Feb-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

February 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

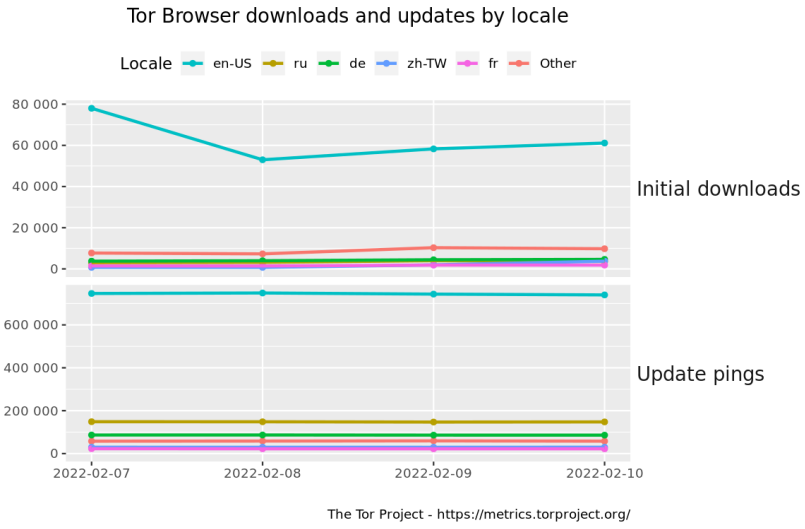
Internet Storm Center Infocon Status

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

Krebs on Security

* Russian Govt. Continues Carding Shop Crackdown
* Microsoft Patch Tuesday, February 2022 Edition
* IRS To Ditch Biometric Requirement for Online Access
* How Phishers Are Slinking Their Links Into LinkedIn
* Fake Investor John Bernard Sinks Norwegian Green Shipping Dreams
* Who Wrote the ALPHV/BlackCat Ransomware Strain?
* Scary Fraud Ensues When ID Theft & Usury Collide
* Crime Shop Sells Hacked Logins to Other Crime Shops
* IRS Will Soon Require Selfies for Online Access
* At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates

Dark Reading

* DDoS Attacks on a Tear in Q4 2021
* Aviatrix Enhances Secure Cloud Networking with Network Behavior Analytics
* Seven Key Ingredients to Effective Incident Response
* Google Paid Record $8.7 Million to Bug Hunters in 2021
* BlackBerry Seeks to Restore Its Past Glory With Services Push
* What CISOs Should Tell the Board About Log4j
* Retailers' Offboarding Procedures Leave Potential Risks
* Credential-Stuffing Attacks on Remote Windows Systems Took Off in 2021
* Apple Releases Security Update for Webkit Flaw
* Defense Contractors Need to Check Their Six
* Dynatrace Adds Real-Time Attack Detection and Blocking, Advancing Cloud Application Security
* Dynatrace Launches DevSecOps Automation Alliance Partner Program
* Orca Security Adds Expanded CIEM Capabilities and Multi-Cloud Security Score to Cloud Platform
* Allure Security Raises $6.8 Million Seed Funding Round
* Titaniam Secures $6 Million in Seed Funding
* Data Transparency Hasn't Made Us Safer Yet. Can It Uncover Breach Causality?
* Bot Marketplaces as a Source of Future Data Breaches
* Putting AI to Practical Use in Cybersecurity
* Experts: Several CVEs From Microsoft's February Security Update Require Prompt Attention
* Linux Malware on the Rise

The Hacker News

* Critical Magento 0-Day Vulnerability Under Active Exploitation - Patch Released
* Hackers Planted Fake Digital Evidence on Devices of Indian Activists and Lawyers
* France Rules That Using Google Analytics Violates GDPR Data Protection Law
* Apple Releases iOS, iPadOS, macOS Updates to Patch Actively Exploited Zero-Day Flaw
* FritzFrog P2P Botnet Attacking Healthcare, Education and Government Sectors
* COVID Does Not Spread to Computers
* CISA, FBI, NSA Issue Advisory on Severe Increase in Ransomware Attacks
* Russia Cracks Down on 4 Dark Web Marketplaces for Stolen Credit Cards
* Critical RCE Flaws in 'PHP Everywhere' Plugin Affect Thousands of WordPress Sites
* U.S. Arrests Two and Seizes $3.6 Billion Cryptocurrency Stolen in 2016 Bitfinex Hack
* Guide: Alert Overload and Handling for Lean IT Security Teams
* Iranian Hackers Using New Marlin Backdoor in 'Out to Sea' Espionage Campaign
* Russian APT Hackers Used COVID-19 Lures to Target European Diplomats
* Microsoft and Other Major Software Firms Release February 2022 Patch Updates
* Palestine-Aligned Hackers Use New NimbleMamba Implant in Recent Attacks

Security Week

* Ransomware Gang Says it Has Hacked 49ers Football Team
* Adobe Releases Emergency Patch for Exploited Commerce Zero-Day
* CISA Says 'HiveNightmare' Windows Vulnerability Exploited in Attacks
* Feds Oppose Immediate Release of Voting Machine Report
* India-Linked Threat Actor Involved in Spying, Planting Evidence
* Spanish Authorities Dismantle SIM Swapping Gang
* Google Paid Out $8.7 Million in Bug Bounty Rewards in 2021
* Lawmakers Introduce Combined Bill for Strengthening Critical Infrastructure Security
* Senators: CIA Has Secret Program That Collects American Data
* Vulnerabilities Found by Google Researchers in 2021 Got Patched on Average in 52 Days
* Alphabet's CapitalG Makes Big Bet on Salt Security
* Apple Says WebKit Zero-Day Hitting iOS, macOS Devices
* Ransomware Recovery Startup Calamu Banks $16.5M Investment
* Data Protection and Privacy Firm Titaniam Raises $6 Million in Seed Funding
* 2021 Record Year for Cybersecurity M&A, Financing: Report
* Meta Sues Two Nigerians Who Lured Facebook Users to Phishing Sites
* New Vulnerabilities Can Allow Hackers to Remotely Crash Siemens PLCs
* Critical Code Execution Flaws Patched in 'PHP Everywhere' WordPress Plugin
* Ransomware Targeted 14 of 16 U.S. Critical Infrastructure Sectors in 2021
* The SASE Conversation in 2022, a Resolution for the Future
* University Project Cataloged 1,100 Ransomware Attacks on Critical Infrastructure
* Web Skimmer Injected Into Hundreds of Magento-Powered Stores
* Canonic Security Emerges From Stealth With $6 Million and SaaS App Sandbox
* Russian Law Enforcement Take Down Several Cybercrime Forums
* Hamas Cyberspies Return With New Malware After Exposure of Operations

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* FBI: Scammers Exploit Job Posting Sites with Fake Jobs to Steal Money and Personal Information
* New Cyberattack Campaign Delivers Multiple RATs via Trusted Cloud Services
* Engaging Your Remote Workforce: Go Beyond Compliance with Training
* Brand Impersonation and the Healthcare Sector
* Introducing the New 'Security Masterminds' Podcast
* Updated Ransomware Hostage Rescue Manual
* Use of Excel .XLL Add-Ins Soars Nearly 600% to Infect Systems in Phishing Attacks
* Average Ransomware Ransoms Jump 130% While Use of Data Exfiltration Grows
* The Evolution and Future of Ransomware
* Scammers Now Exploit 'Slinks' in LinkedIn

ISC2.org Blog

* WANT TO SPEAK AT (ISC)² SECURITY CONGRESS 2022? THE CALL FOR SPEAKERS IS NOW OPEN
* Elevating the Risk Discussion - Quantitative Analytics
* Legislation Watch: 2021 State Cybersecurity Roundup and States to Watch in 2022
* Lasting Impact of the Pandemic - Lessons from the 2021 (ISC)² Workforce Study
* Online CISSP Exam Coming Soon

HackRead

* ModifiedElephant APT hackers plant incriminating evidence on victims devices
* Twitter down - You are not alone Twitter is down for many
* NetWalker ransomware gang member sentenced to 7 years in prison
* Over 500 Magento sites hacked in payment skimmer attack
* Ways to Keep Your Business Data Secure From Cyber Attacks
* Google Drive accounted for 50% of malicious Office document downloads
* What is an SFP transceiver? Tips on choosing the right SFP transceivers

Koddos

* ModifiedElephant APT hackers plant incriminating evidence on victims devices
* Twitter down - You are not alone Twitter is down for many
* NetWalker ransomware gang member sentenced to 7 years in prison
* Over 500 Magento sites hacked in payment skimmer attack
* Ways to Keep Your Business Data Secure From Cyber Attacks
* Google Drive accounted for 50% of malicious Office document downloads
* What is an SFP transceiver? Tips on choosing the right SFP transceivers

Naked Security

* Apple zero-day drama for Macs, iPhones and iPads - patch now!
* S3 Ep69: WordPress woes, Wormhole holes, and a Microsoft change of heart [Podcast + Transcript]
* Self-styled "Crocodile of Wall Street" arrested with husband over Bitcoin megaheist
* At last! Office macros from the internet to be blocked by default
* Microsoft blocks web installation of its own App Installer files
* Wormhole cryptotrading company turns over $340,000,000 to criminals
* S3 Ep68: Bugs, scams, privacy …and fonts?! [Podcast + Transcript]
* Elementor WordPress plugin has a gaping security hole - update now
* Linux kernel patches "performance can be harmful" bug in video driver
* Website operator fined for using Google Fonts "the cloudy way"

Threat Post

* Critical MQTT-Related Bugs Open Industrial Networks to RCE Via Moxa
* Cybercrooks Frame Targets by Planting Fabricated Digital Evidence
* Apple Patches Actively Exploited WebKit Zero Day
* Decryptor Keys Published for Maze, Egregor, Sekhmet Ransomwares
* Sharp SIM-Swapping Spike Causes $68M in Losses
* SAP Patches Severe 'ICMAD' Bugs
* PHP Everywhere Bugs Put 30K+ WordPress Sites at Risk of RCE
* Cybercriminals Swarm Windows Utility Regsvr32 to Spread Malware
* 3 Tips for Facing the Harsh Truths of Cybersecurity in 2022, Part I
* MoleRats APT Flaunts New Trojan in Latest Cyberespionage Campaign

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 ends support for older Visual Studio versions
* Ballerina revamps RESTful services support
* Edge computing vs. cloud computing? Nope!
* What is OLAP? Analytical databases
* CNCF survey: Managed Kubernetes becomes the norm
* WhiteSource report warns of NPM registry risks
* How to work with IAsyncDisposable in .NET 6
* 8 new JavaScript features you might have missed
* Starburst update aims to help develop data products from any source
* One significant cost of multicloud

C4ISRNET - Media for the Intelligence Age Military

* Is Project Blackjack still relevant?
* Air Force Research Lab building momentum on cislunar projects
* Iraq seeks French drones and jets, additional Russian tanks
* America needs a robust, resilient supply chain for semiconductors
* Israel unveils artificial intelligence strategy for armed forces
* Defense Innovation Unit partners with Orbital Insight to take on satellite spoofing
* Pentagon's AI center awards contracts to 79 companies in new test and evaluation agreement
* New space modeling and sim environment to boost cooperation between scientists and force designers
* US Army improving how it tests its tactical network
* Federal and military users can now track potential terrorist activities with an app

The Hacker Corner

Conferences

* 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
* Marketing To Cybersecurity Companies

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.

* VU CYBERTHON 2022
* MHSCTF 2022
* LyonCTF
* CInsects CTF 2022
* T3N4CI0US CTF 2022
* SUSCTF 2022
* TSJ CTF 2022
* Codegate CTF 2022 Preliminary
* Ugra CTF Quals 2022
* D^3CTF 2022

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

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

Tools & Techniques

Packet Storm Security Tools Links

* Wireshark Analyzer 3.6.2
* nfstream 6.4.2
* nfstream 6.4.1
* GNU Privacy Guard 2.2.34
* TOR Virtual Network Tunneling Tool 0.4.6.10
* Scanmycode Community Edition
* Hydra Network Logon Cracker 9.3
* Falco 0.31.0
* OpenStego Free Steganography Solution 0.8.3
* Zeek 4.2.0

Kali Linux Tutorials

* CloudSpec : An Open Source Tool For Validating Your Resources In Your Cloud Providers Using A Logical
* ADenum : A Pentesting Tool That Allows To Find Misconfiguration Through The The Protocol LDAP And Exp
* Tarian : Antivirus for Kubernetes
* DInjector : Collection Of Shellcode Injection Techniques Packed In A D/Invoke Weaponized DLL
* AFLTriage : Tool To Triage Crashing Input Files Using A Debugger
* O365Spray : Username Enumeration And Password Spraying Tool Aimed At Microsoft O365
* SMBeagle : Fileshare Auditing Tool That Hunts Out All Files It Can See In The Network And Reports If
* Fileless-Xec : Stealth Dropper Executing Remote Binaries Without Dropping Them On Disk
* Kali Intelligence Suite : Shall Aid In The Fast, Autonomous, Central, And Comprehensive Collection Of
* Swurg : Parse OpenAPI Documents Into Burp Suite For Automating OpenAPI-based APIs Security Assessment

GBHackers Analysis

* ACTINIUM Hackers Group Targeting Government, Military, NGO to Steal Sensitive Data
* ESET Antivirus Flaw Let Attackers to Escalate Privileges & Execute Arbitrary Code
* How To Protect Your Business From Hackers
* OpenSubtitles Hacked - Over 7 million Subscribers Email, IP Addresses & Usernames Leaked
* Critical Flaw With Zoho Desktop Central Let Attackers to Bypass Authentication

Weekly Cyber Security Video and Podcasts

SANS DFIR

* 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
* SANS Threat Analysis Rundown

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelgänger Your Häx Dollars at Work
* DEF CON 29 Red Team Village - CTF Day 2
* DEF CON 29 Recon Village - Ben S - Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

Hak5

* How Hackers Use PwnKit to Get Root Access in Seconds | HakByte
* HUGE Crypto Theft Happens Again; UEFI Has Vulnerabilities - ThreatWire
* Brute-Forcing Vulnerable WebApps With Python | HakByte

The PC Security Channel [TPSC]

* Malwarebytes 2022: Test vs Malware
* How YouTubers get Hacked: Redline Stealer

Eli the Computer Guy

* Bird TV Introduces Its Antagonist… cancel YouTube, subscribe to life…
* Are You Actually Doing What You Were Hired For (Biden's Horrible Poll Numbers)
* Is Psychological Inertia Damaging Your Life
* YouTube is Bad for Your Health

Security Now

* The Inept Panda - China Olympics, SAMBA CVS 9.9 Vulnerability, Microsoft Office 3rd Party Macros
* The "Topics” API - PwnKit Tech Details, DrawnApart, Zerodium Bug Bounties, Log4Shell Hits Ubiquiti

Troy Hunt

* Weekly Update 282

Intel Techniques: The Privacy, Security, & OSINT Show

* 250-Consequences of Product Refunds
* 249-Requests, Freezes, & Removals

Proof of Concept (PoC) & Exploits

Packet Storm Security

CXSecurity

* Grandstream GXV31XX settimezone Unauthenticated Command Execution
* Strapi CMS 3.0.0-beta.17.4 Privilege Escalation
* QEMU Monitor HMP migrate Command Execution
* Wing FTP Server 4.3.8 Remote Code Execution
* WBCE CMS 1.5.2 Remote Code Execution
* Moxa TN-5900 Firmware Upgrade Checksum Validation
* Fetch Softworks Fetch FTP Client 5.8 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

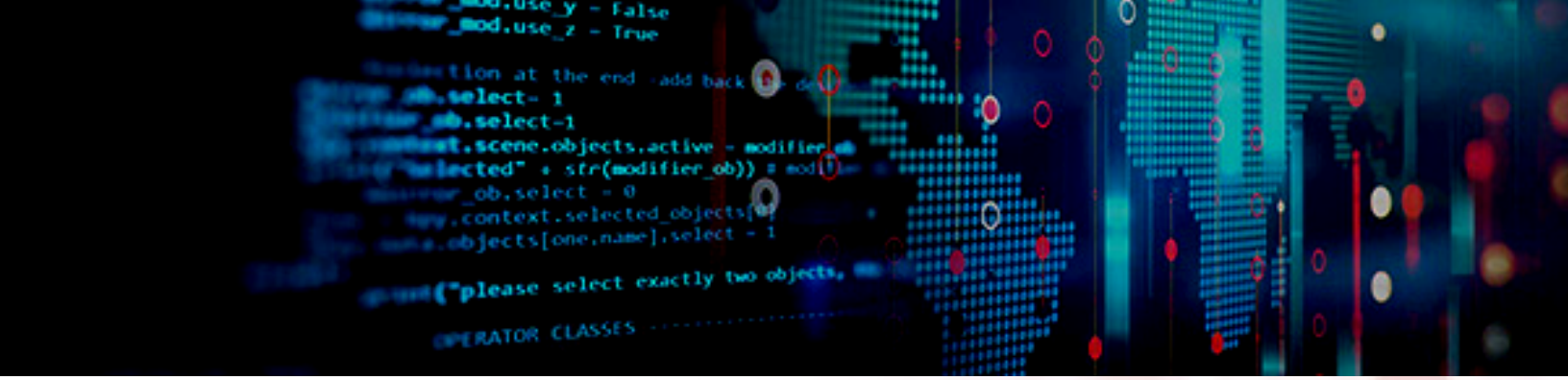
* [webapps] Kyocera Command Center RX ECOSYS M2035dn - Directory Traversal File Disclosure (Unauthentic
* [webapps] Subrion CMS 4.2.1 - Cross Site Request Forgery (CSRF) (Add Amin)
* [webapps] Accounting Journal Management System 1.0 - 'id' SQLi (Authenticated)
* [webapps] WordPress Plugin Jetpack 9.1 - Cross Site Scripting (XSS)
* [webapps] WordPress Plugin Contact Form Builder 1.6.1 - Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Secure Copy Content Protection and Content Locking 2.8.1 - SQL-Injection (
* [webapps] Home Owners Collection Management System 1.0 - 'id' Blind SQL Injection
* [webapps] Home Owners Collection Management System 1.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Home Owners Collection Management System 1.0 - Account Takeover (Unauthenticated)
* [webapps] Hospital Management Startup 1.0 - 'Multiple' SQLi
* [local] Cain & Abel 4.9.56 - Unquoted Service Path
* [webapps] AtomCMS v2.0 - SQLi
* [webapps] Exam Reviewer Management System 1.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Exam Reviewer Management System 1.0 - 'id' SQL Injection
* [webapps] WordPress Plugin CP Blocks 1.0.14 - Stored Cross Site Scripting (XSS)
* [webapps] WordPress Plugin Security Audit 1.0.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin Simple Job Board 2.9.3 - Local File Inclusion
* [remote] Wing FTP Server 4.3.8 - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin International Sms For Contact Form 7 Integration V1.2 - Cross Site Scripti
* [webapps] Hospital Management System 4.0 - 'multiple' SQL Injection
* [webapps] FileBrowser 2.17.2 - Cross Site Request Forgery (CSRF) to Remote Code Execution (RCE)
* [webapps] Strapi CMS 3.0.0-beta.17.4 - Set Password (Unauthenticated) (Metasploit)
* [webapps] Hotel Reservation System 1.0 - SQLi (Unauthenticated)
* [webapps] Servisnet Tessa - Add sysAdmin User (Unauthenticated) (Metasploit)
* [webapps] Servisnet Tessa - MQTT Credentials Dump (Unauthenticated) (Metasploit)

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*

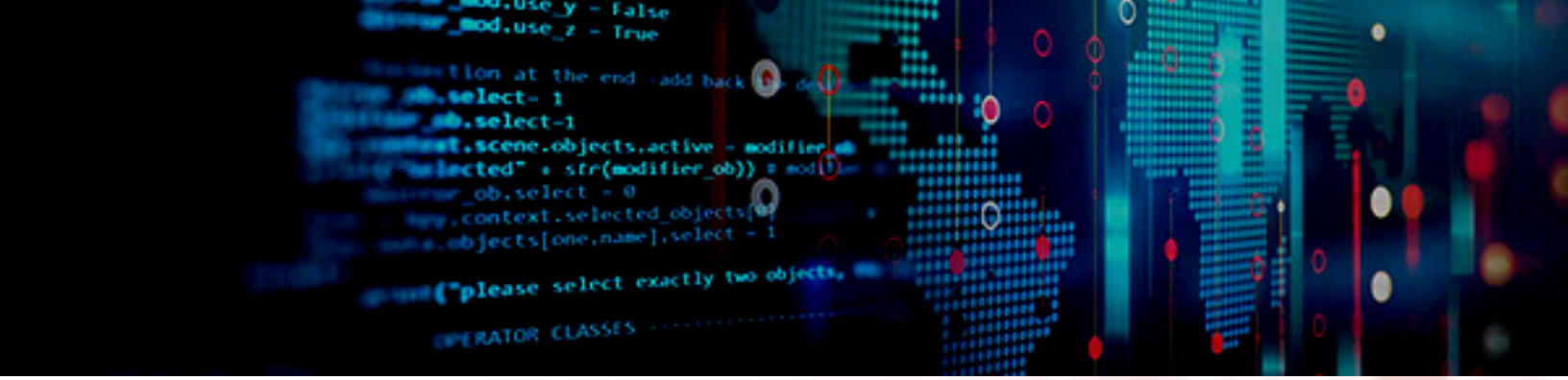
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://phapae.go.th
https://phapae.go.th notified by 0x1998
http://lged-ugiip3.gov.bd/txt.htm
http://lged-ugiip3.gov.bd/txt.htm notified by lamer
http://www.camaraitu.sp.gov.br
http://www.camaraitu.sp.gov.br notified by Paraná Cyber Mafia
https://pa-boyolali.go.id
https://pa-boyolali.go.id notified by MrNyx
https://king9.nrct.go.th/0x48.htm
https://king9.nrct.go.th/0x48.htm notified by lamer
https://guam.gov/gero.html
https://guam.gov/gero.html notified by M15T4k3
http://www.centenario.gov.ar/noname.html
http://www.centenario.gov.ar/noname.html notified by K4TSUY4-GH05T
http://www.centenario.gob.ar/noname.html
http://www.centenario.gob.ar/noname.html notified by K4TSUY4-GH05T
https://www.ugelhuaraz.gob.pe/19.html
https://www.ugelhuaraz.gob.pe/19.html notified by Mr.Rm19
http://punjabinfotech.gov.in/0day.html
http://punjabinfotech.gov.in/0day.html notified by Ren4SploIT
http://pictc.gov.in/0day.html
http://pictc.gov.in/0day.html notified by Ren4SploIT
http://bptpbogor.litbang.dephut.go.id
http://bptpbogor.litbang.dephut.go.id notified by J0keroo
http://saaevilhena.ro.gov.br/o.htm
http://saaevilhena.ro.gov.br/o.htm notified by chinafans
http://comderp.sp.gov.br/o.htm
http://comderp.sp.gov.br/o.htm notified by chinafans
http://fusbemo.sp.gov.br/o.htm
http://fusbemo.sp.gov.br/o.htm notified by chinafans
http://palenque.gob.mx/noname.html
http://palenque.gob.mx/noname.html notified by K4TSUY4-GH05T
http://ipmv.ro.gov.br/o.htm
http://ipmv.ro.gov.br/o.htm notified by chinafans



Dark Web News

Darknet Live

Two Arrested for Conspiring to Launder 119,754 Stolen Bitcoins

Law enforcement arrested two people for conspiring to launder stolen Bitcoin worth approximately $4.5 billion. The Bitcoin had originally been stolen in the 2016 Bitfinex hack. Police arrested Ilya Lichtenstein and Heather Morgan for allegedly laundering stolen cryptocurrency. According to court documents, the duo laundered the Bitcoin a hacker had stolen after hacking the Bitfinex cryptocurrency exchange in 2016. The hack resulted in the theft of 119,754 Bitcoins which ended up in a Bitcoin wallet controlled by Lichtenstein. Since the hack, Lichtenstein and Morgan allegedly laundered approximately 25,000 of those stolen Bitcoins through a "complicated money laundering process.” The duo reportedly transferred the laundered Bitcoins into "financial accounts” they controlled. VCE = virtual currency exchange The original wallet still contained more than 94,000 Bitcoins. After executing search warrants on unspecified "online accounts” owned by Lichtenstein, investigators seized the remaining Bitcoin. According to court documents, the feds obtained a warrant for an account linked to Lichtenstein's email address. They managed to decrypt encrypted files stored in the account. The encrypted files contained a list of Bitcoin public addresses and the corresponding private keys. I would like to know how investigators decrypted the files referenced in the complaint. The criminal complaint alleges that Lichtenstein and Morgan employed numerous sophisticated laundering techniques, including using fictitious identities to set up online accounts; utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period; depositing the stolen funds into accounts at a variety of virtual currency exchanges and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; converting bitcoin to other forms of virtual currency, including anonymity-enhanced virtual currency (AEC), in practice known as "chain hopping”; and using U.S.-based business accounts to legitimize their banking activity. The duo apparently laundered the stolen funds through Alphabay. The darknet market referenced in the Department of Justice announcement is Alphabay. As a part of the conspiracy, Lichtenstein and Morgan allegedly sent the stolen Bitcoin to Alphabay and then withdrew Bitcoin to unhosted addresses. Feds recovered Bitcoin worth more than $3.6 billion-the largest cryptocurrency seizure to date, according to Chief Jim Lee of IRS-Criminal Investigation (IRS-CI). Investigators traced the stolen Bitcoin to at least five other cryptocurrency exchanges. Both defendants face charges of conspiracy to commit money laundering and conspiracy to defraud the United States. The statement of facts contains a lot of interesting information about the alleged laundering conspiracy. I have included the statement of facts and the criminal complaint in both pdf and html formats. statement of facts: pdf, html criminal complaint: pdf, html DoJ Announcement: archive.is, archive.org, .onion Morgan was involved in cybecrime while in the United States… as a Russian national (why move from Russia to the US, lol?). And then remained in the United States even after the Bitfinex theft. All of this of course is in addition to the obvious mistakes outlined in the statement of facts. There are no shortage of those; it seems as if the laundering scheme was basically Bitcoin "tumbling” with more steps. A failure but better than the reverse laundering seen in this case. Although she is a rapper,

she is no Nicki Minaj, according to a source. (via darknetlive.com at https://darknetlive.com/post/two-arrested-for-conspiring-to-launder-4-billion-in-stolen-bitcoin/)

Hungarian Man Bought Two Kilos of Amphetamine Online

The Veszprém County Attorney General's Office filed an indictment against a 27-year-old man accused of purchasing large quantities of drugs on the dark web for resale. In a press release, the Veszprém County Attorney General's Office disclosed that the 27-year-old defendant had ordered a kilogram of amphetamine from an undisclosed darkweb marketplace on two occasions, once in November 2020 and again in March 2021. Investigators intercepted a kilogram of amphetamine addressed to the defendant's address in March 2021. They then executed a search warrant on the defendant's residence on March 16, 2021. Investigators found that the defendant had divided the amphetamine into small packages and stored it in his freezer. During questioning, the defendant admitted ordering a kilogram of amphetamine from an undisclosed darkweb marketplace on March 5, 2021. He paid approximately $870 in Bitcoin for the amphetamine. Investigators also established that the defendant had purchased a similar amount of amphetamine from the darkweb in November 2020. The prosecution asked the Veszprém Tribunal to sentence the 27-year-old to prison and bar him from working in public affairs. The prosecution also asked the court to order the man to pay a fine of approximately $1,900. archive.is, onion (via darknetlive.com at https://darknetlive.com/post/hungarian-man-bought-two-kilos-of-amphetamine-online/)

Second Chemical Revolution Trial Rescheduled Again

Officials in Germany rescheduled the second Chemical Revolution trial again. I do not see why the defendants are unable to reschedule the hearing indefinitely for the same reason. In 2019, German law enforcement shut down Chemical Revolution, the largest darkweb drug shop for Germans. Police arrested 11 suspects as a part of the investigation. The second trial has been postponed for the second time. The second trial, which began on January 10, 2022, involves five defendants. Some defendants are back in front of the court, but this will be their first appearance for others. We will apparently never know the outcome of the trial, though. The BKA circulated dozens pictures of the drugs seized during the investigation. Last year, during the first trial, the co-creator of the shop essentially admitted everything about the drug trafficking operation. The court heard how the defendants had earned at least one million euros in cryptocurrency by selling kilograms of amphetamine, marijuana, cocaine, and ecstasy through the darkweb storefront. After the first trial, the court sentenced seven defendants to terms ranging from two years in prison to nine years in prison. The co-creator received the longest prison sentence. A spokesperson for the district court in Giessen announced that the district court had postponed the second Chemical Revolution trial again. After finally starting on January 10, the court postponed it for some coronavirus reason on January 31, 2022. At the time, the court had scheduled the hearing for February 7, 2022. A court spokesperson revealed that the district court rescheduled the hearing for a second time due to coronavirus. The spokesperson did not provide a date for the rescheduled trial. Hopefully time served is considered during sentencing. (via darknetlive.com at https://darknetlive.com/post/second-chemical-revolution-trial-rescheduled-again/)

Mississippi Woman Admits Paying a "Hitman" to Kill Her Husband

A Mississippi woman admitted attempting to hire a hitman on the darkweb to murder her husband. She used her work computer to find and pay the hitman. Jessica Leeann Sledge, 40, of Pelahatchie, Mississippi, pleaded guilty to one count of using interstate commerce facilities in the commission of murder-for-hire. The case is a typical murder-for-hire case, except for Sledge's interaction with undercover law enforcement officers. In a criminal complaint filed in November 2021, Federal Bureau of Investigation (FBI) Special Agent Justin Schmidt wrote that a source provided law enforcement with information about a murder-for-hire plot involving Sledge's husband. It appears that a source-likely the same source referenced in most of these cases-provided the FBI in Knoxville with copies of chat logs from a murder-for-hire site on the darkweb. The records contained messages between Sledge and the administrator of the murder-for-hire site and proof that Sledge had sent the "hitman” $10,000 in Bitcoin to murder a target. Sledge appears to be standing in front of a piece of cardboard in her mugshot? | WLBT An undercover law enforcement officer, posing as the hitman, called Sledge and asked to speak with "Forward Only,” the username Sledge had

used on the murder-for-hire site. Sledge confirmed that she was "Forward Only.” She also directed the undercover officer to contact her through her WhatsApp account under the same username. During a series of recorded conversations over the phone and through WhatsApp, Sledge confirmed that she had paid $10,000 in Bitcoin to have her husband killed. She sent the undercover officer pictures of the target, pictures of his car, and updates on her husband's whereabouts. On November 1, 2021, Sledge agreed to meet the purported hitman in person in a Home Depot parking lot. During the meeting, Sledge paid the undercover officer an additional $1,000 in cash to complete the job and said she might hire him for another job. The victim of the next hit would be "a female who couldn't keep her mind on her own business,” according to Special Agent Schmidt. Later that day, law enforcement officers arrested Sledge at her place of employment. They asked Sledge if she knew anyone who wanted to hurt her husband. After some back and forth, the officers told Sledge that her husband was dead and placed her under arrest. (Obviously her husband was not dead at the time. And I assume he is still living.) "She kind of told me about Tor. I asked Ms. Sledge about it in the interview. She explained it to me as a web browser… she downloaded to her work computer,” Special Agent Schmidt said. "She didn't recall how she searched for a hitman.” Investigators received permission from Sledge's employer to access her work computer. Sledge gave the investigators her password. Later, an analyst "noticed things were deleted off the computer days after she was arrested.” They eventually learned that a person identified as Ollie Cliburn had remotely accessed Sledge's computer after her arrest in an attempt to delete incriminating content. Sledge, according to WLBT, had an affair with Cliburn. Cliburn had also told Sledge to delete the Tor Browser off her work computer. She will be sentenced on May 16, 2022. She faces up to ten years in prison. Complaint (pdf) Indictment (pdf) (via darknetlive.com at https://darknetlive.com/post/mississippi-woman-paid-a-hitman-10k-in-btc-to-kill-her-husband/)

Dark Web Link

White House Market Plans Retirement: What Important Things You Missed?

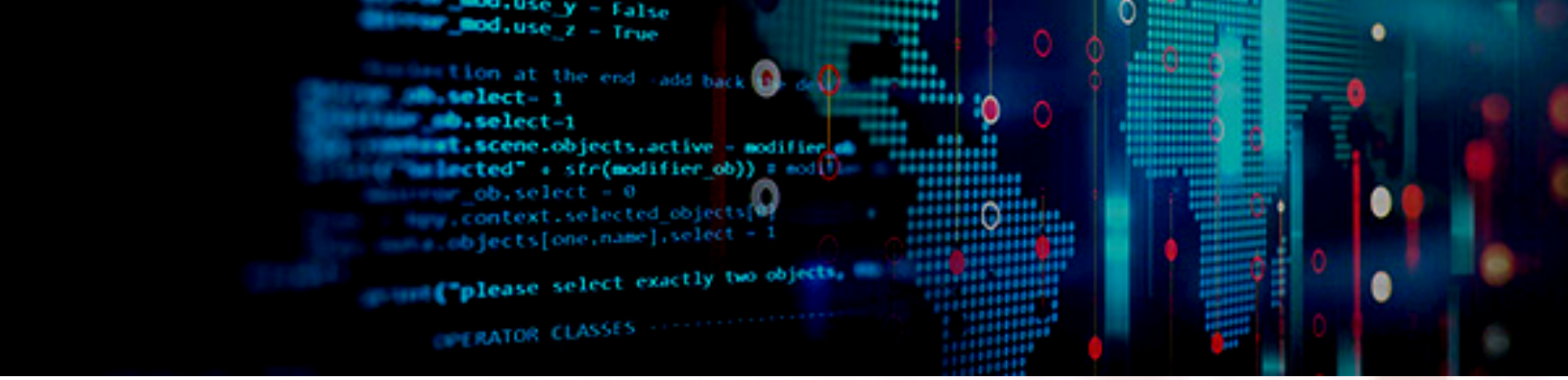
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere 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

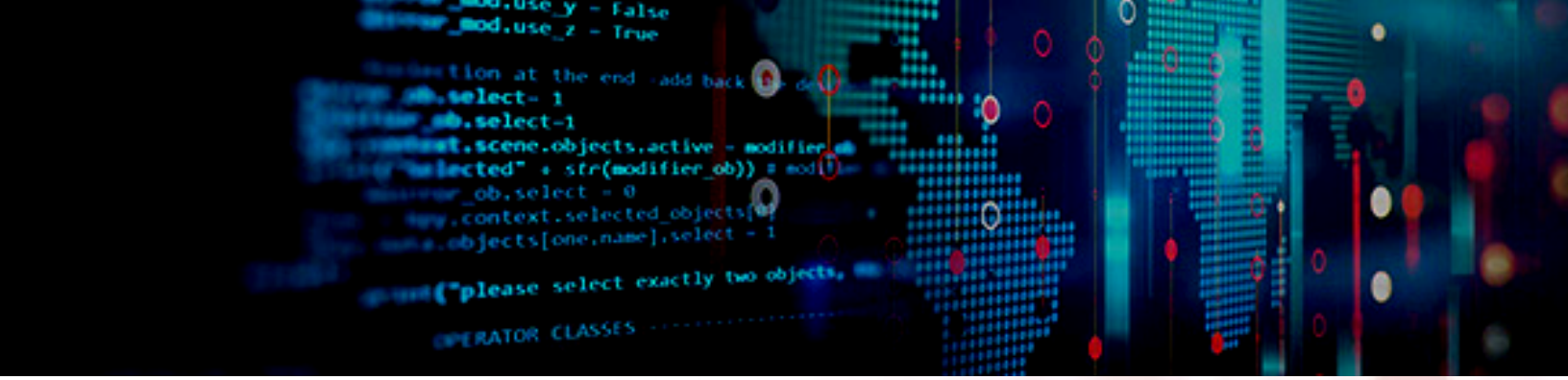
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence 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
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management

FireEye

* Metasploit Wrap-Up
* The Forecast Is Flipped: How Rapid7 Is Flipping L&D for the Future of Work
* Evolving How We Share Rapid7 Research Data
* Patch Tuesday - February 2022
* The Big Target on Cyber Insurers' Backs
* Why Security in Kubernetes Isn't the Same as in Linux: Part 2
* Metasploit Wrap-Up
* 7Rapid Questions With Our APAC Sales Manager, Soumi
* Velociraptor Version 0.6.3: Dig Deeper With More Speed and Scalability
* [Security Nation] John Rouffas on Building a Security Function



Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* Apple Releases Security Updates for Multiple Products
* CISA Adds 15 Known Exploited Vulnerabilities to Catalog
* 2021 Trends Show Increased Globalized Threat of Ransomware
* Adobe Releases Security Updates for Multiple Products
* Citrix Releases Security Updates for Hypervisor
* Microsoft Releases February 2022 Security Updates
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* AA22-040A: 2021 Trends Show Increased Globalized Threat of Ransomware
* AA22-011A: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infras
* Vulnerability Summary for the Week of January 31, 2022
* Vulnerability Summary for the Week of January 24, 2022

Zero Day Initiative Advisories

ZDI-CAN-16337: Dell
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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-10, 4 days ago. The vendor is given until 2022-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16410: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16385: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16053: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16375: 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 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16533: 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: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16534: 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: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16446: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16404: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16373: 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 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16189: Microsoft

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'ZhangYang' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16414: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16392: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16390: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-16314: Trend Micro

A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Simon

Zuckerbraun - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-15310: Docker

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Hashim Jawad (@ihack4falafel)' was reported to the affected vendor on: 2022-02-09, 5 days ago. The vendor is given until 2022-06-09 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-15892: Cisco

A CVSS score 6.3 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N) severity vulnerability discovered by 'Q. Kaiser from IoT Inspector Research Lab' was reported to the affected vendor on: 2022-02-08, 6 days ago. The vendor is given until 2022-06-08 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-16458: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16430: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16427: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16428: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16456: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16450: 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: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 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-16453: Adobe

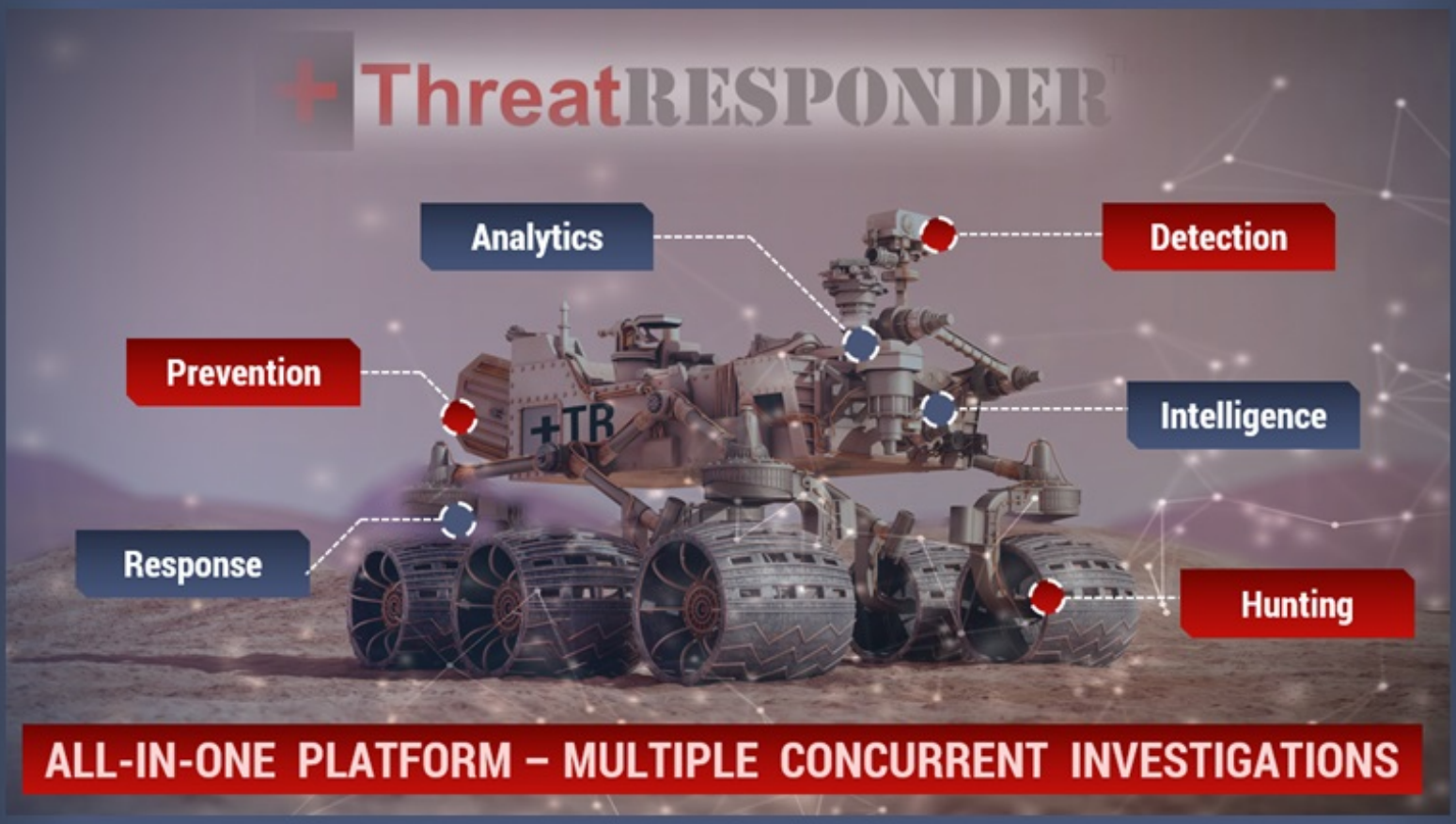
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-04, 10 days ago. The vendor is given until 2022-06-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

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



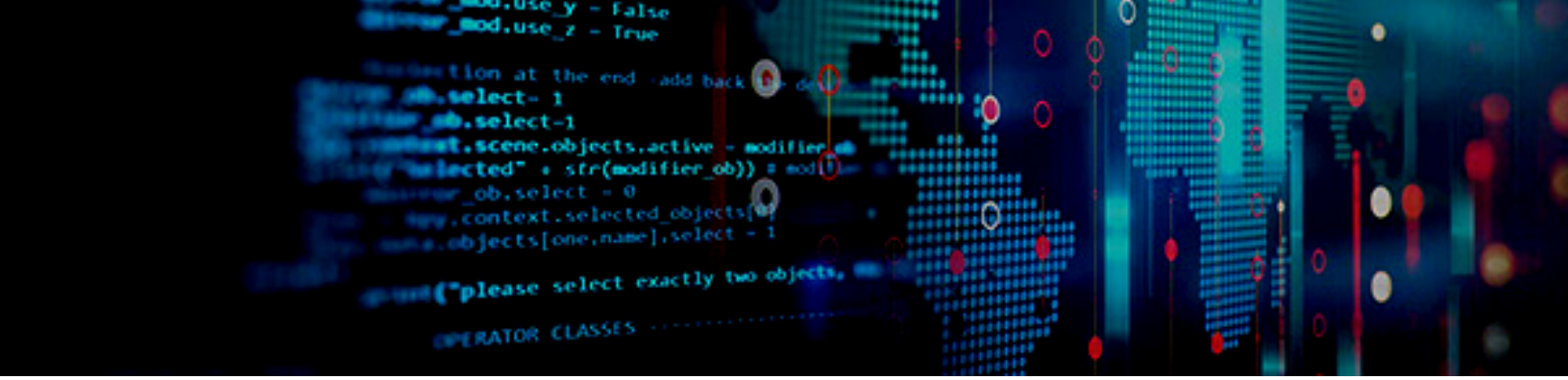
The Solution – ThreatResponder® Platform

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

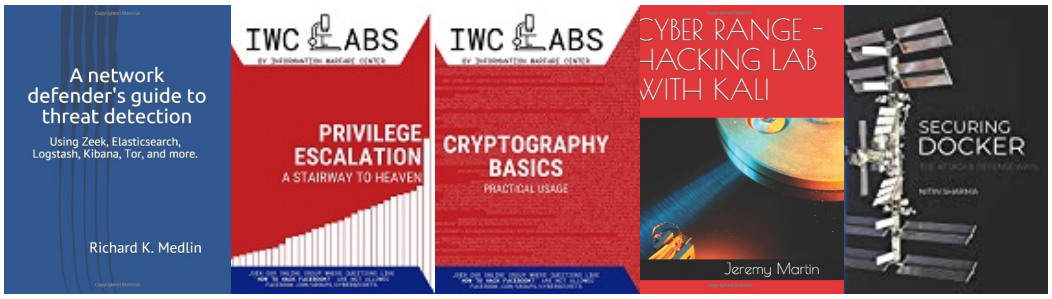


The Cyber Secrets publications on Amazon

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