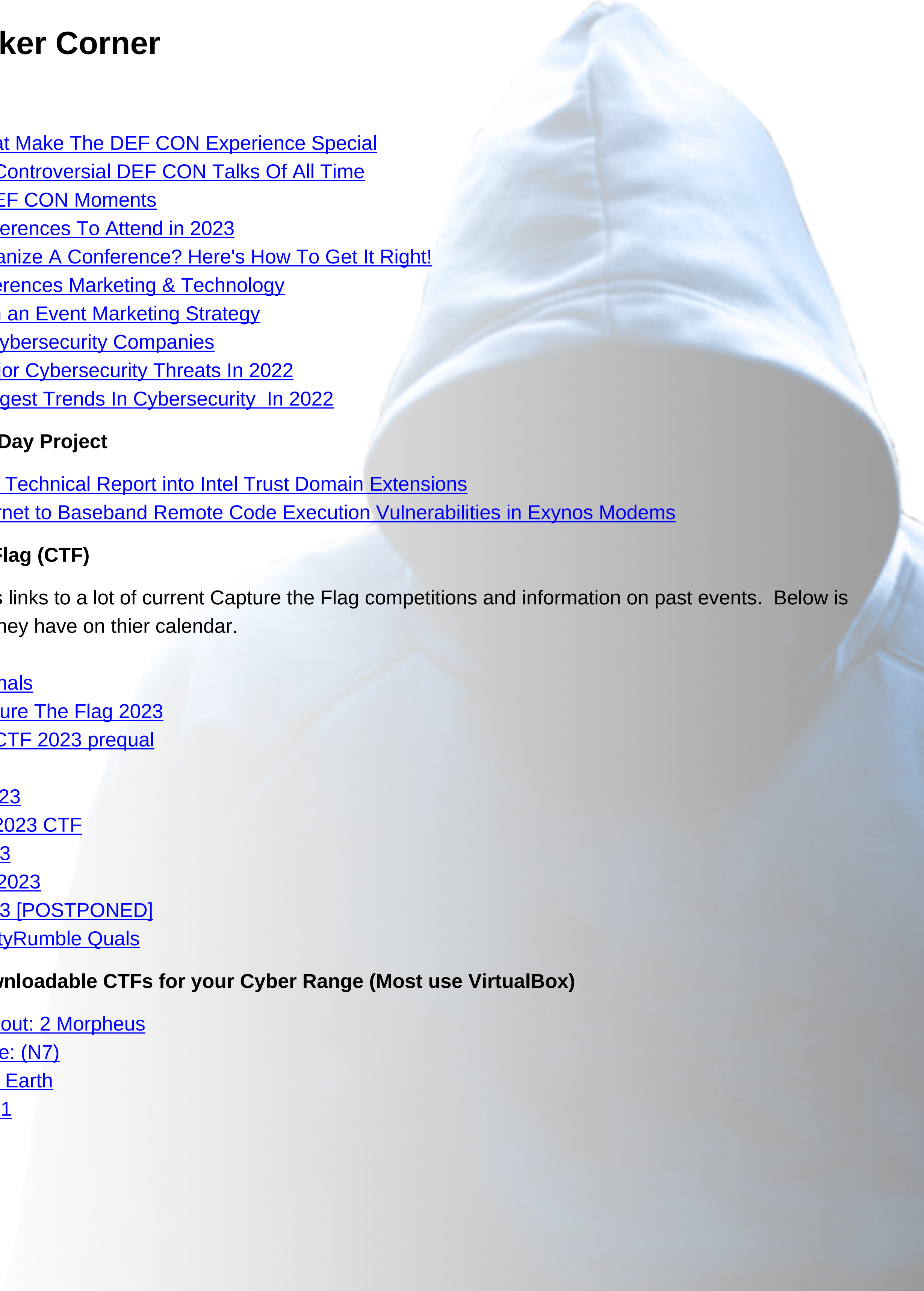
* How Do Some Companies Get Compromised Again and Again?
* Going Up! How to Handle Rising Cybersecurity Costs
* CISA's Known Vulnerabilities Impact 15M Public Services
* ChatGPT and the Race to Secure Your Intellectual Property
* Why Data Security is the Unsung Hero Driving Business Performance
* Merging DevOps and SecOps is a Great Idea: Get Started Now
* Security Awareness Training 101: Which Employees Need It?
* Beyond Requirements: Tapping the Business Potential of Data Governance and Security
* Secure-by-Design: Which Comes First, Code or Security?
* ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People's Republic of Korea

InfoWorld

* Why isn't Apple talking about AI?
* Using Microsoft Azure's Prometheus monitoring with Kubernetes
* GitLab Dedicated offers single-tenant, SaaS-based devsecops
* Multicloud deployments don't have to be so complicated
* Canva design platform unveils developer platform
* Rust most admired language, Stack Overflow survey says
* How to avoid spaghetti code in C#
* Build a real-time AI pipeline with Pulsar Functions
* DataStax adds Schema GPT Translator to Apache Pulsar-based Astra Streaming
* Microsoft unveils C# Dev Kit for Visual Studio Code

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI



The Hacker Corner

Conferences

* 5 Things That Make The DEF CON Experience Special
* The 5 Most Controversial DEF CON Talks Of All Time
* 6 Notable DEF CON Moments
* Best AI Conferences To Attend in 2023
* How To Organize A Conference? Here's How To Get It Right!
* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022

Google Zero Day Project

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

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* p4ctf 2023 finals
* Google Capture The Flag 2023
* Africa battleCTF 2023 prequal
* aupCTF
* AltayCTF 2023
* BSidesTLV 2023 CTF
* UIUCTF 2023
* Crypto CTF 2023
* Zh3r0 CTF v3 [POSTPONED]
* CyberSecurityRumble Quals

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

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

Tools & Techniques

Packet Storm Security Tools Links

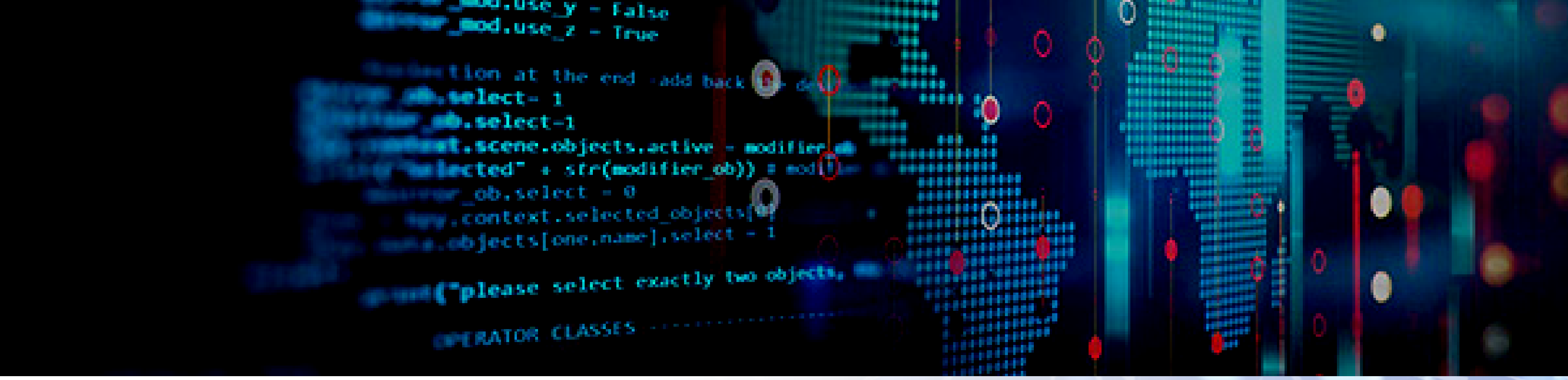
* Suricata IDPE 6.0.13
* AIDE 0.18.4
* Hydra Network Logon Cracker 9.5
* Tenshi Log Monitoring Program 0.18
* Falco 0.35.0
* Faraday 4.4.0
* AIEngine 2.4.0
* OpenSSL Toolkit 3.1.1
* OpenSSL Toolkit 3.0.9
* OpenSSL Toolkit 1.1.1u

Kali Linux Tutorials

* GVision : A Reverse Image Search App That Use Google Cloud Vision API To Detect Landmarks And Web Ent
* debugHunter : Discover Hidden Debugging Parameters And Uncover Web Application Secrets
* Denial of Service (DoS) Attack Using dSniff
* Unveiling the Power of John the Ripper: A Password Cracking Tool
* Pinacolada : Wireless Intrusion Detection System For Hak5's WiFi Coconut
* How to Get Your New Brand 'Known'
* Mastering the Future: Key Data Science Skills for a Competitive Edge
* 5 Essential Crypto Tools For Linux Users In 2023
* QuadraInspect : Android Framework Providing A Powerful Tool For Analyzing The Security Of Android App
* Reportly : An AzureAD User Activity Report Tool

GBHackers Analysis

* Massive Cyber Attack Across the World Against ISPs & Data Centres: More than 200,000 Cisco Switches H
* Microsoft Changed the Method of Naming the Hacker Groups
* Accidental 'write' Permissions In Alibaba PostgreSQL Let Attackers Access Sensitive Data
* Ex-Conti and FIN7 Hackers Team Up To Develop Domino Backdoor Malware
* ChatGPT Account Takeover Bug Allows Hackers To Gain User's Online Account



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Handling Ransomware Incidents: What YOU Need to Know!
* Protecting the Cloud from Ransomware | Host: Ryan Chapman | June 20, 2023
* What is the FOR528: Ransomware for Incident Responders course all about?
* SANS Threat Analysis Rundown | Katie Nickels

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

* Microsoft Fined For Violating Children's Privacy - ThreatWire
* Amazon FINED For Privacy Violations - ThreatWire
* KeePass Master Passwords Could Be Stolen - ThreatWire

The PC Security Channel [TPSC]

* Minecraft Mod Malware
* Edge vs Chrome: Phishing Test

Eli the Computer Guy

* Level.io CEO and Cofounder Jacob Haug - Fireside Chat
* REDDIT ATTACKS 3rd PARTY APPS - they aren't even pretty anyway...
* REDDIT FIRING MODS for PROTESTING - tyrant CEO DEMANDS democracy
* TWITTER EVICTED - Elon Musk Can't Afford Rent

Security Now

* Scanning the Internet - IoT DDoS rising, who pays for Cryptomining, WWDC security announcements
* Windows Platform Binary Table - OWASP, Tor anti-DoS protection, Mandatory SMB Signing on Win 11

Troy Hunt

* Weekly Update 352

Intel Techniques: The Privacy, Security, & OSINT Show

* 300-Self-Hosted 2: Offline Knowledge
* 299-Self-Hosted 1: Introduction

Proof of Concept (PoC) & Exploits

Packet Storm Security

* QuickJob Portal 6.1 Cross Site Scripting
* Quicklancer Freelance Marketplace 2.4 Cross Site Scripting
* QuickHomes Real Estate CMS 1.3 Cross Site Scripting
* Textpattern CMS 4.8.8 Command Injection
* WordPress Abandoned Cart Lite For WooCommerce 5.14.2 Authentication Bypass
* Instagram App 287.0.0.22.85 Denial Of Service
* Quickad Classified Ads CMS 10.4 SQL Injection
* WordPress Unyson 2.7.28 Backup Disclosure
* Online Art Gallery Project 1.0 Arbitrary File Upload
* Rest-Cafe And Restaurant Website CMS 2.0.0 Insecure Settings
* QUICKAD CMS 7.3 Cross Site Request Forgery
* Purle Devloper Panel 1.0 Insecure Direct Object Reference
* Ptclab 3.5 Insecure Settings
* phpFK 8.0 Cross Site Scripting
* PyLoad 0.5.0 Remote Code Execution
* projectSend r1605 CSV Injection
* projectSend r1605 Cross Site Scripting
* Online Examination System Project 1.0 Cross Site Request Forgery
* Teachers Record Management System 1.0 Validation Bypass
* Sales Tracker Management System 1.0 HTML Injection
* Symmetricom SyncServer Unauthenticated Remote Command Execution
* TerraMaster TOS 4.2.29 Remote Code Execution
* ProLogin 1.9 Insecure Direct Object Reference
* Piyanas 0.1 Cross Site Request Forgery
* phpAnalyzer 2.0.4 Insecure Settings

CXSecurity

* WordPress Abandoned Cart Lite For WooCommerce 5.14.2 Authentication Bypass
* Oracle Weblogic PreAuth Remote Command Execution
* Instagram App 287.0.0.22.85 - Local Stack Buffer Overflow (DOS)
* Thruk Monitoring Web Interface 3.06 Path Traversal
* WordPress Theme Workreap 2.2.2 Unauthenticated Upload Leading to Remote Code Execution
* ManageEngine ADManager Plus Command Injection
* SCM Manager 1.60 Cross Site Scripting

Proof of Concept (PoC) & Exploits

Exploit Database

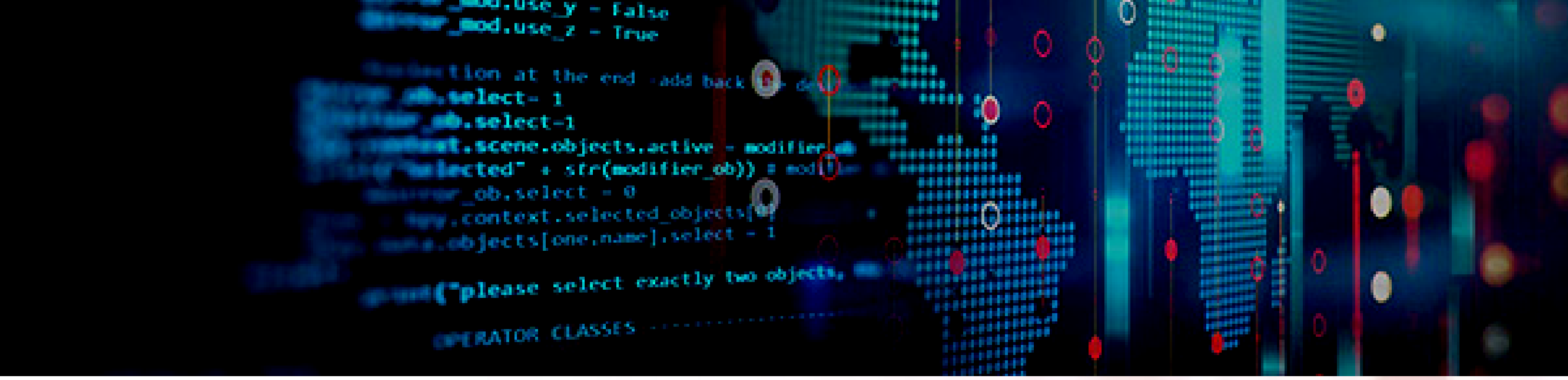
* [webapps] Online Art gallery project 1.0 - Arbitrary File Upload (Unauthenticated)
* [webapps] Textpattern CMS v4.8.8 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] PyLoad 0.5.0 - Pre-auth Remote Code Execution (RCE)
* [webapps] Online Thesis Archiving System v1.0 - Multiple-SQLi
* [webapps] Xoops CMS 2.5.10 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Monstra 3.0.4 - Stored Cross-Site Scripting (XSS)
* [webapps] projectSend r1605 - Stored XSS
* [webapps] projectSend r1605 - CSV injection
* [remote] Anevia Flamingo XL 3.2.9 - Remote Root Jailbreak
* [remote] Anevia Flamingo XL 3.6.20 - Authenticated Root Remote Code Execution
* [remote] Anevia Flamingo XS 3.6.5 - Authenticated Root Remote Code Execution
* [webapps] Sales Tracker Management System v1.0 - Multiple Vulnerabilities
* [webapps] Teachers Record Management System 1.0 - File Upload Type Validation
* [webapps] Online Examination System Project 1.0 - Cross-site request forgery (CSRF)
* [webapps] WordPress Theme Workreap 2.2.2 - Unauthenticated Upload Leading to Remote Code Execution
* [webapps] Thruk Monitoring Web Interface 3.06 - Path Traversal
* [local] USB Flash Drives Control 4.1.0.0 - Unquoted Service Path
* [webapps] Tree Page View Plugin 1.6.7 - Cross Site Scripting (XSS)
* [local] Macro Expert 4.9 - Unquoted Service Path
* [webapps] File Manager Advanced Shortcode 2.3.2 - Unauthenticated Remote Code Execution (RCE)
* [webapps] MotoCMS Version 3.4.3 - SQL Injection
* [webapps] STARFACE 7.3.0.10 - Authentication with Password Hash Possible
* [webapps] Barebones CMS v2.0.2 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Enrollment System Project v1.0 - SQL Injection Authentication Bypass (SQLI)
* [webapps] Total CMS 1.7.4 - Remote Code Execution (RCE)

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
```

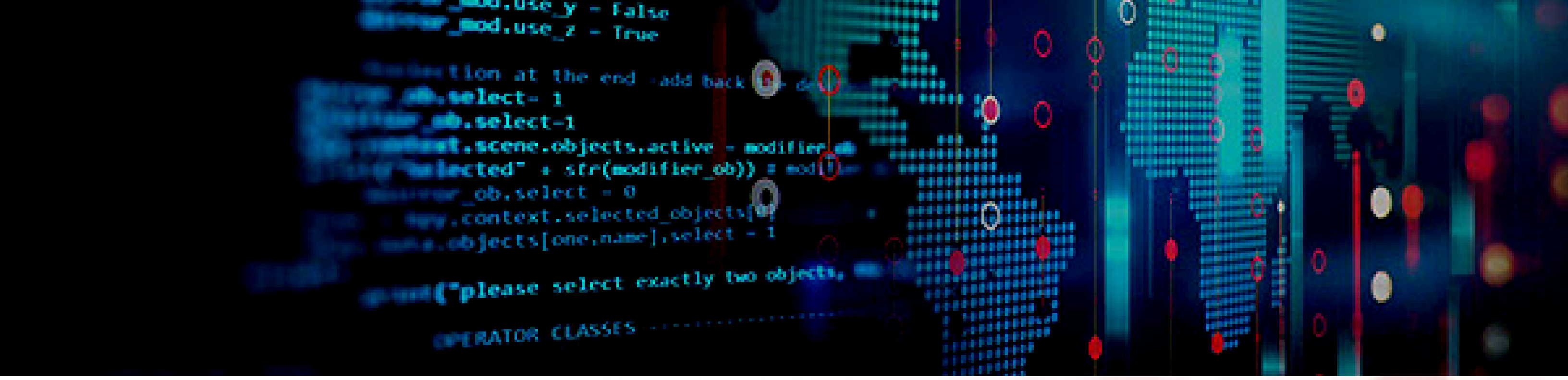
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


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

Latest Hacked Websites

Published on Zone-h.org

http://tbmccs.go.th
http://tbmccs.go.th notified by EFETR
https://sesc-se.com.br/robots.txt
https://sesc-se.com.br/robots.txt notified by Ramil Feyziyev
https://su.gov.mn
https://su.gov.mn notified by Indonesia Attacker
http://www.fundarte.rs.gov.br
http://www.fundarte.rs.gov.br notified by HighD0me
https://www.santaluzia.mg.gov.br
https://www.santaluzia.mg.gov.br notified by ZoRRoKiN
http://epmapachunchi.gob.ec/o.htm
http://epmapachunchi.gob.ec/o.htm notified by chinafans
http://health.gov.fj/o.htm
http://health.gov.fj/o.htm notified by chinafans
http://portal.mmwgh.gov.ph/pxd.txt
http://portal.mmwgh.gov.ph/pxd.txt notified by D3Vnull
https://kejari-kediri.go.id/s.html
https://kejari-kediri.go.id/s.html notified by natanazuma
https://ariits.mof.go.tz/readme.txt
https://ariits.mof.go.tz/readme.txt notified by xNot_RespondinGx
https://datapack.cgcla.go.tz/readme.txt
https://datapack.cgcla.go.tz/readme.txt notified by xNot_RespondinGx
https://diskominfos.baliprov.go.id/readme.txt
https://diskominfos.baliprov.go.id/readme.txt notified by xNot_RespondinGx
https://bpbd.sidoarjokab.go.id/readme.txt
https://bpbd.sidoarjokab.go.id/readme.txt notified by xNot_RespondinGx
https://sakip.acehtamiangkab.go.id/readme.txt
https://sakip.acehtamiangkab.go.id/readme.txt notified by xNot_RespondinGx
https://nayangklak.go.th/AnonSec.php
https://nayangklak.go.th/AnonSec.php notified by Indonesia Attacker
http://lupon.gov.ph/87.txt
http://lupon.gov.ph/87.txt notified by White System&#039;./404
http://alorkab.go.id/read.txt
http://alorkab.go.id/read.txt notified by Mr.L3RB1

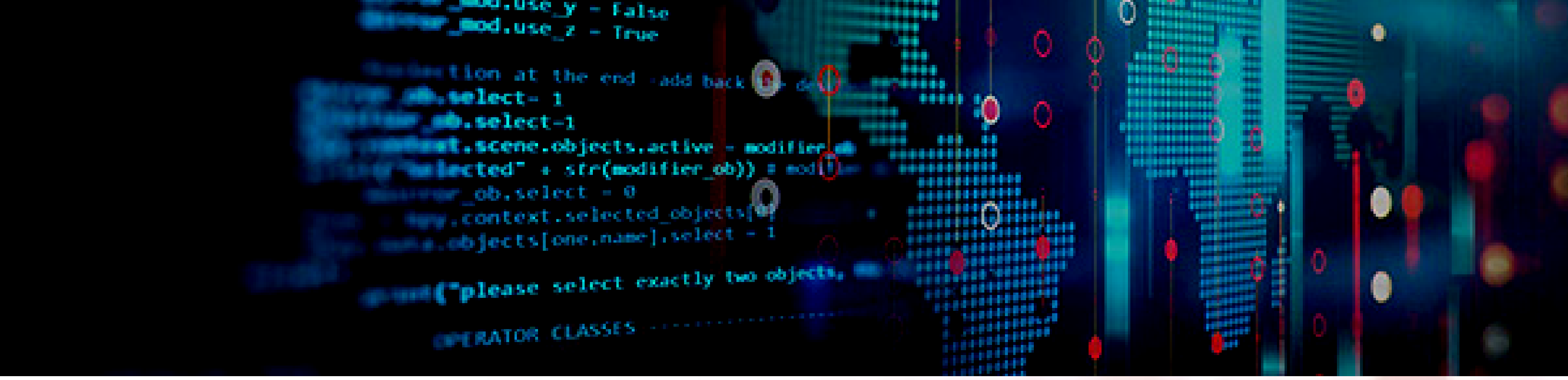

mod.use_z = True
.select= 1
.select=1
.scene.objects.active = modifier_ob
_ob.select = 0
.context.selected_objects
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Dark Web News

Darknet Live

[Indian Duo Arrested for Importing MDMA]()
[Russian Duo Charged for Hacking Mt. Gox]()
[Opiates Vendor "DopeKingUSA" Imprisoned for Distributing Fentanyl]()
[One of the Operators of "CaliCartel" Drugs Vendor Account Sentenced]()

Dark Web Link


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

Trend Micro Anti-Malware Blog

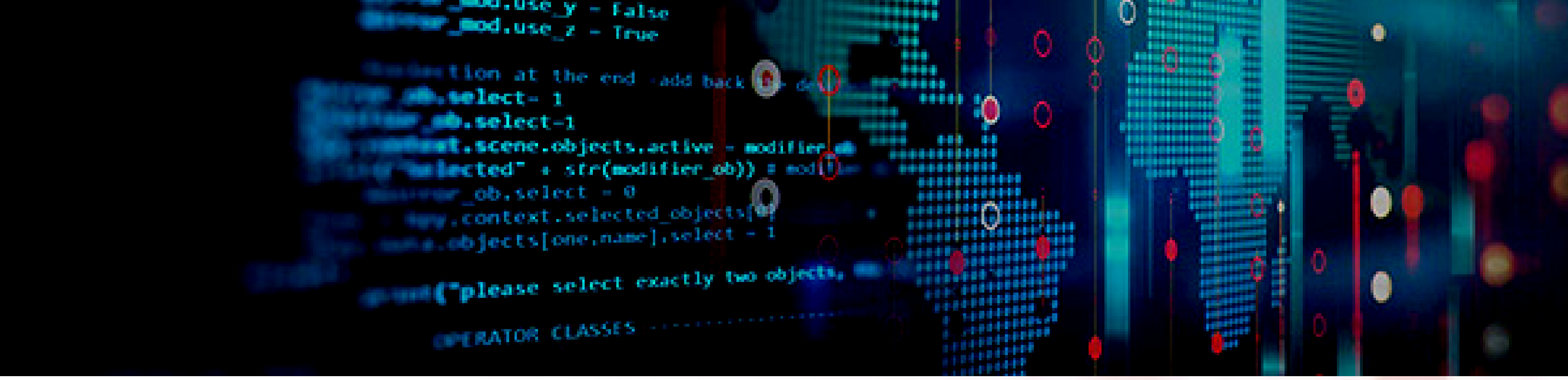
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-Up
* CVE-2023-34362: MOVEit Vulnerability Timeline of Events
* Patch Tuesday - June 2023
* CVE-2023-27997: Critical Fortinet Fortigate Remote Code Execution Vulnerability
* Metasploit Weekly Wrap-Up
* OWASP TOP 10 API Security Risks: 2023!
* Detect and Prioritize Identity-Related Cloud Risk with InsightCloudSec
* CVE-2023-2868: Total Compromise of Physical Barracuda ESG Appliances
* Velociraptor 0.6.9 Release: Digging Even Deeper with SMB Support, Azure Storage and Lockdown Server M
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA, FBI, and MS-ISAC Update Joint CSA on Progress Telerik Vulnerabilities
* Progress Software Releases Security Advisory for MOVEit Transfer Vulnerability
* Barracuda Networks Releases Update to Address ESG Vulnerability
* CISA Releases Fourteen Industrial Control Systems Advisories
* CISA and Partners Release Joint Advisory on Understanding Ransomware Threat Actors: LockBit
* CISA and NSA Release Joint Guidance on Hardening Baseboard Management Controllers (BMCs)
* CISA Issues BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces
* Adobe Releases Security Updates for Multiple Products
* Understanding Ransomware Threat Actors: LockBit
* #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability
* Vulnerability Summary for the Week of June 5, 2023
* Vulnerability Summary for the Week of May 29, 2023

Zero Day Initiative Advisories

ZDI-CAN-20914: SonicWALL
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 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21221: SonicWALL
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N) severity vulnerability discovered by 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21164: Linux
A CVSS score 7.1 (AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:H) severity vulnerability discovered by 'Laurence Wit' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21165: Linux
A CVSS score 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Laurence Wit' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21325: Foxit
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to

publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21304: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21213: X.Org

A CVSS score 7.4 (AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sri' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21403: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20975: Microsoft

A CVSS score 2.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21404: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21405: Sante

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-13, 6 days ago. The vendor is given until 2023-10-11 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20968: GStreamer

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'MICHAEL RANDRIANANTENAINA [https://elkamika.blogspot.com/]' was reported to the affected vendor on: 2023-06-12, 7 days ago. The vendor is given until 2023-10-10 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-20994: GStreamer

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'MICHAEL RANDRIANANTENAINA [https://elkamika.blogspot.com/]' was reported to the affected vendor on: 2023-06-12, 7 days ago. The vendor is given until 2023-10-10 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-20775: GStreamer

A CVSS score 7.6 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H) severity vulnerability discovered by 'Michael Randrianantenaina' was reported to the affected vendor on: 2023-06-12, 7 days ago. The vendor is given until 2023-10-10 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-21266: 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 'Anonymous' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21032: Schneider Electric

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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21155: 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 'Anonymous' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21138: 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 'Anonymous' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21109: 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 'Anonymous' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21065: Schneider Electric

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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21263: 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 'Anonymous' was reported to the affected vendor on: 2023-06-09, 10 days ago. The vendor is given until 2023-10-07 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-21252: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-08, 11 days ago. The vendor is given until 2023-10-06 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-21371: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-08, 11 days ago. The vendor is given until 2023-10-06 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-21387: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-08, 11 days ago. The vendor is given until 2023-10-06 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 5431-1

Debian Linux Security Advisory 5431-1 - Xu Biang discovered that missing input sanitizing in Sofia-SIP, a SIP User-Agent library could result in denial of service.

Ubuntu Security Notice USN-6156-2

Ubuntu Security Notice 6156-2 - USN-6156-1 fixed a vulnerability in SSSD. In certain environments, not all packages ended up being upgraded at the same time, resulting in authentication failures when the PAM module was being used. This update fixes the problem. It was discovered that SSSD incorrectly sanitized certificate data used in LDAP filters. When using this issue in combination with FreeIPA, a remote attacker could possibly use this issue to escalate privileges.

Debian Security Advisory 5430-1

Debian Linux Security Advisory 5430-1 - Several vulnerabilities have been discovered in the OpenJDK Java runtime, which may result in denial of service, information disclosure or bypass of sandbox restrictions.

Red Hat Security Advisory 2023-3644-01

Red Hat Security Advisory 2023-3644-01 - Red Hat OpenShift Service Mesh is the Red Hat distribution of the Istio service mesh project, tailored for installation into an on-premise OpenShift Container Platform installation. This advisory covers container images for the release.

Red Hat Security Advisory 2023-3645-01

Red Hat Security Advisory 2023-3645-01 - Red Hat OpenShift Service Mesh is Red Hat's distribution of the Istio service mesh project, tailored for installation into an OpenShift Container Platform installation. This advisory covers the RPM packages for the release. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-6169-1

Ubuntu Security Notice 6169-1 - It was discovered that GNU SASL's GSSAPI server could make an out-of-bounds reads if given specially crafted GSS-API authentication data. A remote attacker could possibly use this issue to cause a denial of service or to expose sensitive information.

Red Hat Security Advisory 2023-3641-01

Red Hat Security Advisory 2023-3641-01 - This release of Camel for Spring Boot 3.18.3.P2 serves as a replacement for Camel for Spring Boot 3.18.3.P1 and includes bug fixes and enhancements, which are documented in the Release Notes linked in the References. Issues addressed include denial of service, deserialization, resource exhaustion, and server-side request forgery vulnerabilities.

Red Hat Security Advisory 2023-3642-01

Red Hat Security Advisory 2023-3642-01 - Red Hat Ceph Storage is a scalable, open, software-defined storage platform that combines the most stable version of the Ceph storage system with a Ceph management platform, deployment utilities, and support services. This new container image is based on Red Hat Ceph Storage 6.1 and Red Hat Enterprise Linux 9. Issues addressed include bypass, cross site scripting, denial of service, information leakage, spoofing, and traversal vulnerabilities.

Debian Security Advisory 5429-1

Debian Linux Security Advisory 5429-1 - Multiple vulnerabilities have been discovered in Wireshark, a network protocol analyzer which could result in denial of service or the execution of arbitrary code.

Ubuntu Security Notice USN-6168-1

Ubuntu Security Notice 6168-1 - Gregory James Duck discovered that libx11 incorrectly handled certain Request, Event, or Error IDs. If a user were tricked into connecting to a malicious X Server, a remote attacker could possibly use this issue to cause libx11 to crash, resulting in a denial of service.

Debian Security Advisory 5428-1

Debian Linux Security Advisory 5428-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code, denial of service or information disclosure.

Red Hat Security Advisory 2023-3622-01

Red Hat Security Advisory 2023-3622-01 - Jenkins is a continuous integration server that monitors executions of repeated jobs, such as building a software project or jobs run by cron. Issues addressed include bypass, code execution, cross site request forgery, denial of service, information leakage, insecure permissions, and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2023-3624-01

Red Hat Security Advisory 2023-3624-01 - The Migration Toolkit for Containers enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-3623-01

Red Hat Security Advisory 2023-3623-01 - Red Hat Ceph Storage is a scalable, open, software-defined storage platform that combines the most stable version of the Ceph storage system with a Ceph management platform, deployment utilities, and support services. These new packages include numerous enhancements and bug fixes. Issues addressed include cross site scripting and denial of service vulnerabilities.

Ubuntu Security Notice USN-6155-2

Ubuntu Security Notice 6155-2 - USN-6155-1 fixed a vulnerability in Requests. This update provides the corresponding update for Ubuntu 16.04 ESM and 18.04 ESM. Dennis Brinkrolf and Tobias Funke discovered that Requests incorrectly leaked Proxy-Authorization headers. A remote attacker could possibly use this issue to obtain sensitive information.

Debian Security Advisory 5427-1

Debian Linux Security Advisory 5427-1 - An anonymous researcher discovered that processing web content may disclose sensitive information. Apple is aware of a report that this issue may have been actively exploited. An anonymous researcher discovered that processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Red Hat Security Advisory 2023-3610-01

Red Hat Security Advisory 2023-3610-01 - Jenkins is a continuous integration server that monitors executions of repeated jobs, such as building a software project or jobs run by cron. Issues addressed include bypass, code execution, cross site request forgery, cross site scripting, denial of service, memory exhaustion, and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2023-3609-01

Red Hat Security Advisory 2023-3609-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Data Foundation. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Ubuntu Security Notice USN-6163-1

Ubuntu Security Notice 6163-1 - It was discovered that pano13 did not properly validate the prefix provided for PTcrop's output. An attacker could use this issue to cause pano13 to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. It was discovered that pano13 did not properly handle certain crafted TIFF images. An attacker could use this issue to cause pano13 to crash, resulting in a denial of service.

Ubuntu Security Notice USN-6166-1

Ubuntu Security Notice 6166-1 - David Gstir discovered that libcap2 incorrectly handled certain return codes. An attacker could possibly use this issue to cause libcap2 to consume memory, leading to a denial of service. Richard Weinberger discovered that libcap2 incorrectly handled certain long input strings. An attacker could use this issue to cause libcap2 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-6165-1

Ubuntu Security Notice 6165-1 - It was discovered that GLib incorrectly handled non-normal GVariants. An attacker could use this issue to cause GLib to crash, resulting in a denial of service, or perform other unknown attacks.

Red Hat Security Advisory 2023-3542-01

Red Hat Security Advisory 2023-3542-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing

Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.11.43. Issues addressed include denial of service and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-6162-1

Ubuntu Security Notice 6162-1 - Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-3541-01

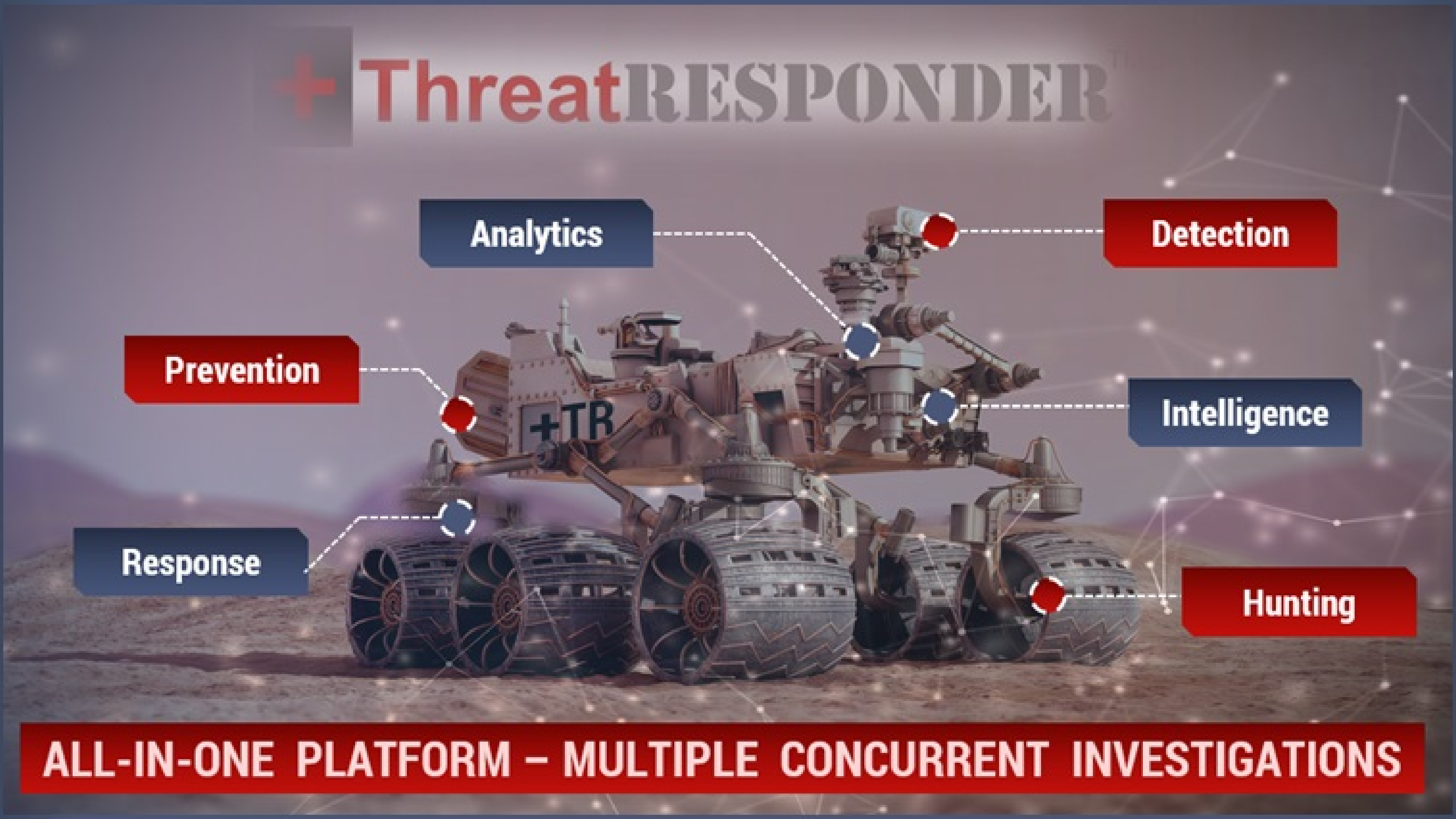
Red Hat Security Advisory 2023-3541-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.11.43.

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



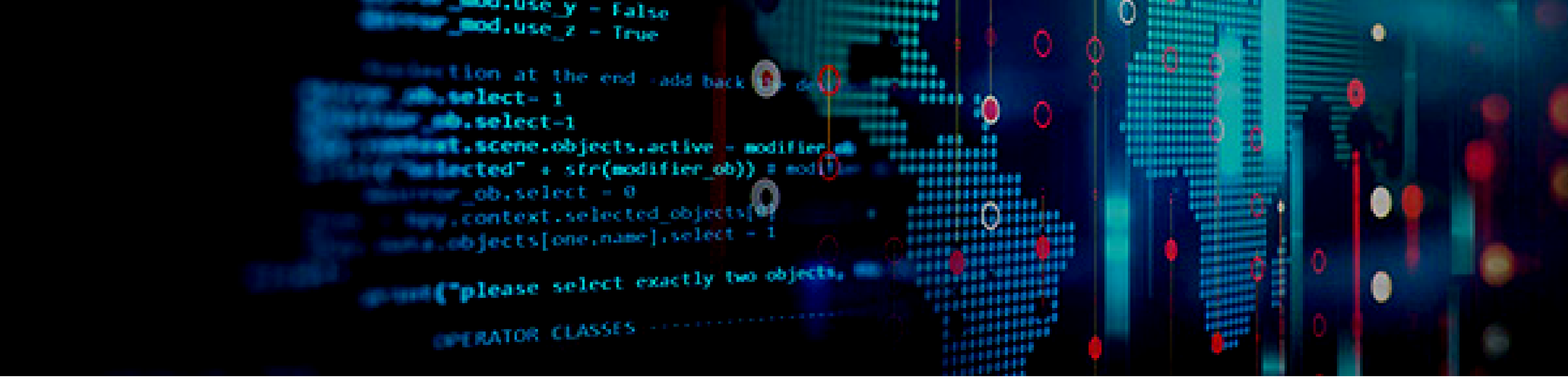
The Solution – ThreatResponder® Platform

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

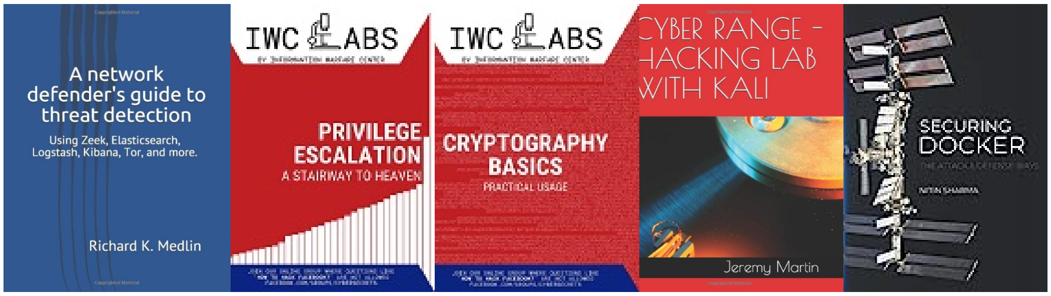


The Cyber Secrets publications on Amazon

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


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
THE ATTACK & DEFENSE WAYS
NITIN SHARMA

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