Feb-20-23

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

February 20, 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

infocon:GREEN
http://isc.sans.edu

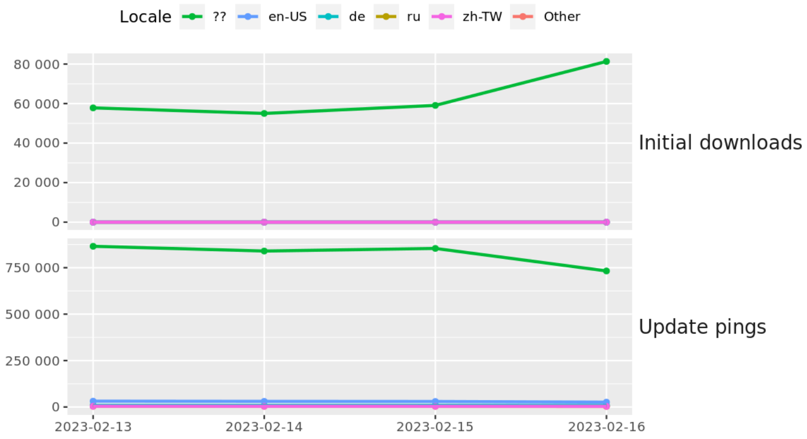
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* GoDaddy Says A Multi-Year Breach Hijacked Customer Websites And Accounts
* Twitter's Two Factor Authentication Change Doesn't Make Sense
* What Mary, Queen Of Scots, Can Teach Today's Cybersec Royalty
* Spain To Extradite British Suspect To US Over Twitter Hack
* Mirai Botnet Variant V3G4 Targeting 13 Unpatched IoT Vulnerabilities
* Actually, America Loves Spy Balloons
* FBI Says It Has Contained Cyber Incident On Their Network
* Researchers Unearth Windows Backdoor That's Unusually Stealthy
* US Issues Declaration On Responsible Use Of AI In The Military
* Intel Patches Up SGX Best It Can After Another Load Of Security Holes Found
* Info For 1 Million Patients Stolen Using Critical GoAnywhere Vulnerability
* CommonSpirit Health Cyberattack, Month-Long Network Outage Cost $150M
* Two Zero-Days Fixed In Patch Tuesday Can Escalate Privileges To SYSTEM
* ESXiArgs Ransomware Fights Off Team America's Data Recovery Script
* Beep Malware Shows Clever Evasion Techniques, As Well As Rookie Mistakes
* A-Salt: Attacking SaltStack
* Latest Attack On PyPi Users Shows Crooks Are Only Getting Better
* Solving Open Source Security - From Alpha To Omega
* Apple Splats Zero-Day Bug, Other Gremlins In macOS, iOS
* Android Launches Another Way To Spy On Users With Privacy Sandbox Beta
* Cloudflare Blocked Largest Reported DDoS Attack At 71M Requests Per Second
* Revealed: The Hacking And Disinformation Team Meddling In Elections
* High Severity DLP Flaw Impacts Trellix For Windows
* Hyundai And Kia Issue Software Upgrades To Thwart TikTok Car Theft Hack
* The White House Wants You To Believe Those UFOs Weren't Aliens

Krebs on Security

* New Protections for Food Benefits Stolen by Skimmers
* Microsoft Patch Tuesday, February 2023 Edition
* U.S., U.K. Sanction 7 Men Tied to Trickbot Hacking Group
* KrebsOnSecurity in Upcoming Hulu Series on Ashley Madison Breach
* Finland's Most-Wanted Hacker Nabbed in France
* Experian Glitch Exposing Credit Files Lasted 47 Days
* Administrator of RSOCKS Proxy Botnet Pleads Guilty
* New T-Mobile Breach Affects 37 Million Accounts
* Thinking of Hiring or Running a Booter Service? Think Again.
* Microsoft Patch Tuesday, January 2023 Edition

LATEST NEWS

Dark Reading

* Modern Software: What's Really Inside?
* Despite Breach, LastPass Demonstrates the Power of Password Management
* Researchers Create an AI Cyber Defender That Reacts to Attackers
* Majority of Ransomware Attacks Last Year Exploited Old Bugs
* Is OWASP at Risk of Irrelevance?
* Check Point Boosts AppSec Focus With CNAPP Enhancements
* Novel Spy Group Targets Telecoms in 'Precision-Targeted' Cyberattacks
* Google Translate Helps BEC Groups Scam Companies in Any Language
* Inglis Retires as National Cyber Director Ahead of Biden's Cybersecurity EO
* Not Stoked: Burton Snowboards' Online Orders Disrupted After Cyberattack
* Massive GoAnywhere RCE Exploit: Everything You Need to Know
* AppSec Threats Deserve Their Own Incident Response Plan
* ESXi Ransomware Update Outfoxes CISA Recovery Script
* Atlassian: Leaked Data Stolen via Third-Party App
* SASE Market to Exceed Over $60B Between 2022 and 2027, According to Dell'Oro Group
* MVP Vibe Fest Bridges Gap Between Athletics and Cybersecurity
* WatchGuard Launches New Line of Firewall Products to Enhance Unified Security for Remote and Distribu
* Cybersecurity Jobs Remain Secure Despite Recession Fears
* SideWinder APT Spotted Targeting Crypto
* Window Snyder's Startup Launches Security Platform for IoT Device Makers

The Hacker News

* Norway Seizes $5.84 Million in Cryptocurrency Stolen by Lazarus Hackers
* How to Detect New Threats via Suspicious Activities
* Google Reveals Alarming Surge in Russian Cyber Attacks Against Ukraine
* Cyber Espionage Group Earth Kitsune Deploys WhiskerSpy Backdoor in Latest Attacks
* Samsung Introduces New Feature to Protect Users from Zero-Click Malware Attacks
* Fortinet Issues Patches for 40 Flaws Affecting FortiWeb, FortiOS, FortiNAC, and FortiProxy
* Twitter Limits SMS-Based 2-Factor Authentication to Blue Subscribers Only
* GoDaddy Discloses Multi-Year Security Breach Causing Malware Installations and Source Code Theft
* Experts Warn of RambleOn Android Malware Targeting South Korean Journalists
* &#9889;Top Cybersecurity News Stories This Week - Cybersecurity Newsletter
* Armenian Entities Hit by New Version of OxtaRAT Spying Tool
* New Mirai Botnet Variant 'V3G4' Exploiting 13 Flaws to Target Linux and IoT Devices
* Critical RCE Vulnerability Discovered in ClamAV Open Source Antivirus Software
* Researchers Hijack Popular NPM Package with Millions of Downloads
* Researchers Link SideWinder Group to Dozens of Targeted Attacks in Multiple Countries

LATEST NEWS

Security Week

* Twitter Shuts Off Text-Based 2FA for Non-Subscribers
* Coinbase Attack Linked to Group Behind Last Year's Twilio, Cloudflare Hacks
* New Samsung Message Guard Protects Mobile Devices Against Zero-Click Exploits
* Fortinet Patches Critical Code Execution Vulnerabilities in FortiNAC, FortiWeb
* Cybersecurity M&A Roundup for February 1-15, 2023
* GoDaddy Says Recent Hack Part of Multi-Year Campaign
* Spain Orders Extradition of British Alleged Hacker to US
* Newly Disclosed Vulnerability Exposes EOL Arris Routers to Attacks
* 'Frebniis' Malware Hijacks Microsoft IIS Function to Deploy Backdoor
* Security Experts Warn of Foreign Cyber Threat to 2024 Voting

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Corporate Transitions Represent Times of Heightened Danger
* The Curse of Cybersecurity Knowledge
* Will AI and Deepfakes Weaken Biometric MFA
* [HEADS UP] Russian Hacker Group Launches New Spear Phishing Campaign with Targets in US and Europe
* [LIVE DEMO] Are Your Users Making Risky Security Mistakes? Deliver Real-Time Coaching in Respons
* Security Awareness: The Top Trend of 2023
* [INFOGRAPHIC] 9 Cognitive Biases Hackers Exploit the Most
* New Survey Reveals Employees are the Attack Surface
* Reddit is the Latest Victim of a Spear Phishing Attack Resulting in a Data Breach
* FTC: Romance Scams Cost U.S. Victims a Total of $1.3 Billion

ISC2.org Blog

* Latest Cyberthreats and Advisories - February 17, 2023
* Analysis: White House Cybersecurity Policy Maker - Secure Open Source Software Even If It Benefits 'A
* Recession, what recession? (ISC)&sup2; Study Shows Cybersecurity Expected to Weather Tech Sector Jobs
* CAP Is Now Certified in Governance, Risk and Compliance (CGRC)
* Cybersecurity Industry News Review: February 15, 2023

HackRead

* New Samsung Message Guard protects users against Zero-Click attacks
* Hackers Stole GoDaddy Source Code in a Multi-Year Data Breach
* Indian Ticketing Platform RailYatri Hacked - 31 Million Impacted
* QR code generator My QR Code leaks users' login data and addresses
* SMS-Based 2FA Will Be Limited to Twitter Blue Users
* 6 Factors to Consider When Shopping for Crypto Debit Card
* FBI Hack - Agency Investigating Internal Network Breach

Koddos

* New Samsung Message Guard protects users against Zero-Click attacks
* Hackers Stole GoDaddy Source Code in a Multi-Year Data Breach
* Indian Ticketing Platform RailYatri Hacked - 31 Million Impacted
* QR code generator My QR Code leaks users' login data and addresses
* SMS-Based 2FA Will Be Limited to Twitter Blue Users
* 6 Factors to Consider When Shopping for Crypto Debit Card
* FBI Hack - Agency Investigating Internal Network Breach

LATEST NEWS

Naked Security

* Twitter tells users: Pay up if you want to keep using insecure 2FA
* GoDaddy admits: Crooks hit us with malware, poisoned customer websites
* S3 Ep122: Stop calling every breach "sophisticated"! [Audio + Text]
* Microsoft Patch Tuesday: 36 RCE bugs, 3 zero-days, 75 CVEs
* Apple fixes zero-day spyware implant bug - patch now!
* Serious Security: GnuTLS follows OpenSSL, fixes timing attack bug
* Reddit admits it was hacked and data stolen, says "Don't panic"
* S3 Ep121: Can you get hacked and then prosecuted for it? [Audio + Text]
* OpenSSL fixes High Severity data-stealing bug - patch now!
* VMWare user? Worried about "ESXi ransomware"? Check your patches 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

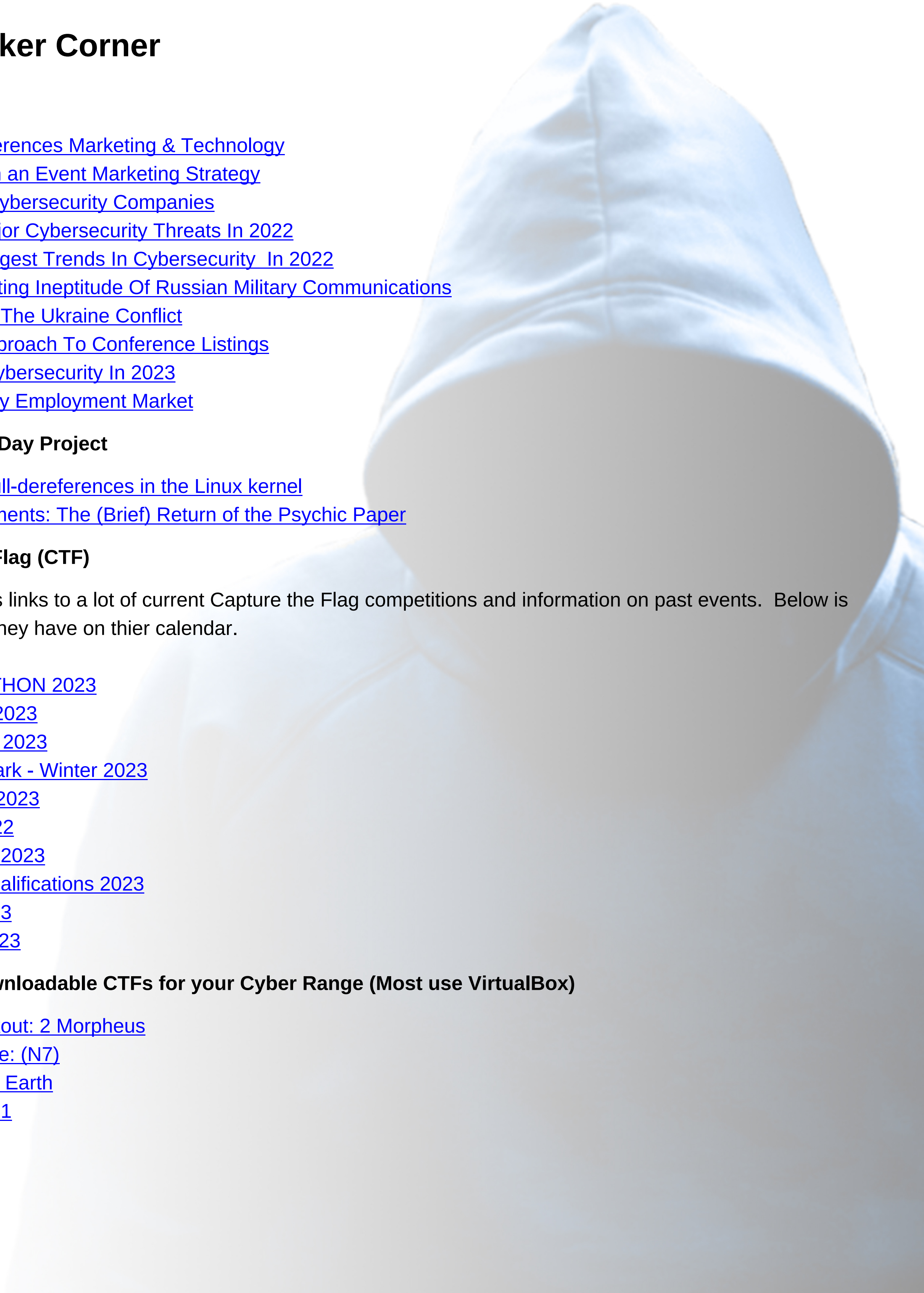
* The Growing Threat to Critical Infrastructure
* How Falling Crypto Prices Impacted Cyber Crime
* Cybersecurity in the Next-Generation Space Age, Pt. 2: Cybersecurity Threats in the New Space
* Detecting the Undetected: The Risk to Your Info
* What are the Duties of a Malware Analyst?
* What's Going Into NIST's New Digital Identity Guidelines?
* Breaking Down the Seven Steps of an SQL Injection Kill Chain
* Avoid Being a Downstream Victim of Service Provider Attacks
* Six Common Ways That Malware Strains Get Their Names
* What is a Pentester, and Can They Prevent Data Breaches?

InfoWorld

* AI still requires human expertise
* Should you leave Twitter for the fediverse?
* Google Cloud Flex Agreements woo users during a slowdown in demand
* Microsoft offers Visual Studio IDE extension for .NET upgrades
* The cost and sustainability of generative AI
* Real-time Ubuntu Linux now available
* Project Valhalla: A look inside Java's epic refactor
* Orchestration and choreography in .NET microservices
* GitHub Copilot update includes security vulnerability filtering
* Cybersecurity startup Oligo debuts with new application security tech

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

* 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
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* Exploiting null-dereferences in the Linux kernel
* DER Entitlements: The (Brief) Return of the Psychic Paper

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.

* VU CYBERTHON 2023
* Trellix HAX 2023
* Cyber-Bytes 2023
* CTF After Dark - Winter 2023
* KalmarCTF 2023
* hxp CTF 2022
* DaVinciCTF 2023
* HackDay Qualifications 2023
* vikeCTF 2023
* WolvCTF 2023

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

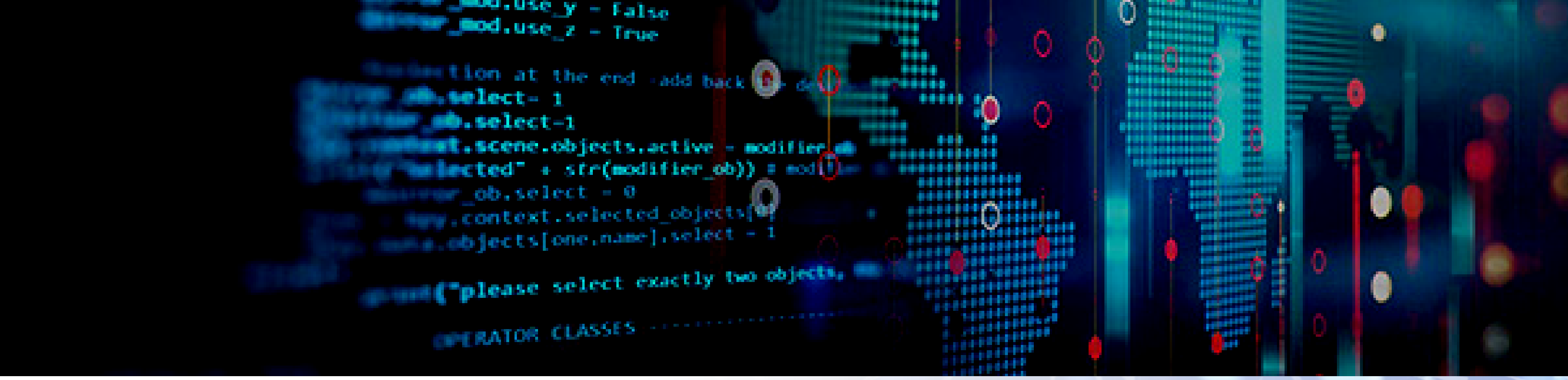
* AIEngine 2.3.0
* Falco 0.34.1
* Faraday 4.3.3
* Clam AntiVirus Toolkit 1.0.1
* Mandos Encrypted File System Unattended Reboot Utility 1.8.16
* OpenSSL Toolkit 3.0.8
* OpenSSL Toolkit 1.1.1t
* AIDE 0.18
* Falco 0.34.0
* NDC Protocol Fuzzer

Kali Linux Tutorials

* Latma : Lateral movement analyzer tool
* PowerHuntShares : Audit Script Designed In Inventory, Analyze, And Report Excessive Privileges Config
* KRIe :To Detect Linux Kernel Runtime Integrity Exploits With eBPF
* Bkcrack : Crack legacy zip encryption with Biham and Kocher's known plaintext attack.
* SQLiDetector : Simple Python Script Supported With BurpBouty Profile To Detect SQL Injection
* Popeye - A Kubernetes Cluster Sanitizer And Reports Potential Issues
* Tai-e : A New Efficient Static Analysis Framework For Java
* DragonCastle : A PoC That Combines AutodialDLL Lateral Movement Technique
* Ghauri : Automates The Process Of Detecting And Exploiting SQL Injection Security Flaws
* APTRS : Automated Penetration Testing Reporting System

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown (STAR) | Live Stream
* SANS Threat Analysis Rundown
* The Truth about Ransomware: Its not Complicated!
* Think DFIRently: What is Digital Forensics & Incident Response (DFIR)?

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

* Inject Keystrokes in only 25 milliseconds! [PAYLOAD]
* New Ransomware Targets Linux - ThreatWire
* Learn Polymorphic Powershell Payload Techniques! [PAYLOAD]

The PC Security Channel [TPSC]

* New Discord Ransomware
* Elon Musk Cryptoscams

Eli the Computer Guy

* Susan Wojcicki FIRED from YOUTUBE
* Is Being "WOKE" Racist?
* eBeggar Wednesday- ChatGPT SUCKS
* Being a "WOKE" Entrepreneur

Security Now

* Ascon - Malicious ChatGPT Use, Goole Security Key Giveaway, OTPAuth
* How ESXi Fell - EU Internet Surveillance, QNAP returns, .DEV is always HTTPS

Troy Hunt

* Weekly Update 335

Intel Techniques: The Privacy, Security, & OSINT Show

* 289-Combo Lists & Extreme Privacy Series
* 288-Privacy, Security, & OSINT Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Kardex Mlog MCC 5.7.12+0-a203c2a213-master File Inclusion / Remote Code Execution
* Best POS Management System 1.0 Shell Upload
* Best POS Management System 1.0 SQL Injection
* Best POS Management System 1.0 Cross Site Scripting
* Zabbix Agent 6.2.7 Insecure Permissions / Privilege Escalation
* Demanzo Matrimony 1.5 Cross Site Request Forgery
* Argon Dashboard 1.1.2 SQL Injection
* Atrocore 1.5.25 Shell Upload
* B&R Systems Diagnostics Manager Cross Site Scripting
* WordPress Quiz And Survey Master 8.0.8 Cross Site Request Forgery
* WordPress Quiz And Survey Master 8.0.8 Media Deletion
* GitLab GitHub Repo Import Deserialization Remote Code Execution
* Korenix JetWave Command Injection / Denial Of Service
* Arris Router Firmware 9.1.103 Remote Code Execution
* Cisco RV Series Authentication Bypass / Command Injection
* XWorm Trojan 2.1 NULL Pointer Dereference
* Global Infotech CMS 1.0 SQL Injection
* ChiKoi 1.0 Directory Traversal
* ChiKoi 1.0 Cross Site Scripting
* Monitorr 1.7.6 Shell Upload
* Windows Kernel Registry Virtualization Incompatibility
* Windows Kernel Virtualizable Hive Key Deletion
* WEBY 1.2.5 Cross Site Request Forgery
* Windows Kernsl SID Table Poisoning
* Windows Kernel Key Replication Issues

CXSecurity

* Zoho ManageEngine Endpoint Central / MSP 10.1.2228.10 Remote Code Execution
* Wordpress Multiple themes - Unauthenticated Arbitrary File Upload
* Fortra GoAnywhere MFT Unsafe Deserialization Remote Code Execution
* ManageEngine ADSelfService Plus Unauthenticated SAML Remote Code Execution
* Lenovo Diagnostics Driver Memory Access
* macOS Dirty Cow Arbitrary File Write Local Privilege Escalation
* F5 Big-IP Create Administrative User

Proof of Concept (PoC) & Exploits

Exploit Database

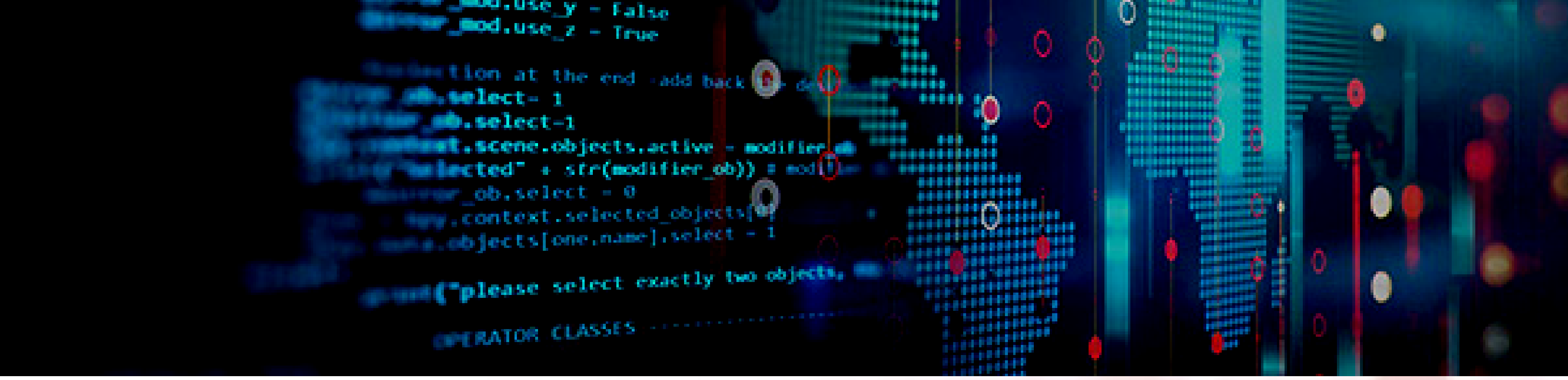
* [webapps] pfBlockerNG 2.1.4_26 - Remote Code Execution (RCE)
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [webapps] Open Web Analytics 1.7.3 - Remote Code Execution
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (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)

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
```

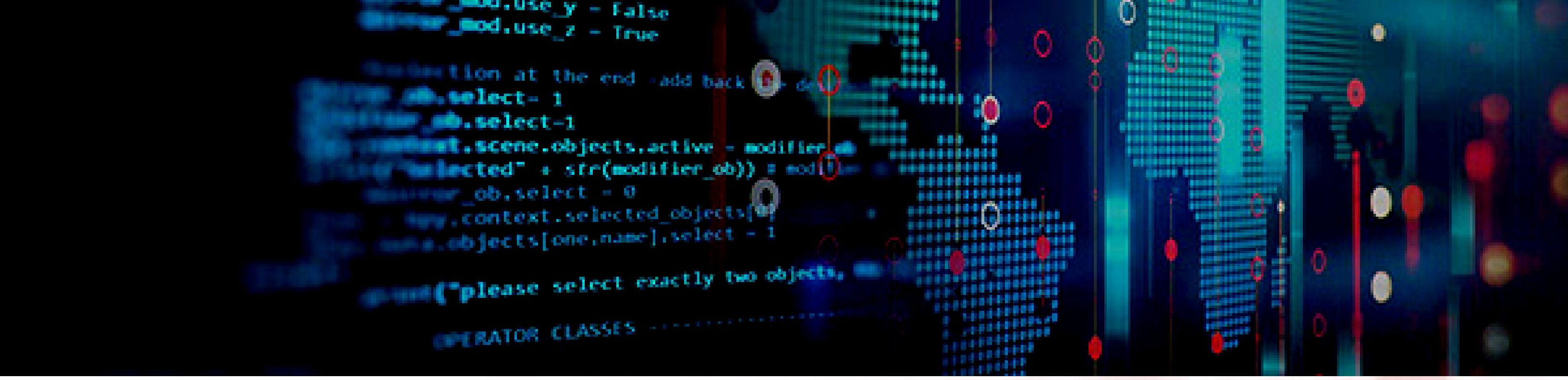
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://pa-pagaralam.go.id/LICENSE.txt
https://pa-pagaralam.go.id/LICENSE.txt notified by UnM@SK
https://municarmendelalegua.gob.pe/xx.html
https://municarmendelalegua.gob.pe/xx.html notified by xstro0
http://hcdgeneralviamonte.gob.ar/xx.html
http://hcdgeneralviamonte.gob.ar/xx.html notified by xstro0
http://ligs.gov.my/0x7e.html
http://ligs.gov.my/0x7e.html notified by 0x7e
http://registropropiedadpuertoquito.gob.ec/baka.html
http://registropropiedadpuertoquito.gob.ec/baka.html notified by ./KeyzNet
https://www.trabajoarequipa.gob.pe/kurd.html
https://www.trabajoarequipa.gob.pe/kurd.html notified by 0x1998
https://bima.ntb.polri.go.id/wp-mail.php
https://bima.ntb.polri.go.id/wp-mail.php notified by ivanN4kPol0Z
https://www.pccb.go.tz
https://www.pccb.go.tz notified by Maniak k4sur
https://bpemc.gov.bd/hallo.txt
https://bpemc.gov.bd/hallo.txt notified by Mr.Rm19
https://www.oag.gov.fj/milo.html
https://www.oag.gov.fj/milo.html notified by ./G1L4N6_ST86
http://acaa.gov.af/o.htm
http://acaa.gov.af/o.htm notified by chinafans
https://tuxpan.gob.mx/kurd.html
https://tuxpan.gob.mx/kurd.html notified by 0x1998
https://sgp.gob.gt/kurd.html
https://sgp.gob.gt/kurd.html notified by 0x1998
http://yedikirsulamabirligi.gov.tr/1877.html
http://yedikirsulamabirligi.gov.tr/1877.html notified by 1877
http://acipayam-tavassulama.gov.tr/1877.html
http://acipayam-tavassulama.gov.tr/1877.html notified by 1877
http://bayramic-ezinesulama.gov.tr/1877.html
http://bayramic-ezinesulama.gov.tr/1877.html notified by 1877
http://bigaicmesuyu.gov.tr/1877.html
http://bigaicmesuyu.gov.tr/1877.html notified by 1877

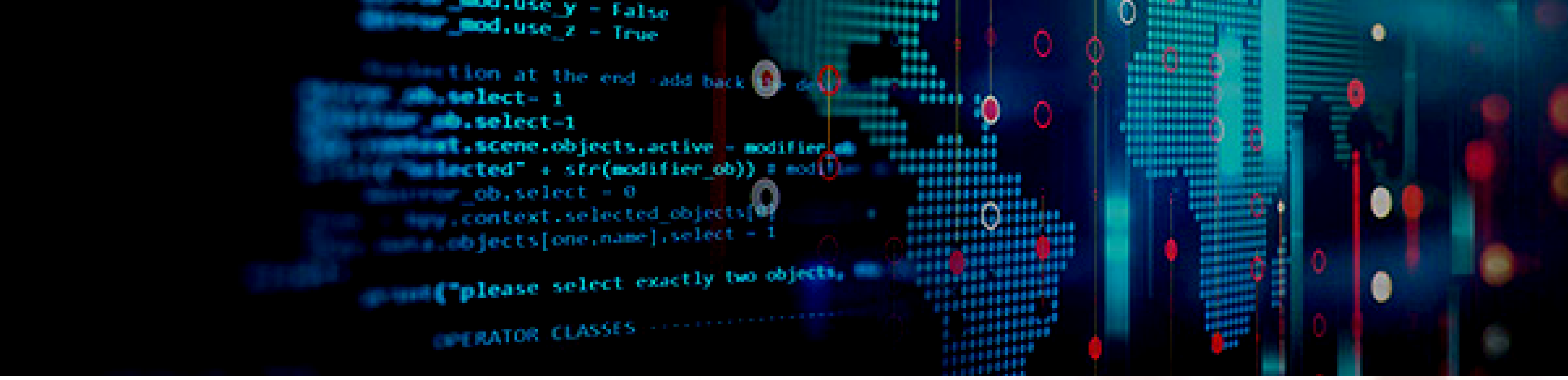


Dark Web News

Darknet Live

[Iowa Man Resold Drugs Purchased on the Dark Web](#)
[Tor.taxi linked with Kilos exit scam](#)
[The Hitchhiker's Guide to Bitcoin](#)
[Tor is slow right now. Here is what is happening](#)

Dark Web Link



Trend Micro Anti-Malware Blog

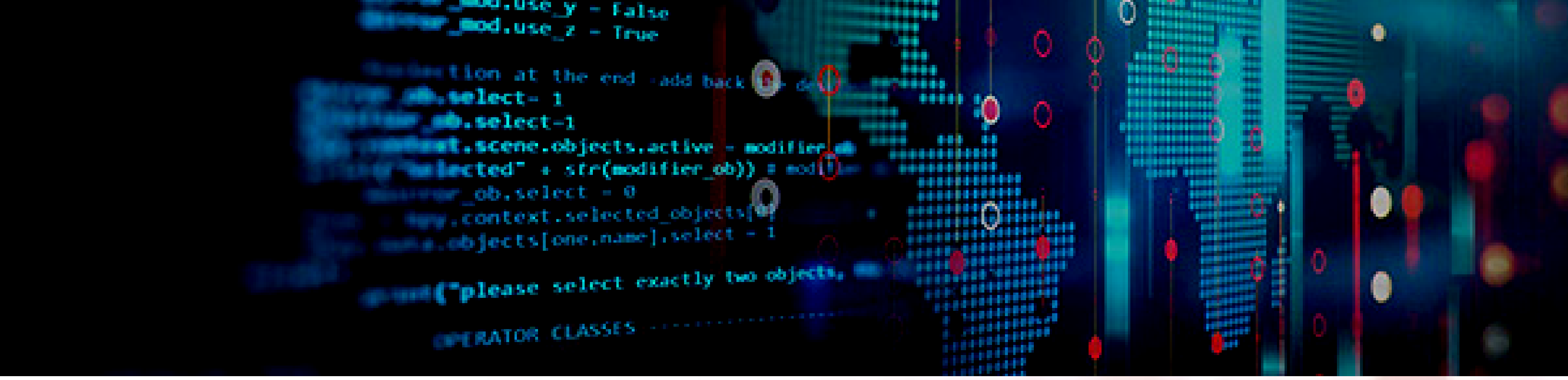
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Wrap-Up
* Rapid7 CEO Corey E. Thomas Appointed To National Security Telecommunications Advisory Committee
* CIEM is Required for Cloud Security and IAM Providers to Compete: GartnerÂ® Report
* Patch Tuesday - February 2023
* A Deep Dive into Reversing CODESYS
* Rapid7 and USF: Building a diverse cybersecurity workforce is not optional
* Metasploit Weekly Wrap-Up
* Nearly 19,000 ESXi Servers Still Vulnerable to CVE-2021-21974
* Evasion Techniques Uncovered: An Analysis of APT Methods
* Year In Review: Rapid7 InsightIDR


_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

Advisories

US-Cert Alerts & bulletins

* CISA Releases Fifteen Industrial Control Systems Advisories
* CISA Adds One Known Exploited Vulnerability to Catalog
* Cisco Releases Security Advisories for Multiple Products
* Adobe Releases Security Updates for Multiple Products
* Mozilla Releases Security Updates for Firefox 110 and Firefox ESR
* Citrix Releases Security Updates for Workspace Apps, Virtual Apps and Desktops
* CISA Adds Four Known Exploited Vulnerabilities to Catalog
* Microsoft Releases February 2023 Security Updates
* AA23-040A: #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber A
* AA23-039A: ESXiArgs Ransomware Virtual Machine Recovery Guidance
* Vulnerability Summary for the Week of February 6, 2023
* Vulnerability Summary for the Week of January 30, 2023

Zero Day Initiative Advisories

ZDI-CAN-19904: Parse
A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'hir0ot' was reported to the affected vendor on: 2023-02-17, 3 days ago. The vendor is given until 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-19716: NETGEAR
A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Steven Seeley of Source Incite' was reported to the affected vendor on: 2023-02-17, 3 days ago. The vendor is given until 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-19919: LG
A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20012: LG
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19924: LG
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was

reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20005: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20015: LG

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19952: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20010: LG

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19922: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19925: LG

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20048: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19926: LG

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19978: LG

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19920: LG

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19923: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20016: LG

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20006: LG

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19921: LG

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20011: LG

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19953: LG

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19951: LG

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-19944: LG

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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-20014: LG

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2023-02-14, 6 days ago. The vendor is given until 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 5354-1

Debian Linux Security Advisory 5354-1 - Multiple security vulnerabilities were discovered in snort, a flexible Network Intrusion Detection System, which could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or bypass filtering technology on an affected device and ex-filtrate data from a compromised host.

Debian Security Advisory 5353-1

Debian Linux Security Advisory 5353-1 - Christian Holler discovered that incorrect handling of PKCS 12 Safe Bag attributes in nss, the Mozilla Network Security Service library, may result in execution of arbitrary code if a specially crafted PKCS 12 certificate bundle is processed.

Ubuntu Security Notice USN-5880-1

Ubuntu Security Notice 5880-1 - Christian Holler discovered that Firefox did not properly manage memory when using PKCS 12 Safe Bag attributes. An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes. Johan Carlsson discovered that Firefox did not properly manage child iframe's unredacted URI when using Content-Security-Policy-Report-Only header. An attacker could potentially exploits this to obtain sensitive information.

Red Hat Security Advisory 2023-0809-01

Red Hat Security Advisory 2023-0809-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0805-01

Red Hat Security Advisory 2023-0805-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0808-01

Red Hat Security Advisory 2023-0808-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0810-01

Red Hat Security Advisory 2023-0810-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0811-01

Red Hat Security Advisory 2023-0811-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0807-01

Red Hat Security Advisory 2023-0807-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0812-01

Red Hat Security Advisory 2023-0812-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2023-0806-01

Red Hat Security Advisory 2023-0806-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.8.0 ESR. Issues addressed include a use-after-free vulnerability.

Microsoft Windows Contact File Remote Code Execution

This advisory ties together older research on a contact file handling flaw on Microsoft Windows as well as recent research discovered that uses the same methodologies.

Debian Security Advisory 5352-1

Debian Linux Security Advisory 5352-1 - 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 2023-0803-01

Red Hat Security Advisory 2023-0803-01 - An update is now available for Red Hat OpenShift GitOps 1.7. Red Hat Product Security has rated this update as having a security impact of Important.

Red Hat Security Advisory 2023-0804-01

Red Hat Security Advisory 2023-0804-01 - An update is now available for Red Hat OpenShift GitOps 1.5. Red Hat Product Security has rated this update as having a security impact of Important.

Red Hat Security Advisory 2023-0802-01

Red Hat Security Advisory 2023-0802-01 - An update is now available for Red Hat OpenShift GitOps 1.6. Red Hat Product Security has rated this update as having a security impact of Important.

Red Hat Security Advisory 2023-0728-01

Red Hat Security Advisory 2023-0728-01 - 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 4.12.3.

Debian Security Advisory 5351-1

Debian Linux Security Advisory 5351-1 - 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 2023-0727-01

Red Hat Security Advisory 2023-0727-01 - 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 4.12.3.

Red Hat Security Advisory 2023-0577-01

Red Hat Security Advisory 2023-0577-01 - This release of Red Hat build of Eclipse Vert.x 4.3.7 GA includes security updates. For more information, see the release notes listed in the References section. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5879-1

Ubuntu Security Notice 5879-1 - Kyle Zeng discovered that the sysctl implementation in the Linux kernel contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service or execute arbitrary code. Tam&aacute;s Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5878-1

Ubuntu Security Notice 5878-1 - It was discovered that the Bluetooth HCI implementation in the Linux kernel did not properly deallocate memory in some situations. An attacker could possibly use this cause a denial of service. It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5778-2

Ubuntu Security Notice 5778-2 - USN-5778-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Jan-Niklas Sohn discovered that X.Org X Server extensions contained multiple security issues. An attacker could possibly use these issues to cause the X Server to crash, execute arbitrary code, or escalate privileges.

Ubuntu Security Notice USN-5873-1

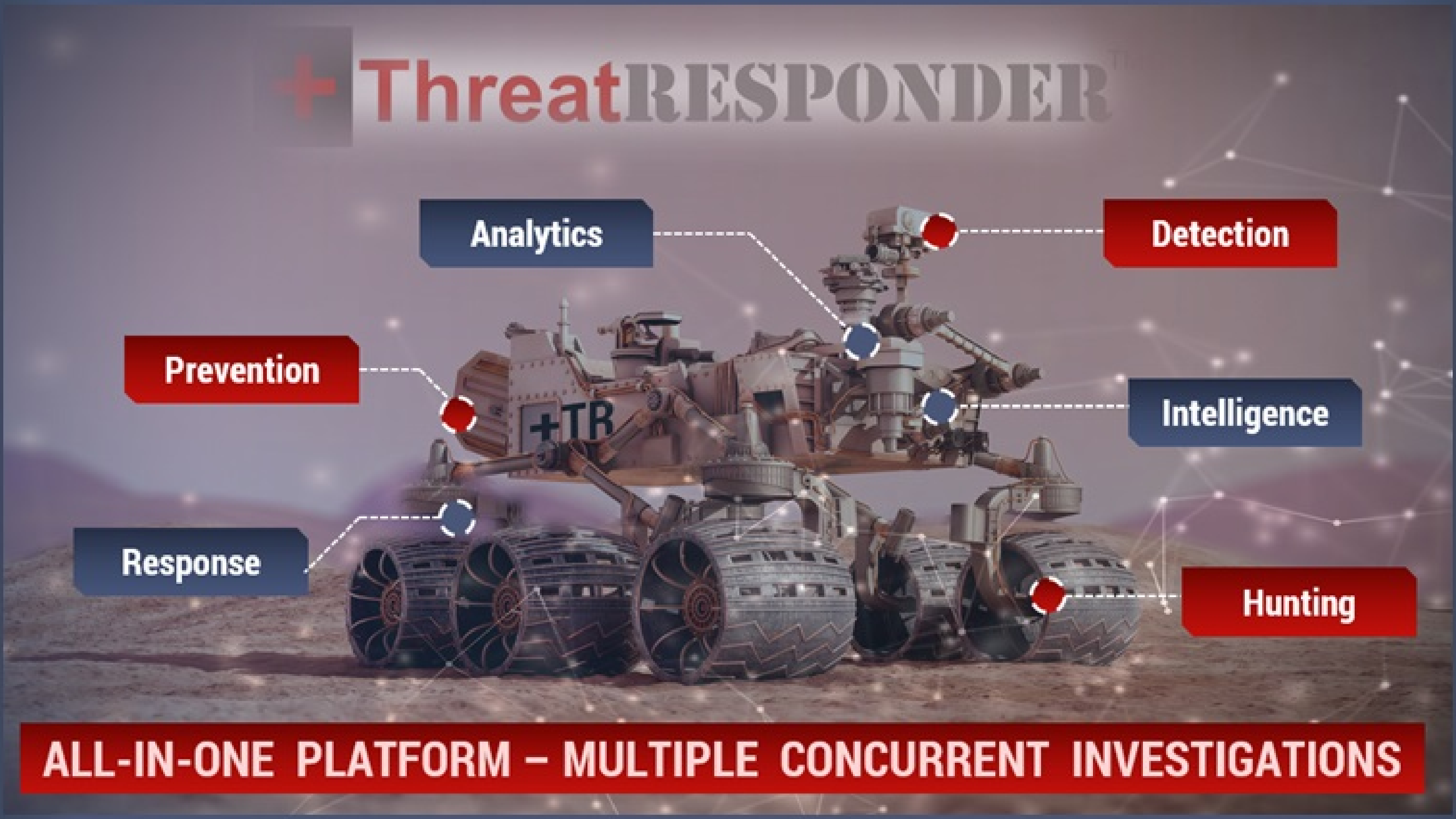
Ubuntu Security Notice 5873-1 - It was discovered that Go Text incorrectly handled certain encodings. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. It was discovered that Go Text incorrectly handled certain BCP 47 language tags. An attacker could possibly use this issue to cause a denial of service. CVE-2020-28851, CVE-2020-28852, and CVE-2021-38561 affected only Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

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



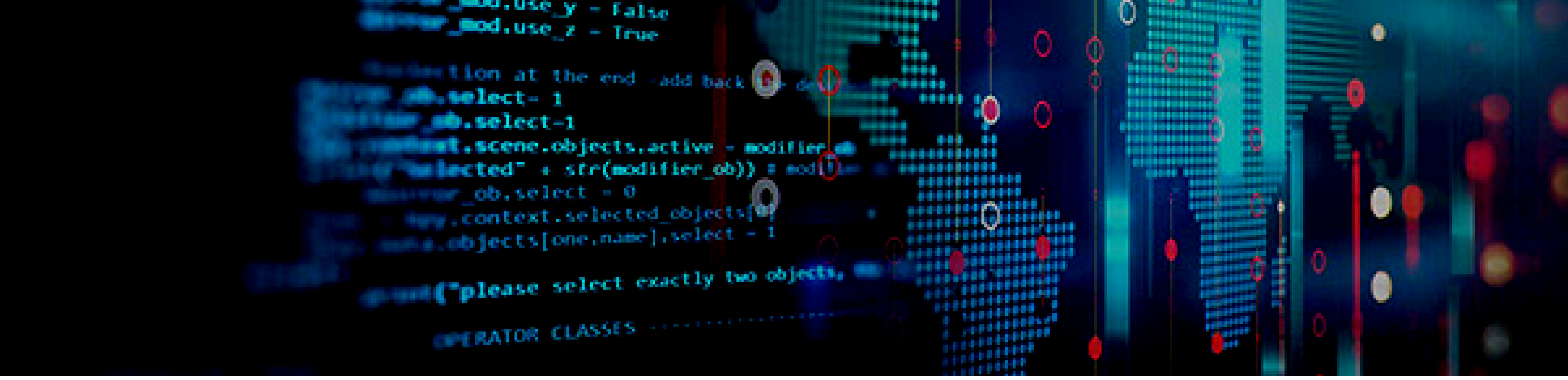
The Solution – ThreatResponder® Platform

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



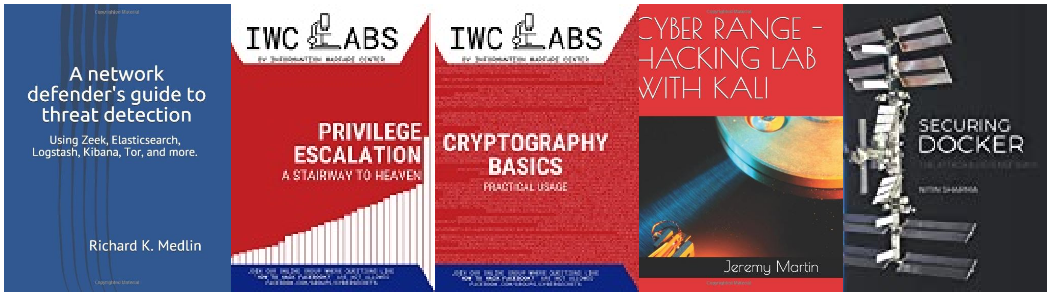
The Cyber Secrets publications on Amazon

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
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel
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 DO NOT CROSS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV