Mar-14-22

CYBER WEEKLY AWARENESS REPORT

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

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

March 14, 2022

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

Summary

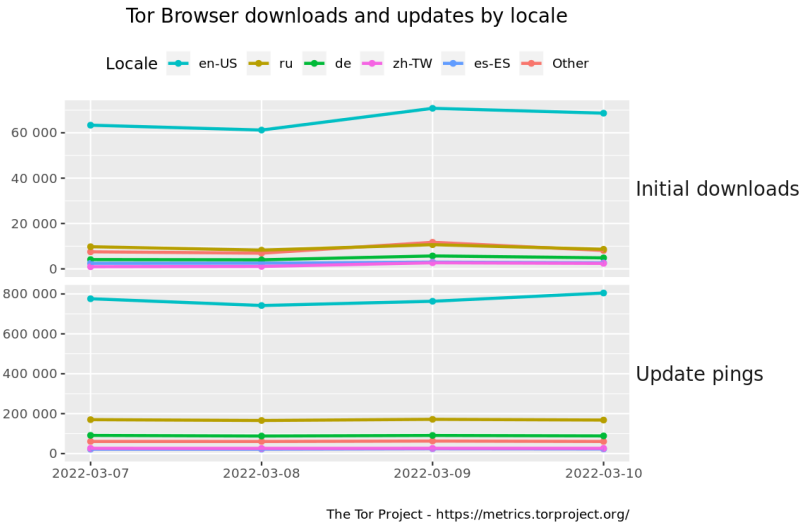
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



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

Packet Storm Security

* NetWalker Ransomware Affiliate Extradited To The US For Further Charges
* 'We Are Not Ready': A Cyber Expert On US Vulnerability To A Russian Attack
* DDoS Releases Alleged Leak Of Russian Censorship Agency
* Raccoon Stealer Crawls Into Telegram
* Moscow To Issue HTTPS Certs To Russian Websites
* Republican County Clerk Indicted In Voting Machine Breach, Arrest Warrant Issued
* Alleged REvil Suspect Extradited And Arraigned On Ransomware Spree Charges
* Mitel VoIP Systems Used In Staggering DDoS Attacks
* Qakbot Botnet Sprouts Fangs, Injects Malware Into Email Threads
* Bugcrowd's Top Bug Bounty Reward Increases To $1 Million
* Russia May Use Ransomware Payouts To Avoid Sanctions
* Chinese APT Zero Days Compromised US State Governments
* New Method That Amplifies DDoSes By 4 Billion-Fold. What Could Go Wrong?
* Millions Of APC Smart-UPS Devices Vulnerable To TLStorm
* Seventy-One Vulnerabilities Addressed By Microsoft On Patch Tuesday
* Linux Has Been Bitten By Its Most High Severity Bug In Years
* Russia Mulls Legalizing Software Piracy As It's Cut Off From Western Tech
* 7 Vulnerabilities Patched In Axeda IIoT Remote Mgmt Tool
* Phishing Attempts From FancyBear And Ghostwriter Stepping Up
* AutoWarp: Critical Cross-Account Vulnerability In Microsoft Azure Automation Service
* Google Is Buying Mandiant For $5.4 Billion
* Global Consultancies Quit Russia
* Hackers Stoke Pandemonium Amid Russia's War In Ukraine
* Massive Meris Botnet Embeds Ransomware Notes From REvil
* Mozilla Fixes Two Critical Firefox Flaws That Are Being Actively Exploited

Krebs on Security

* Report: Recent 10x Increase in Cyberattacks on Ukraine
* Microsoft Patch Tuesday, March 2022 Edition
* Internet Backbone Giant Lumen Shuns .RU
* Conti Ransomware Group Diaries, Part IV: Cryptocrime
* Conti Ransomware Group Diaries, Part III: Weaponry
* Conti Ransomware Group Diaries, Part II: The Office
* Conti Ransomware Group Diaries, Part I: Evasion
* Russia Sanctions May Spark Escalating Cyber Conflict
* IRS: Selfies Now Optional, Biometric Data to Be Deleted
* Report: Missouri Governor's Office Responsible for Teacher Data Leak

Dark Reading

* When IT Spending Plans Don't Reflect Security Priorities
* The Fight Against the Hydra: New DDoS Report from Link11
* How Enterprises Can Get Used to Deploying AI for Security
* Is XDR Right for My Organization?
* Identity Attacks Threaten Workloads, Not Just Humans
* Ukrainian Man Arrested for Alleged Role in Ransomware Attack on Kaseya, Others
* How to Combat the No. 1 Cause of Security Breaches: Complexity
* Over 40% of Log4j Downloads Are Vulnerable Versions of the Software
* Security Teams Prep Too Slowly for Cyberattacks
* Spotlight on First Dan Kaminsky Fellow: Jonathan Leitschuh
* Ex-Canadian Government Employee Charged in NetWalker Ransomware Attacks
* Cyber Insurance and Business Risk: How the Relationship Is Changing Reinsurance & Policy Guidance
* Why You Should Be Using CISA's Catalog of Exploited Vulns
* Log4j and Livestock Apps: APT41 Wages Persistent Cyberattack Campaign on US Government
* What Security Controls Do I Need for My Kubernetes Cluster?
* FBI Alert: Ransomware Attacks Hit Critical Infrastructure Organizations
* Bitdefender Launches New Password Manager Solution for Consumers
* Palo Alto Networks Introduces Prisma Cloud Supply Chain Security
* The Cloud-Native Opportunity for Zero Trust
* 10 Signs of a Poor Security Leader

The Hacker News

* Researchers Find New Evidence Linking Kwampirs Malware to Shamoon APT Hackers
* Multiple Security Flaws Discovered in Popular Software Package Managers
* Russian Pushing New State-run TLS Certificate Authority to Deal With Sanctions
* Here's How to Find if WhatsApp Web Code on Your Browser Has Been Hacked
* Iranian Hackers Targeting Turkey and Arabian Peninsula in New Malware Campaign
* New Exploit Bypasses Existing Spectre-V2 Mitigations in Intel, AMD, Arm CPUs
* Ukrainian Hacker Linked to REvil Ransomware Attacks Extradited to United States
* Emotet Botnet's Latest Resurgence Spreads to Over 100,000 Computers
* Hackers Abuse Mitel Devices to Amplify DDoS Attacks by 4 Billion Times
* Critical Bugs Could Let Attackers Remotely Hack, Damage APC Smart-UPS Devices
* The Incident Response Plan - Preparing for a Rainy Day
* Chinese APT41 Hackers Broke into at Least 6 U.S. State Governments: Mandiant
* Critical RCE Bugs Found in Pascom Cloud Phone System Used by Businesses
* Critical Security Patches Issued by Microsoft, Adobe and Other Major Software Firms
* New 16 High-Severity UEFI Firmware Flaws Discovered in Millions of HP Devices

Security Week

* Filter Blocked 70,000 Emails to Indiana Lawmakers on Bill
* Hacked US Companies to Face New Reporting Requirements
* Google Attempts to Explain Surge in Chrome Zero-Day Exploitation
* Russian Cyber Restraint in Ukraine Puzzles Experts
* High-Severity Vulnerabilities Patched in Omron PLC Programming Software
* Meta Releases Open Source Browser Extension for Checking Code Authenticity
* Canadian NetWalker Ransomware Operator Extradited to U.S.
* EU Lawmakers to Probe 'Political' Pegasus Spyware Use
* U.S. Warns of Conti Ransomware Attacks as Gang Deals With Leak Fallout
* From Cyber Threats to Cyber Talent, Insights From the Front Lines
* 1Password Increases Top Bug Bounty Reward to $1 Million
* Vodafone Investigating Source Code Theft Claims
* Threat Intelligence Firm Cybersixgill Raises $35 Million
* New Variant of Spectre Attack Bypasses Intel and Arm Hardware Mitigations
* All About the Bots: What Botnet Trends Portend for Security Pros
* China's Hacking of European Diplomats Aligns With Russia-Ukraine Conflict
* Italy Fines US Facial Recognition Firm
* Alleged Ukrainian Hacker in US Court After Extradition From Poland
* HelpSystems to Acquire MDR Services Firm Alert Logic
* Google Blocks Chinese Phishing Campaign Targeting U.S. Government
* Security Leaders Find Value in Veterans to Solve Cyber Skills Shortage
* Siemens Addresses Over 90 Vulnerabilities Affecting Third-Party Components
* Security and the Peter Principle - Seven Signs That You Are Working for a "Peter"
* Mitel Devices Abused for DDoS Vector With Record-Breaking Amplification Ratio
* Microsoft Warns of Spoofing Vulnerability in Defender for Endpoint

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Email-Based Vishing Attacks Skyrocket 554% as Phishing, Social Media, and Malware Attacks Are All on
* "Warm Greetings" (or not) : Saudi Aramco Impersonation
* Phishing and Scam Pages Increase by 153% as Cybercriminals Seek to Establish Credibility
* Passwords are Reused 64% of the Time as the Number of Passwords to Remember Reaches Over 100
* KnowBe4's Position On Recent Russian Aggression
* Up and To the Right: Ransomware Attacks Grow by 105% in 2021
* 83% of all Successful Ransomware Attacks Featured Double and Triple Extortion
* Social Engineering a Major Factor in Cyberattack on Camera Maker Axis Communications
* Domains Associated with Phishing Directed Against Ukraine
* Phishing Impersonation and Attack Trends in 2021

ISC2.org Blog

* Changes to the CISSP Exam Length Coming Soon
* KnowBe4 Spreads Cyber Awareness Training to Their Community
* The Dilemma of Defense in Depth
* Women in Cyber Webinar - Tackling Gender Bias and Defining Success
* CELEBRATING YOUNG WOMEN IN CYBERSECURITY - WEIJIA YAN, (ISC)² UNDERGRADUATE SCHOLARSHIP RECIPIEN

HackRead

* Anonymous sent 7 million texts to Russians plus hacked 400 of their security cams
* Cyber Security Incident Pushes Ubisoft to Issue Internal Password Reset
* Anonymous Hacks Russian Media Censoring Agency Roskomnadzor
* Alleged Ukrainian Member of REvil Ransomware Gang Extradited to US
* Anonymous & its affiliates hacked 90% of Russian misconfigured databases
* Is Hacktivism Good or Bad? How Could It Affect Your Business?
* Top Cybersecurity Trends to Watch Out for in 2022

Koddos

* Anonymous sent 7 million texts to Russians plus hacked 400 of their security cams
* Cyber Security Incident Pushes Ubisoft to Issue Internal Password Reset
* Anonymous Hacks Russian Media Censoring Agency Roskomnadzor
* Alleged Ukrainian Member of REvil Ransomware Gang Extradited to US
* Anonymous & its affiliates hacked 90% of Russian misconfigured databases
* Is Hacktivism Good or Bad? How Could It Affect Your Business?
* Top Cybersecurity Trends to Watch Out for in 2022

Naked Security

* Alleged Kaseya ransomware attacker arrives in Texas for trial
* S3 Ep73: Ransomware with a difference, dirty Linux pipes, and much more [Podcast + Transcript]
* "Dirty Pipe" Linux kernel bug lets anyone write to any file
* Adafruit suffers GitHub data breach - don't let this happen to you
* Firefox patches two actively exploited 0-day holes: update now!
* S3 Ep72: AirTag stalking, web server coding woes and Instascams [Podcast + Transcript]
* Ransomware with a difference: "Derestrict your software, or else!"
* Instagram scammers as busy as ever: passwords and 2FA codes at risk
* Did we learn nothing from Y2K? Why are some coders still stuck on two digit numbers?
* S3 Ep71: VMware escapes, PHP holes, WP plugin woes, and scary scams [Podcast + Transcript]

Threat Post

* Russia Issues Its Own TLS Certs
* Raccoon Stealer Crawls Into Telegram
* Malware Posing as Russia DDoS Tool Bites Pro-Ukraine Hackers
* Most Orgs Would Take Security Bugs Over Ethical Hacking Help
* Russia May Use Ransomware Payouts to Avoid Sanctions' Financial Harm
* Multi-Ransomwared Victims Have It Coming-Podcast
* Qakbot Botnet Sprouts Fangs, Injects Malware into Email Threads
* APT41 Spies Broke Into 6 US State Networks via a Livestock App
* Most ServiceNow Instances Misconfigured, Exposed
* Russian APTs Furiously Phish Ukraine - Google

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

IBM Security Intelligence

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

InfoWorld

* Microsoft pushes optional type annotations for JavaScript
* Google, Microsoft, Apple, Mozilla address browser pain points
* The biggest obstacle to cloud is people
* What is a serverless database? Elastic compute for the data tier
* React 18 brings concurrent renderer, automatic batching
* Project Loom: Understand the new Java concurrency model
* How to work with disconnected entities in Entity Framework Core
* How Trade Ledger switched to microservices for its cloud-based software
* Microsoft opens Azure-based Startups Founders Hub, easing eligibility rules
* In an evolving cloud world, Azure passes AWS

C4ISRNET - Media for the Intelligence Age Military

* Why has Russia's emerging tech had so little impact on its invasion of Ukraine?
* Congress wants to give Air Force an extra $65 million for ABMS
* Lawmakers recommend $800 million budget increase for defense lab and testing infrastructure
* How JADC2 is improving nuclear command and control
* Proposed Space Development Agency funding boost falls short of earlier request
* How to improve the force? Info and tech investments, says HASC chair.
* NORTHCOM needs better sensors to protect against Russian submarine, missile threat
* Washington must do more to support companies facing Russian hackers
* BAE Systems buys military simulations firm for $200 million
* Five steps the Defense Department should consider for its data management strategy

The Hacker Corner

Conferences

* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The Hybrid Conference Model
* Best Ways To Market A Conference

Google Zero Day Project

* A walk through Project Zero metrics
* Zooming in on Zero-click Exploits

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.

* picoCTF 2022
* zer0pts CTF 2022
* Hack In Tangerang Kota Capture the Flag 2022 Quals
* VishwaCTF 2022
* OFPPT-CTF Morocco
* T3N4CI0US CTF 2022
* Wicked 6: 2022 Women's Global Cyber League
* Insomni'hack 2022
* LINE CTF 2022
* Space Heroes CTF

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

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

Tools & Techniques

Packet Storm Security Tools Links

* Falco 0.31.1
* UFONet 1.8
* Samhain File Integrity Checker 4.4.7
* GRAudit Grep Auditing Tool 3.4
* Packet Fence 11.2.0
* OpenSSH 8.9p1
* I2P 1.7.0
* OpenStego Free Steganography Solution 0.8.4
* TestSSL 3.0.7
* Collabfiltrator 2.1

Kali Linux Tutorials

* CRT : CrowdStrike Reporting Tool for Azure
* Mininode : A CLI Tool To Reduce The Attack Surface Of The Node.js Applications By Using Static Analys
* Gh-Dork : Github Dorking Tool
* BloodyAD : An Active Directory Privilege Escalation Framework
* Ninjas workout : Vulnerable NodeJS Web Application
* FACT : A Tool To Collect, Process And Visualise Forensic Data From Clusters Of Machines
* Xolo : Tool To Crawl, Visualize And Interact With SQL Server Links In A D3 Graph
* Dontgo403 : Tool To Bypass 40X Response Codes
* VulnLab : A Web Vulnerability Lab Project
* Http2Smugl : Tool to detect and exploit HTTP request smuggling

GBHackers Analysis

* Critical Flaws With Cisco Expressway Series and TelePresence VCS Let Attackers Execute Arbitrary Code
* Flaws With Horde Webmail Let Attackers Gain Full Access to the Email Account
* VMware Issues Patches for Shell Injection and Privilege Vulnerability
* Critical Magento 0-Day Let Attackers Execute Arbitrary Code
* ACTINIUM Hackers Group Targeting Government, Military, NGO to Steal Sensitive Data

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Network Forensics: Tools of the Trade… At Scale and on a Budget
* You Get What You Ask For: Building Intelligent Teams for CTI Success - CTI Summit 2022
* SANS Threat Analysis Rundown

Defcon Conference

* DEF CON 29 Ham Radio Village - Kurtis Kopf - An Introduction to RF Test Equipment
* DEF CON 29 Ham Radio Village - Tyler Gardner - Amateur Radio Mesh Networking
* DEF CON 29 Ham Radio Village - Bryan Fields - Spectrum Coordination for Amateur Radio
* DEF CON 29 Ham Radio Village - Eric Escobar - Getting started with low power/long distance Comms

Hak5

* Cyberwarfare: Ukraine vs Russia - ThreatWire
* Live Hacking Q&A with Kody and Alex
* Can Wireshark Spot Hidden Cameras For Free?

The PC Security Channel [TPSC]

* Hermetic Wiper: Ukraine Cyberattack Analysis
* Standard vs Admin User: Ransomware Test

Eli the Computer Guy

* DELETING VIDEOS - download your rawrs now
* Louis Rossmann WINS - I'm Going on Hiatus
* NEW MACBOOK PRO's with M1 Pro and M1 MAX are AWESOME
* DON'T GET A CYBERSECURITY DEGREE

Security Now

* Rogue Nation Cyber Consequences - Russia vs. Ukraine, Crypto, StarLink, Namecheap, Telegram
* Trust Dies in Darkness - Samsung's TrustZone Keymaster Design, Daxin, Windows 11 compatibility

Troy Hunt

* Weekly Update 286

Intel Techniques: The Privacy, Security, & OSINT Show

* 253-Dash Cams
* 252-Secure Communications Conversion

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Seowon SLR-120 Router Remote Code Execution
* Employee Performance Evaluation System 1.0 SQL Injection
* Tdarr 2.00.15 Command Injection
* FLEX 1080/1085 Web 1.6.0 Information Disclosure
* Dirty Pipe Local Privilege Escalation
* Zabbix 5.0.17 Remote Code Execution
* Siemens S7-1200 4.5 Unauthenticated Access
* WOW21 5.0.1.9 Unquoted Service Path
* Sandboxie-Plus 5.50.2 Unquoted Service Path
* McAfee Safe Connect VPN Unquoted Service Path
* BattlEye 0.9 Unquoted Service Path
* Sony Playmemories Home Unquoted Service Path
* DEOS AG OPEN 710/810 Cross Site Scripting
* Audio Conversion Wizard 2.01 Buffer Overflow
* Printix Client 1.3.1106.0 Privilege Escalation
* Webmin 1.984 Remote Code Execution
* Cobian Backup 0.9 Unquoted Service Path
* Wondershare Dr.Fone 12.0.18 Unquoted Service Path
* Dirty Pipe SUID Binary Hijack Privilege Escalation
* Dirty Pipe Linux Privilege Escalation
* Apache APISIX Remote Code Execution
* Attendance And Payroll System 1.0 Remote Code Execution
* Attendance And Payroll System 1.0 SQL Injection
* Hasura GraphQL 2.2.0 Information Disclosure
* Spring Cloud Gateway 3.1.0 Remote Code Execution

CXSecurity

* Dirty Pipe Local Privilege Escalation
* Zabbix 5.0.17 Remote Code Execution
* Audio Conversion Wizard 2.01 Buffer Overflow
* Linux Kernel 5.8
* Apache APISIX Remote Code Execution
* pfSense 2.5.2 Shell Upload
* Microsoft Exchange Server Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

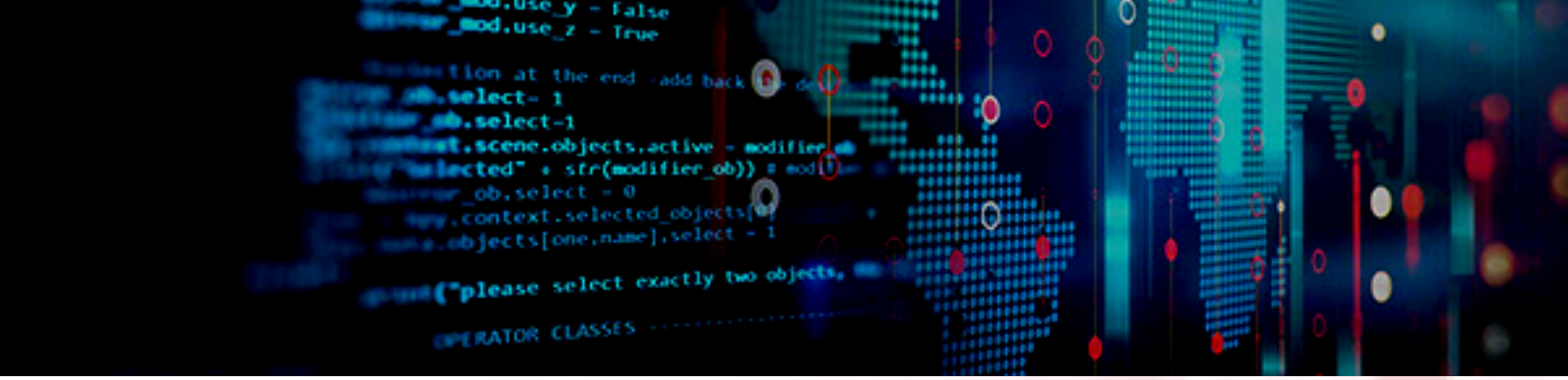
* [remote] Tdarr 2.00.15 - Command Injection
* [remote] Seowon SLR-120 Router - Remote Code Execution (Unauthenticated)
* [remote] Siemens S7-1200 - Unauthenticated Start/Stop Command
* [local] Sandboxie-Plus 5.50.2 - 'Service SbieSvc' Unquoted Service Path
* [local] WOW21 5.0.1.9 - 'Service WOW21_Service' Unquoted Service Path
* [local] Sony playmemories home - 'PMBDeviceInfoProvider' Unquoted Service Path
* [webapps] Zabbix 5.0.17 - Remote Code Execution (RCE) (Authenticated)
* [local] BattlEye 0.9 - 'BEService' Unquoted Service Path
* [local] McAfee(R) Safe Connect VPN - Unquoted Service Path Elevation Of Privilege
* [local] Wondershare Dr.Fone 12.0.18 - 'Wondershare InstallAssist' Unquoted Service Path
* [local] Printix Client 1.3.1106.0 - Privilege Escalation
* [local] Audio Conversion Wizard v2.01 - Buffer Overflow
* [local] Cobian Backup 0.9 - Unquoted Service Path
* [webapps] Webmin 1.984 - Remote Code Execution (Authenticated)
* [local] Linux Kernel 5.8
* [local] Foxit PDF Reader 11.0 - Unquoted Service Path
* [local] Malwarebytes 4.5 - Unquoted Service Path
* [local] Cloudflare WARP 1.4 - Unquoted Service Path
* [local] Private Internet Access 3.3 - 'pia-service' Unquoted Service Path
* [webapps] Hasura GraphQL 2.2.0 - Information Disclosure
* [webapps] Attendance and Payroll System v1.0 - SQLi Authentication Bypass
* [webapps] Attendance and Payroll System v1.0 - Remote Code Execution (RCE)
* [webapps] part-db 0.5.11 - Remote Code Execution (RCE)
* [webapps] Spring Cloud Gateway 3.1.0 - Remote Code Execution (RCE)
* [remote] Printix Client 1.3.1106.0 - 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*

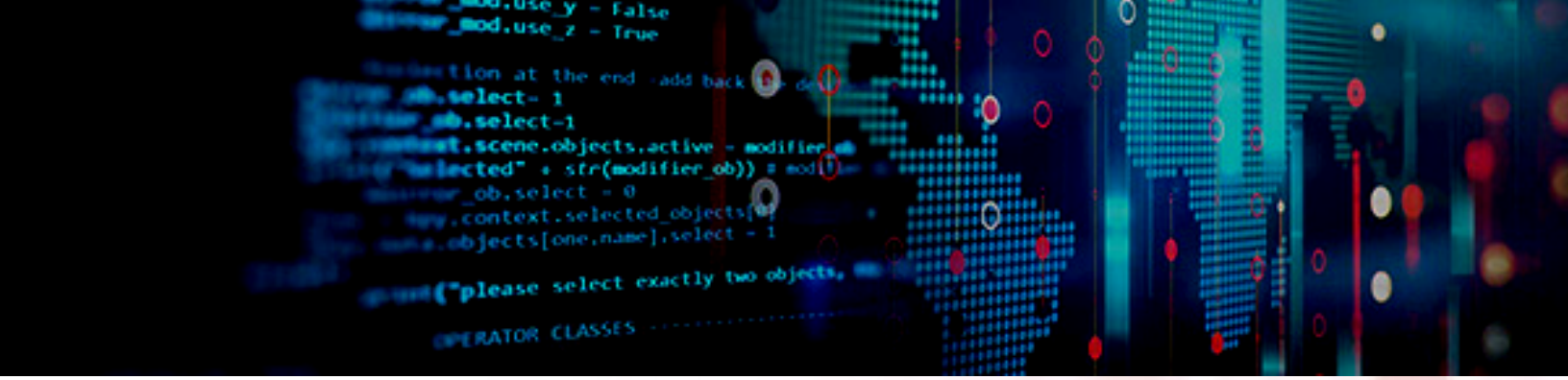
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.nanchital.gob.mx
http://www.nanchital.gob.mx notified by MarkwelliPukaskwA
http://zie.go.tz/sp1cy.php
http://zie.go.tz/sp1cy.php notified by sp1cy
https://zvapfier.gov.al/h28.html
https://zvapfier.gov.al/h28.html notified by H28
https://training.gov.np
https://training.gov.np notified by djebbaranon
http://danangtourism.gov.vn/luffy.html
http://danangtourism.gov.vn/luffy.html notified by ph.luffy
https://www.gppb.gov.ph/indo.php
https://www.gppb.gov.ph/indo.php notified by Imkey7
https://opd.pesisirbaratkab.go.id
https://opd.pesisirbaratkab.go.id notified by ./G1L4N6_ST86
http://kvda.gov.np
http://kvda.gov.np notified by djebbaranon
http://doad.p5.gov.np/o.txt
http://doad.p5.gov.np/o.txt notified by Mr.ToKeiChun69
https://www.albptc.gov.np/o.txt
https://www.albptc.gov.np/o.txt notified by Mr.ToKeiChun69
http://phd.gov.np/o.txt
http://phd.gov.np/o.txt notified by Mr.ToKeiChun69
http://fmd.gov.np/o.txt
http://fmd.gov.np/o.txt notified by Mr.ToKeiChun69
https://lacendf.saude.df.gov.br
https://lacendf.saude.df.gov.br notified by Paraná Cyber Mafia
https://jucis.df.gov.br
https://jucis.df.gov.br notified by Paraná Cyber Mafia
https://www.turismo.df.gov.br
https://www.turismo.df.gov.br notified by Paraná Cyber Mafia
https://www.internacional.df.gov.br
https://www.internacional.df.gov.br notified by Paraná Cyber Mafia
https://www.arpdf.df.gov.br
https://www.arpdf.df.gov.br notified by Paraná Cyber Mafia



Dark Web News

Darknet Live

Austrian Man Arrested for Alleged Amphetamine Purchase

The Styria State Police Directorate announced the arrest of a 28-year-old man from Fürstenfeld, Styria, for allegedly ordering amphetamine and ecstasy on the darkweb. The investigation began on February 9, 2022, when Customs officers in Vienna intercepted a suspicious package. The package was allegedly addressed to the suspect. Authorities opened the package and reportedly discovered unspecified quantities of amphetamine and ecstasy. On March 8, the Fürstenfeld Police Inspectorate executed a search warrant at the suspect's home. The search resulted in the seizure of 75 LSD tabs, 110 grams of cannabis, six cannabis plants, cannabis oil, and growing equipment. The 28-year-old "did not confess,” according to the police. He is currently in police custody. archive.org (via darknetlive.com at https://darknetlive.com/post/austrian-man-arrested-for-alleged-amphetamine-purchase/)

Washington Man Admits Selling Fake Oxys on the Darkweb

A Washington man pleaded guilty to distributing a wide variety of drugs through the darkweb. According to court documents, 28-year-old Nicholas Partlow of Issaquah, Washington, distributed fentanyl, heroin, methamphetamine, and other drugs through undisclosed darkweb marketplaces. Partlow also admitted to possession of firearms during his drug trafficking operation. In total, Partlow had more than 400 completed transactions on darkweb marketplaces. Through his darknet sales, Partlow sold an aggregate amount of at least 52 grams of heroin, 13 grams of methamphetamine, 142 pills containing fentanyl, 866 suboxone strips, and 1,513 pills containing other controlled substances. The pills containing fentanyl were counterfeit oxycodone pills. In 2020, postal inspectors ordered drugs from Partlow's vendor account on an undisclosed marketplace. Court documents do not reveal the identity of the vendor account Partlow had operated. The drugs ordered by undercover feds included 1 gram of heroin, 4.07 grams of methamphetamine, and 79 pills containing other controlled substances. Feds also intercepted packages Partlow had shipped to his customers. The intercepted packages contained 3.25 grams of heroin, two pills containing fentanyl, 18 suboxone strips, and 1,680 pills containing other controlled substances. On November 18, 2020, feds executed a federal search warrant at a house in Issaquah, Washington, where Partlow was living. During the search, agents found 21.446 grams of heroin, 27.234 grams of methamphetamine, a bottle of GHB, 27 pills containing fentanyl,

As of the acceptance of the plea agreement, the darknet includes zero of those sites. 0.859 grams of Ketamine, and 33 pills containing other controlled substances. They also found supplies that Partlow used for selling and shipping drugs, including a scale, U.S. Postal Service envelopes, bags, and vacuum-seal bags. Agents seized five firearms, $4,360 in cash, a Trezor cold storage wallet, jewelry, and several electronic devices. After the November 18, 2020, search, Partlow knowingly and voluntarily gave law enforcement permission to seize all cryptocurrency funds from any darknet markets associated with him and all cash found in the November 18 search. Approximately 11.219267790574 Monero (XMR) cryptocurrency and 0.0064688 BTC (Bitcoin cryptocurrency) were seized on or about December 11, 2020. Partlow admits that the cash and cryptocurrency funds are, or are traceable to, proceeds from the drug trafficking conspiracy After the house search on November 18, 2020, Partlow continued to sell drugs to his customers. On March 31, 2021, police in

Bellevue, Washington, caught Partlow and an associate using heroin in a parking garage. Partlow possessed 27 counterfeit oxycodone pills, five alprazolam pills, and a drug ledger notebook containing information about his transactions. Authorities freed Partlow after the March 31, 2021 arrest. On September 9, 2021, in Renton, Washington, Partlow crashed a car. A federal warrant had already been issued for Partlow's arrest. When the police showed up at the accident scene, they arrested Partlow. In his possession, the police found 57 pills marked as Xanax, 12 blue pills marked "M30,” and 0.05 grams of methamphetamine. Partlow had a taser in his pocket. He also had a silver, key-shaped LaCie brand computer thumb drive. On March 7, 2022, the defendant pleaded guilty to conspiring to distribute controlled substances and to possessing firearms in furtherance of a drug trafficking crime. Partlow agreed to forfeit assets found in his possession, including approximately 11.2192 Monero and 0.0064688 Bitcoin. On July 1, 2022, Partlow will be sentenced by US District Judge Richard A. Jones in the US District Court in Seattle. He could be sentenced to 20 years in prison for conspiracy to distribute drugs and a minimum of five years for the firearms offense. archive.ph/archive.org plea agreement (pdf) (via darknetlive.com at https://darknetlive.com/post/washington-man-admits-selling-counterfeit-oxys-on-the-darkweb/)

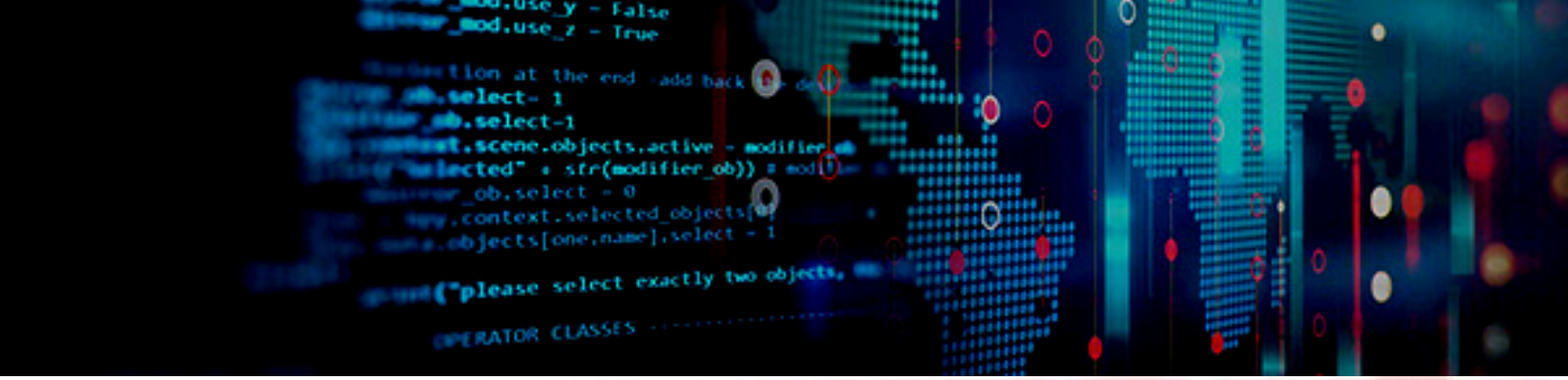
Dread V3: New Captcha, Market Standards, Search, and More

Dread is back online. The update, Dread V3, includes some of the most significant changes in Dread's history. The most obvious and perhaps most welcome changes include new captchas. The developers of Dread-HugBunter, Paris, and whoever else-reworked the site's search function to include a full-text index of Dread's 2+ million posts, suggestions, fuzziness adjustments, and various search operations. Dread V3 provides several avenues through which Dread can generate income, including a premium membership and a shop with trophies. Upvoting or downvoting a post or comment no longer refreshes the page. The use of a form within an iframe is not something I have seen on any other site. __ No page refresh! Paris covered many changes in the "Welcome to Dread V3” post. One significant change I did not see Paris mention was the new "Market Standards” chart. (dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/page/marketstandards/) Rejection Negative Positive Super Positive Script Markets - No or minimal skin No/little organic growth @ 3 Months Accepts Monero Harm Reduction Efforts Bitcoin Only (no multisig) No Monero Support Bitcoin Multisig Lightweight, Custom Stylesheet (__ Coinbase BTC > Electrum Wallet Windows > Electrum Wallet Tails > Vendor. Laundering 101. Banning Russian Addresses _ Coinbase recently published a blog post about enforcing sanctions on users in various countries. Unlike Uphold, Coinbase claims to be banning sanctioned individuals instead of an entire nation. Coinbase CEO Brian Armstrong has opposed calls from outraged Twitter users to restrict the accounts of all Russian Coinbase users. People should not expect Coinbase or other legitimate companies operating in the United States to ignore sanctions. Like it or not, that is just the reality of the situation. Such an expectation is akin to expecting an email service to tell law enforcement "no” when the feds show up with a subpoena for a user's email address. But these companies are under no legal obligation to ban an entire country. Companies taking action against their Russian customers are just signaling and allowing an emotional mob to dictate their decisions. __ His opposition to the banning of Russians is pretty weak. He will not be holding the line. The blog post blurred the lines between accounts held by regular Russian users and those used by sanctioned Russian oligarchs. Today, Coinbase blocks over 25,000 addresses related to Russian individuals or entities we believe to be engaging in illicit activity, many of which we have identified through our own proactive investigations. My personal opinion is that not all 25,000 addresses are associated with sanctioned Russians. Coinbase claimed to have "identified” most of these addresses before Russia invaded the Ukraine. "Once we identified these addresses, we shared them with the government to further support sanctions enforcement,” Paul Grewal, Coinbase Chief Legal Officer, wrote. Even Coinbase seems to be admitting that the blocked addresses belong to users who are not sanctioned. Coinbase: Why Not to Use Coinbase _ Coinbase, probably in a proactive defense of its existence, explained why digital assets enhanced the ability to detect sanction evasion. The explanations provided in the blog post apply to the illicit use of Coinbase or cryptocurrency in general. A possible exception is Monero (and perhaps other privacy coins). Public. Public blockchains offer

unprecedented visibility into the details of transactions, including information about the date and time of each transaction, the type of virtual asset transacted, the amount, the wallet addresses involved, and the unique transaction identifier. Suspicious transaction activity can be traced without needing to gather information from multiple financial institutions. These advantages for investigation and enforcement simply do not exist with cash transactions or transactions across multiple countries. Traceable. When applied to public blockchain data, analytics tools offer law enforcement additional capabilities. In many cases, law enforcement can trace the transaction history of a wallet from the very first transaction, follow transactions in real time, and group transactions according to risk level based on interactions with other wallets. Other techniques can help authorities to follow transactions between chains or through intermediaries. For example, Coinbase's proactive on-chain analysis identified more than 16,000 addresses possibly associated with Iranian exchanges, many of which had not yet been identified by others. We used this analysis to strengthen our compliance systems and inform law enforcement in order to enhance industry-wide awareness. Permanent. Once recorded on the blockchain, transactions remain immutable. No one (not crypto companies, not governments, not even bad actors) can destroy, alter, or withhold information to evade detection. There you have it. Why not to use Coinbase in the company's words. I am still skeptical about what the rest of their blog post means, though. Coinbase appears to be claiming that the 25,000 blocked addresses of Russian users are not associated with sanctioned individuals. Grewal throws an "or” in-between "Russian individuals” and "entities […] engaged in illicit activity.” Word games? I do not know. Nobody should do anything illegal anyway. But they certainly should not use Coinbase to do illegal things. I suppose the issues with Coinbase are not relevent to people who are using it for lawful purposes who do not care about linking their identity to their transactions or having their funds arbitrarily frozen. But nobody should store funds in a wallet outside of their control. I think they are the PayPal of the crypto world. Also, the Secret Service pays Coinbase for blockchain analysis software. (via darknetlive.com at https://darknetlive.com/post/coinbase-explained-why-criminals-should-avoid-coinbase/)

Dark Web Link

White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats
Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from “Dark web” persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that “you didn't take any shit from anyone.” During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug
Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

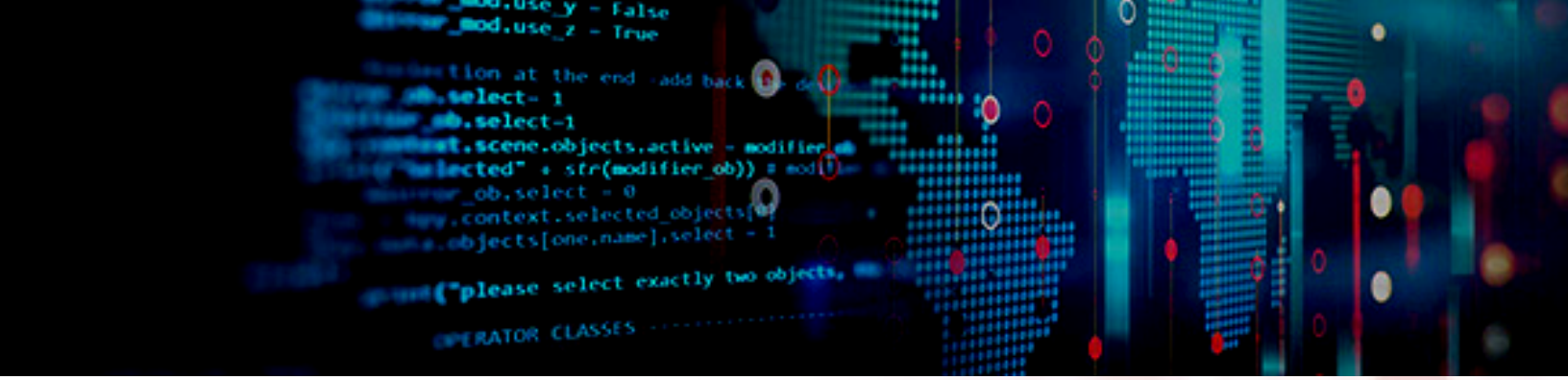
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* 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
* 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
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses

FireEye

* Metasploit Weekly Wrap-Up
* Run Faster Log Searches With InsightIDR
* 7Rapid Questions: Growing From BDR to Commercial Sales Manager With Maria Loughrey
* New US Law to Require Cyber Incident Reports
* CVE-2022-0847: Arbitrary File Overwrite Vulnerability in Linux Kernel
* 3 Reasons to Join Rapid7's Cloud Security Summit
* Patch Tuesday - March 2022
* InsightVM Scan Engine: Understanding MAC Address Discovery
* Metasploit Weekly Wrap-Up
* Graph Analysis of the Conti Ransomware Group Internal Chats



Advisories

US-Cert Alerts & bulletins

* Dirty Pipe Privilege Escalation Vulnerability in Linux
* Updated: Conti Ransomware
* Adobe Releases Security Updates for Multiple Products
* SAP Releases March 2022 Security Updates
* Microsoft Releases March 2022 Security Updates
* Mozilla Releases Security Updates
* FBI Releases Indicators of Compromise for RagnarLocker Ransomware
* CISA Releases Security Advisory on PTC Axeda Agent and Desktop Server
* AA22-057A: Destructive Malware Targeting Organizations in Ukraine
* AA22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government an
* Vulnerability Summary for the Week of February 28, 2022
* Vulnerability Summary for the Week of February 21, 2022

Zero Day Initiative Advisories

ZDI-CAN-16805: 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: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16861: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16539: Trend Micro
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 'Abdelhamid Naceri' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16754: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16757: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16755: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16784: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16792: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16788: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16793: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16790: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16785: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16787: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16786: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16791: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16789: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16865: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16803: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16809: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16794: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16863: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16864: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16817: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-11, 3 days ago. The vendor is given until 2022-07-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16724: Advantech

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 '@rgod777' was reported to the affected vendor on: 2022-03-09, 5 days ago. The vendor is given until 2022-07-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5322-1
Ubuntu Security Notice 5322-1 - Thomas Akesson discovered that Subversion incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service.
Red Hat Security Advisory 2022-0821-01
Red Hat Security Advisory 2022-0821-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0823-01
Red Hat Security Advisory 2022-0823-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0822-01
Red Hat Security Advisory 2022-0822-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements.
Red Hat Security Advisory 2022-0056-01
Red Hat Security Advisory 2022-0056-01 - 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 4.10.3. Issues addressed include bypass, cross site request forgery, denial of service, and traversal vulnerabilities.
Red Hat Security Advisory 2022-0820-01
Red Hat Security Advisory 2022-0820-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0818-01
Red Hat Security Advisory 2022-0818-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.7.0 ESR. Issues addressed include bypass, code execution, integer overflow, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0815-01
Red Hat Security Advisory 2022-0815-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.7.0 ESR. Issues addressed include bypass, code execution, integer overflow, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0816-01
Red Hat Security Advisory 2022-0816-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.7.0 ESR. Issues addressed include bypass, code execution, integer overflow, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0817-01
Red Hat Security Advisory 2022-0817-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.7.0 ESR. Issues addressed include bypass, code execution, integer overflow, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0825-01
Red Hat Security Advisory 2022-0825-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include denial of service, double free, memory leak, privilege escalation, and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-0826-01
Red Hat Security Advisory 2022-0826-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 6.0.103 and .NET Runtime 6.0.3. Issues addressed include a denial of service vulnerability.
Red Hat Security Advisory 2022-0827-01
Red Hat Security Advisory 2022-0827-01 - .NET is a managed-software framework. It implements a subset of

the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 3.1.417 and .NET Runtime 3.1.23. Issues addressed include buffer overflow and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0828-01

Red Hat Security Advisory 2022-0828-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 5.0.212 and .NET Runtime 5.0.15. Issues addressed include buffer overflow and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0829-01

Red Hat Security Advisory 2022-0829-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 3.1.417 and .NET Runtime 3.1.23. Issues addressed include buffer overflow and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0830-01

Red Hat Security Advisory 2022-0830-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 5.0.212 and .NET Runtime 5.0.15. Issues addressed include buffer overflow and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0831-01

Red Hat Security Advisory 2022-0831-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Red Hat Security Advisory 2022-0819-01

Red Hat Security Advisory 2022-0819-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include denial of service, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0824-01

Red Hat Security Advisory 2022-0824-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.7.0 ESR. Issues addressed include bypass, code execution, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0832-01

Red Hat Security Advisory 2022-0832-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address security vulnerabilities are now available. The updated versions are .NET SDK 6.0.103 and .NET Runtime 6.0.3. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-0055-01

Red Hat Security Advisory 2022-0055-01 - 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 4.10.3. Issues addressed include bypass and cross site scripting vulnerabilities.

Ubuntu Security Notice USN-5320-1

Ubuntu Security Notice 5320-1 - USN-5288-1 fixed several vulnerabilities in Expat. For CVE-2022-25236 it caused a regression and an additional patch was required. This update address this regression and several other vulnerabilities. It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service. It was discovered that Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.10.

Ubuntu Security Notice USN-5319-1

Ubuntu Security Notice 5319-1 - Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by Intel to their processors to address Spectre-BTI were

insufficient. A local attacker could potentially use this to expose sensitive information.

Red Hat Security Advisory 2022-0790-01

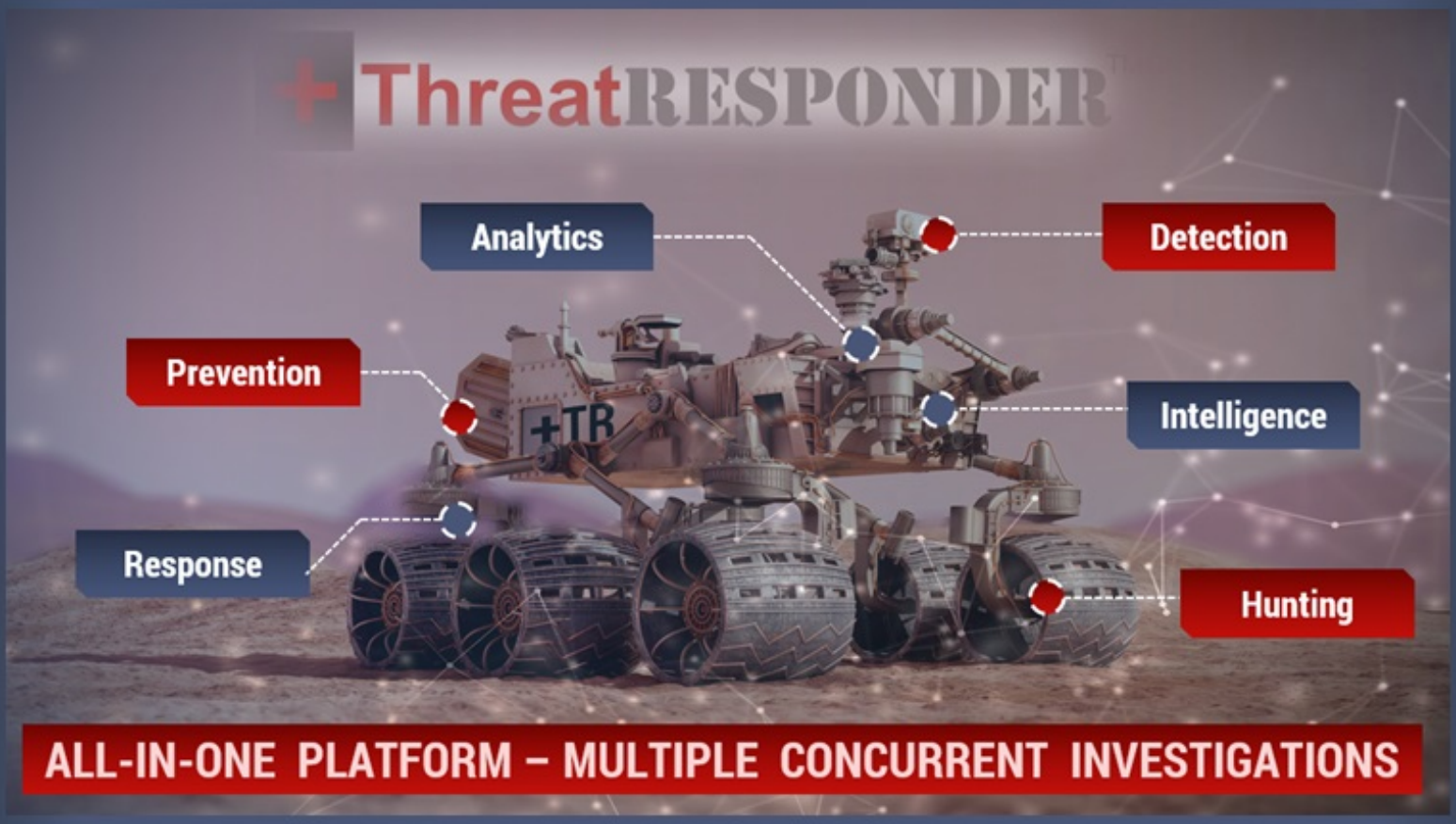
Red Hat Security Advisory 2022-0790-01 - Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments.

Are You...

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

Do DFIR Investigations Better

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



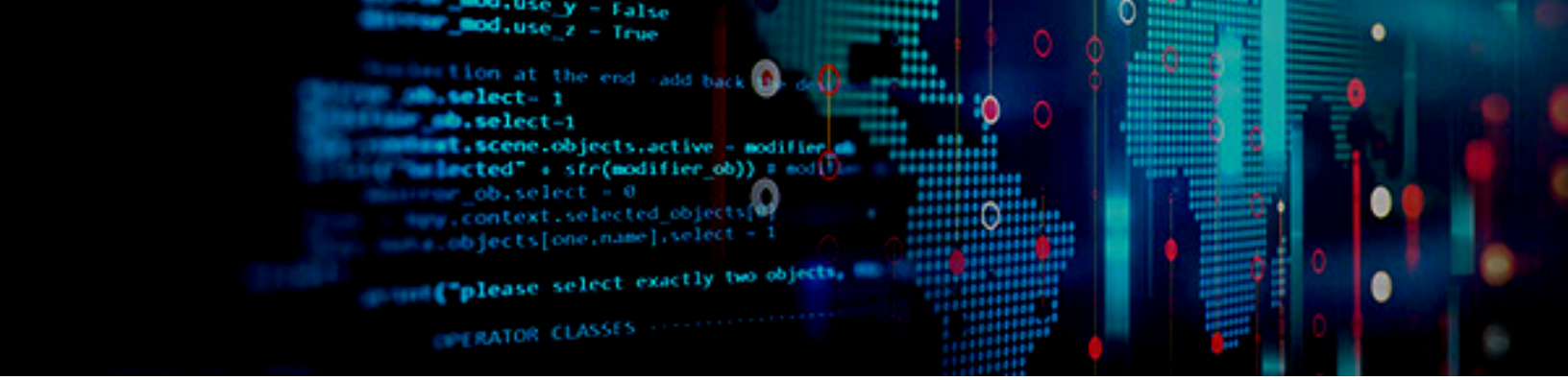
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

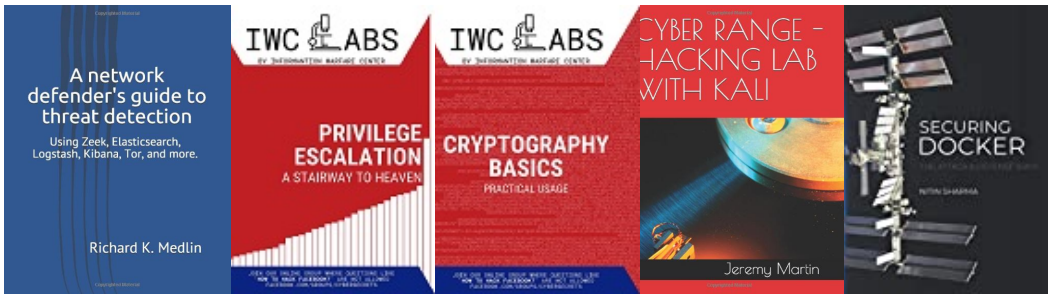


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP