Mar-21-22

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 21, 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

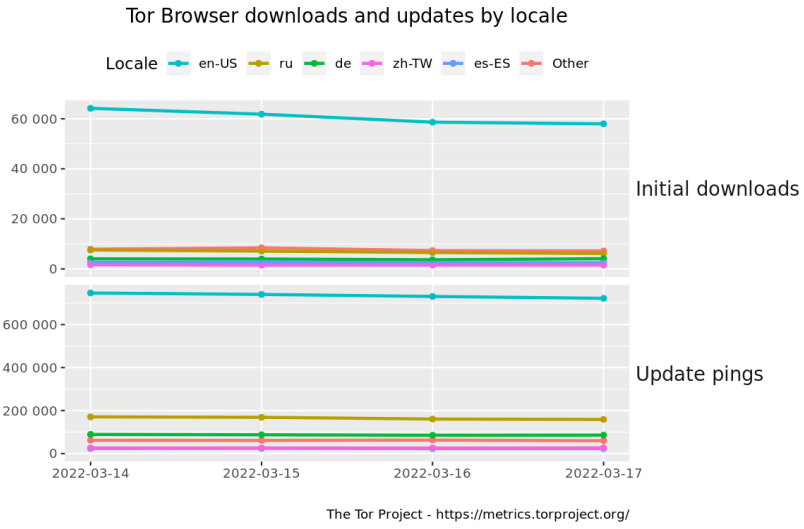
Internet Storm Center Infocon Status

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

* Attacks Are Crippling Russian Government Websites
* Why We Haven't Seen Debilitating Cyberwar In Ukraine
* SAP Community Website Leaks Member Data To Savvy Users
* Google Blows Lid Off Conti, Diavol Ransomware Ops
* Agencies Aware Of Hacking Threats To US, Allied Satellite Networks
* Be Ready To Lose All Your Money In Crypto, EU Regulators Warn
* Hackers Provide Livestream Of Dozens Of Cameras Inside Russia
* Misconfigured Firebase Databases Exposing Data In Mobile Apps
* CafePress Fined For Covering Up 2019 Customer Info Leak
* Russian Cyclops Blink Botnet Launches Assault Against Asus Routers
* Most QNAP NAS Devices Affected By Dirty Pipe Linux Flaw
* OpenSSL Patches Crash-Me Bug Triggered By Rogue Certs
* The 300,000 Volunteer Hackers Coming Together To Fight Russia
* RSA Sells Conference To Become Standalone Business
* Fraudsters Use Intelligent Bots To Attack Financial Institutions
* Germany Warns Against Russian Anti-Virus Use
* Phony Instagram Support Staff Emails Hit Insurance Company
* Russia-Linked Attackers Breach NGO By Exploiting MFA, PrintNightmare Vuln
* Researcher Uses Dirty Pipe Exploits To Fully Root A Pixel 6 Pro And Samsung S22
* Researcher Uses 379-Year-Old Algorithm To Crack Crypto Keys
* Banks On Alert For Russian Reprisal Cyberattacks On Swift
* Another Data Leaking Spectre Bug Found, Smashes Intel, Arm Defenses
* CaddyWiper: More Destructive Wiper Malware Strikes Ukraine
* Russia's Disinformation Machinery Breaks Down In Wake Of Ukraine Invasion
* Ukraine Reportedly Adopts Clearview AI To Track Russian Invaders

Krebs on Security

* Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware
* Lawmakers Probe Early Release of Top RU Cybercrook
* 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

Dark Reading

* Half of Orgs Use Web Application Firewalls to Paper Over Flaws
* Code-Sabotage Incident in Protest of Ukraine War Exposed Open Source Risks
* CyCognito Launches Exploit Intelligence
* A Chance to Raise Shields Right
* Menlo Security: Less Than Three in 10 Organizations Are Equipped to Combat Growing Wave of Web-Based
* Security Teams Struggle to Get Started With Zero Trust
* Satellite Networks Worldwide at Risk of Possible Cyberattacks, FBI & CISA Warn
* The Road Ahead for Cyber and Infrastructure Security
* 6 Reasons Not to Pay Ransomware Attackers
* ThreatMapper Updated With New Scanning Tools
* Firefly Announces Release of ValidIaC Open Source Solution
* Nok Nok Labs Unveils S3 Authentication Suite
* Multiple Automotive Manufacturers Infected With Emotet
* Cloudflare Announces API Gateway
* Titaniam Announces Completion of Product Suite
* Glasswall Launches Freemium Version of its Desktop Content Disarm and Reconstruction App
* Stopping Russian Cyberattacks at Their Source
* Cut Down on Alert Overload and Leverage Layered Security Measures
* Enhancing DLP With Natural Language Understanding for Better Email Security
* How Pen Testing Gains Critical Security Buy-in and Defense Insight

The Hacker News

Security Week

* Most Hood Plants Up After Cyber 'Event,' Schools Concerned
* High-Severity Vulnerabilities Patched in BIND Server
* US Critical Infrastructure Targeted by AvosLocker Ransomware
* Google Analyzes Activity of 'Exotic Lily' Initial Access Broker
* TransUnion Confirms Data Breach at South Africa Business
* Gh0stCringe RAT Targeting Database Servers in Recent Attacks
* SATCOM Cybersecurity Alert Issued as Authorities Probe Possible Russian Attack
* Todyl Banks $28M Series A Investment
* Microsoft Releases Open Source Tool for Securing MikroTik Routers
* Software Supply Chain Weakness: Snyk Warns of 'Deliberate Sabotage' of NPM Ecosystem
* SolarWinds Warns of Attacks Targeting Web Help Desk Users
* Most NASA Systems at Risk From Insider Threats: Audit
* NIST Releases ICS Cybersecurity Guidance for Manufacturers
* Public and Private Sector Security: Better Protection by Collaboration
* 'LokiLocker' Ransomware Packs Data Wiping Capabilities
* Cyber Security Takeover May Harm Competition: UK Regulator
* Hackuity Emerges From Stealth With $13 Million in Funding
* Google Patches Critical Vulnerability With Chrome 99 Update
* CISA Adds 14 Windows Vulnerabilities to 'Must-Patch' List
* Cloudflare Announces New Security Tools for Email, Applications, APIs
* Severe Vulnerability Patched in CRI-O Container Engine for Kubernetes
* US Warns About Russian Attacks Exploiting MFA Protocols, PrintNightmare Flaw
* Senators Ask DHS About Efforts to Protect US Against Russian Cyberattacks
* Cybersecurity M&A Roundup for March 1-15, 2022
* Germany Warns Against Russia's Kaspersky Anti-Virus Software

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [Heads Up] New Evil Ransomware Feature: Disk Wiper if You Don't Pay
* KnowBe4 Named a Leader in The Forrester Wave for Security Awareness and Training Solutions
* Ransomware-Related Data Leaks Increase 82% as the Number of Cybercriminal Groups Nearly Triples
* Backups Become the Focus as Three-Fourths of Organizations Experienced Ransomware Attacks
* New Phishing Method Uses VNC to Bypass MFA Measures and Gives Cybercriminals Needed Access
* [Eye Opener] Ukraine Is Now Being Hit With 4 Different Strains Of Wiper Malware
* We Are In The First Open Source Intelligence War
* CyberheistNews Vol 12 #11 [Heads Up] FBI: Ransomware Gang Breached 52 U.S. Critical Infrastructure Or
* Shipping Fraud Rises Nearly 800% in 2021
* Cybercrime-as-a-Service: Its Evolution and What You Can Do to Fight Back

ISC2.org Blog

* Meet the Young Women Tackling Gender Bias in Cybersecurity
* How is the CISSP-ISSMP Exam Changing?
* What Can Flexible Work Conditions Do for Cyber?
* Changes to the CISSP Exam Length Coming Soon
* KnowBe4 Spreads Cyber Awareness Training to Their Community

HackRead

* Anonymous Leaks 79GB of Russian Oil Pipeline Giant's Email Data
* Targeting Satellite? CISA, FBI Warns of Attacks on SATCOM Network Providers
* Ukranian News Channel Hacked to Run Deepfake video of President Zelensky
* Ukrainian Secret Service Arrested Hacker Helping Russian Troops
* Simple Tips to Protect Youself From Being Catfished
* 16 Ways to Stay Safe While Online Shopping
* German Authorities Warn Against Using Kaspersky Products

Koddos

* Anonymous Leaks 79GB of Russian Oil Pipeline Giant's Email Data
* Targeting Satellite? CISA, FBI Warns of Attacks on SATCOM Network Providers
* Ukranian News Channel Hacked to Run Deepfake video of President Zelensky
* Ukrainian Secret Service Arrested Hacker Helping Russian Troops
* Simple Tips to Protect Youself From Being Catfished
* 16 Ways to Stay Safe While Online Shopping
* German Authorities Warn Against Using Kaspersky Products

Naked Security

* OpenSSL patches infinite-loop DoS bug in certificate verification
* S3 Ep74: Cybercrime busts, Apple patches, Pi Day, and disconnect effects [Podcast]
* Beware bogus Betas - cryptocoin scammers abuse Apple's TestFlight system
* CISA warning: "Russian actors bypassed 2FA" - what happened and how to avoid it
* Apple patches 87 security holes - from iPhones and Macs to Windows
* Happy #PiDay - even if you aren't in North America!
* Cryptocoin ATMs ruled illegal - "Shut down at once", says regulator
* 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

Threat Post

* Agencies Warn on Satellite Hacks & GPS Jamming Affecting Airplanes, Critical Infrastructure
* DarkHotel APT Targets Wynn, Macao Hotels to Rip Off Guest Data
* Sandworm APT Hunts for ASUS Routers with Cyclops Blink Botnet
* Google Blows Lid Off Conti, Diavol Ransomware Access-Broker Ops
* Dev Sabotages Popular NPM Package to Protest Russian Invasion
* Misconfigured Firebase Databases Exposing Data in Mobile Apps
* Reporting Mandates to Clear Up Feds' Hazy Look into Threat Landscape - Podcast
* 'CryptoRom' Crypto-Scam is Back via Side-Loaded Apps
* Another Destructive Wiper Targets Organizations in Ukraine
* Phony Instagram 'Support Staff' Emails Hit Insurance Company

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

* Cloud convenience and open source
* Improve agile and app dev meetings
* Microsoft emphasizes regex source generation in .NET 7
* What happened to performance engineering in the cloud?
* Deno gets faster Rust calls
* Oracle OCI compute, storage, networking tools aim to cut cloud complexity
* ServiceNow adds incident response platform to SaaS portfolio
* Microsoft .NET MAUI nears the finish line
* How to craft a cloud services catalog entry
* Vercel CEO: Deployment should be instantaneous

C4ISRNET - Media for the Intelligence Age Military

* Pentagon's JADC2 strategy focuses on 'approach'
* US government clients unaffected by Viasat cyberattack
* Boeing completes critical design review for protected satellite communications payload
* US Space Force preparing to decommission legacy command and control system
* Pentagon taps LMI, MORSE for AI data deal
* Congress wants new $200 million program to strengthen AI at combatant commands
* Space Development Agency to launch next missile warning satellites earlier than expected
* New venture capital fund focused on high-need, dual-use technology
* Blue, yellow and gray zone: The cyber factor in Ukraine
* US Space Force won't say it why it delayed an upcoming Wide-Field-of-View Testbed launch

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.

* OFPPT-CTF Morocco
* T3N4CI0US CTF 2022
* Wicked 6: 2022 Women's Global Cyber League
* Insomni'hack 2022
* LINE CTF 2022
* Space Heroes CTF
* RITSEC CTF 2022
* UMassCTF 2022
* Midnight Sun CTF 2022 Quals
* Imperial CTF 22

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

* nfstream 6.4.3
* OpenSSL Toolkit 3.0.2
* OpenSSL Toolkit 1.1.1n
* 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

Kali Linux Tutorials

* SocialPwned : An OSINT Tool That Allows To Get The Emails, From A Target, Published In Social Network
* SentryPeer : A Distributed Peer To Peer List Of Bad Actor IP Addresses And Phone Numbers Collected
* Instaloctrack : An Instagram OSINT Tool To Collect All The Geotagged Locations
* Espionage : A Network Packet And Traffic Interceptor For Linux. Spoof ARP And Wiretap A Network
* Invoke-EDRChecker : Checks Running Processes, Process Metadata, Dlls Loaded Into Your Current Process
* IDACode : An Integration For IDA And VS Code Which Connects Both To Easily Execute And Debug
* SMBSR : Lookup For Interesting Stuff In SMB Shares
* How To Track Down Your Lost Devices?
* SQLRecon : A C# MS SQL Toolkit Designed For Offensive Reconnaissance And Post-Exploitation
* Elfloader : An Architecture-Agnostic ELF File Flattener For Shellcode

GBHackers Analysis

* CISA Has Added 15 New Flaws to the List of Actively Exploited Vulnerabilities
* FBI Warns that Hackers Gain Network Access by Exploiting MFA and "PrintNightmare" Vulnerability
* QNAP Escalation Vulnerability Let Attackers Gain Administrator Privileges and Inject Malicious Code
* 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

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Keynote - Use Your Voice: Why Diversity and Inclusion Matter for Cyber Threat Intelligence
* Mind Your Gaps: Leveraging Intelligence Gaps to Drive Your Intelligence Activities
* We're in Now, Now: The Tyranny of Current Intelligence and How to Manage It
* Práctico uso de Inteligencia De Amenazas para operacionalizar Purple Teaming

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

* DDoS Attack Size Breaks Historical Records - ThreatWire
* Live Hacking Q&A with Kody and Alex
* Introducing: The OMG Adapter

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* 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
* Office Hours - Guest host Tomer Shvueli (Digital Nomad)

Security Now

* QWACs on? or QWACs off? - Patch Tuesday Recap, NVIDIA Hacked, EUFI Firmware Flaw, ProtonMail
* Rogue Nation Cyber Consequences - Russia vs. Ukraine, Crypto, StarLink, Namecheap, Telegram

Troy Hunt

* Weekly Update 287

Intel Techniques: The Privacy, Security, & OSINT Show

* 254-OSINT+Fugitives=Rewards
* 253-Dash Cams

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Chrome chrome_pdf::PDFiumEngine::RequestThumbnail Heap Buffer Overflow
* Simple Mobile Comparison Website 1.0 Cross Site Scripting
* BuilderRevengeRAT XML Injection
* BuilderTorCTPHPRAT.b Cross Site Scripting
* BuilderTorCTPHPRAT.b Shell Upload
* BuilderTorCTPHPRAT.b Insecure Credential Storage
* BuilderPandoraRat.b Insecure Credential Storage
* BuilderOrcus Insecure Credential Storage
* BuilderOrcus Insecure Permissions
* Windows SpoolFool Privilege Escalation
* Chrome HandleTable::AddDispatchersFromTransit Integer Overflow
* Moodle 3.11.5 SQL Injection
* Pluck CMS 4.7.16 Shell Upload
* Hikvision IP Camera Backdoor
* Tiny File Manager 2.4.6 Shell Upload
* Apache APISIX 2.12.1 Remote Code Execution
* Laravel Media Library Pro 2.1.6 Shell Upload
* College Website Management System 1.0 SQL Injection
* Hades RAT Web Panel Cross Site Scripting
* Hades RAT Web Panel Information Disclosure
* Hades RAT Web Panel Insecure Credential Storage
* RedLine.MainPanel Insecure Permissions
* Automatic Question Paper Generator System 1.0 Cross Site Scripting
* VIVE Runtime Service 1.0.0.4 Unquoted Service Path
* Automatic Question Paper Generator System 1.0 Insecure Direct Object Reference

CXSecurity

* Moodle 3.11.5 SQL Injection
* 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

Proof of Concept (PoC) & Exploits

Exploit Database

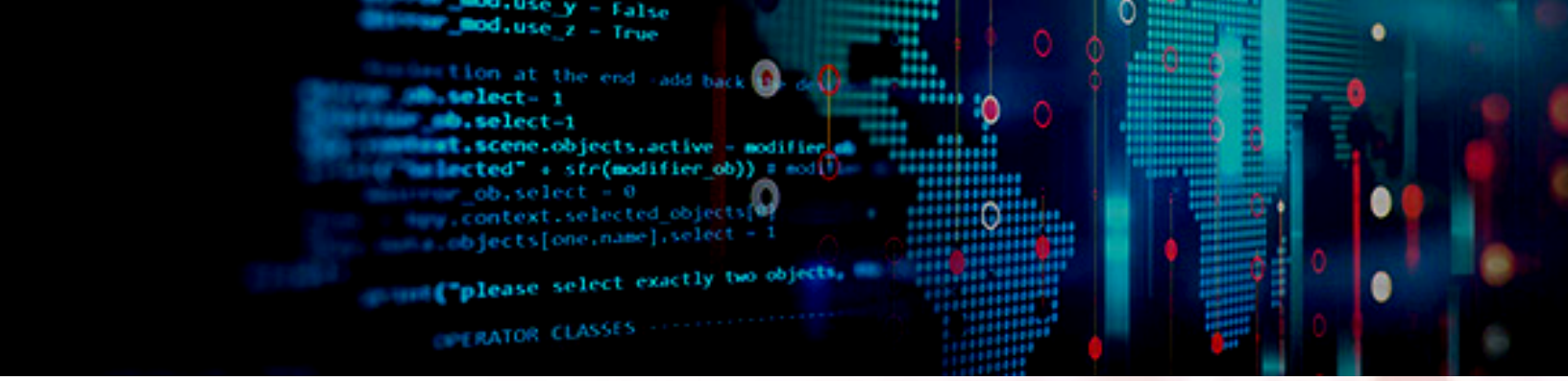
* [webapps] Wordpress Plugin iQ Block Country 1.2.13 - Arbitrary File Deletion via Zip Slip (Authentica
* [remote] Apache APISIX 2.12.1 - Remote Code Execution (RCE)
* [webapps] Tiny File Manager 2.4.6 - Remote Code Execution (RCE)
* [webapps] Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Moodle 3.11.5 - SQLi (Authenticated)
* [local] VIVE Runtime Service - 'ViveAgentService' Unquoted Service Path
* [webapps] Baixar GLPI Project 9.4.6 - SQLi
* [remote] Tdarr 2.00.15 - Command Injection
* [remote] Seowon SLR-120 Router - Remote Code Execution (Unauthenticated)
* [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

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*

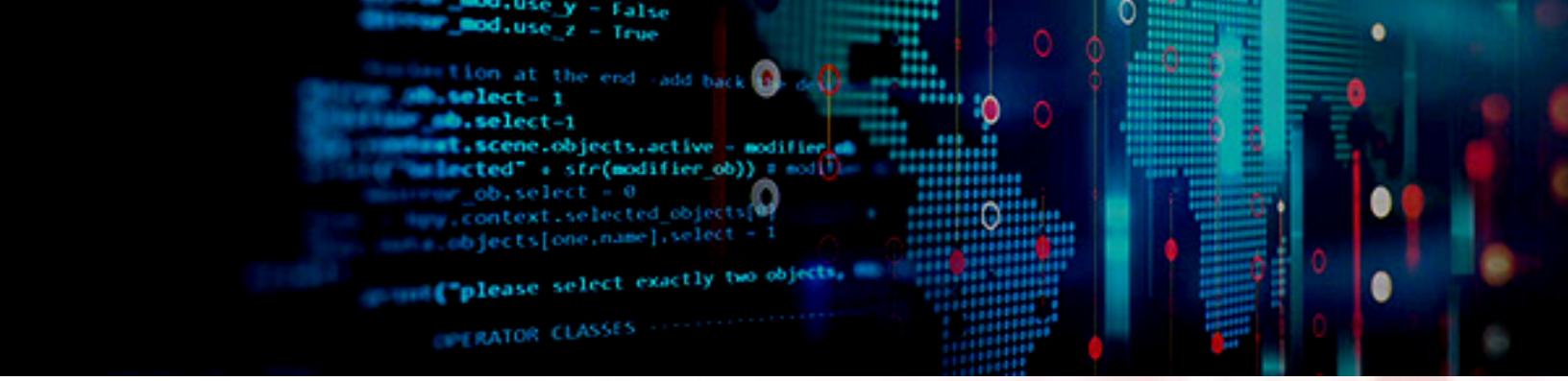
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://munisanjeronimocusco.gob.pe/CR4P5.txt
http://munisanjeronimocusco.gob.pe/CR4P5.txt notified by Mr.CR4P5
http://gahar.gov.eg/o.htm
http://gahar.gov.eg/o.htm notified by chinafans
https://pa-tarutung.go.id/fake.php
https://pa-tarutung.go.id/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
http://msc.gov.mk/0day.html
http://msc.gov.mk/0day.html notified by Ren4SploIT
http://www.dbe.gov.jo
http://www.dbe.gov.jo notified by Charles1337
http://bondcountyil.gov/cryp.html
http://bondcountyil.gov/cryp.html notified by Cryptonic HaXori
https://rsudalihsan.jabarprov.go.id
https://rsudalihsan.jabarprov.go.id notified by Mr.spongebob
https://diskominfo.jabarprov.go.id
https://diskominfo.jabarprov.go.id notified by Mr.spongebob
http://smoer.gov.lk
http://smoer.gov.lk notified by eRRoR 7rB
https://bdlh.go.th/noname.html
https://bdlh.go.th/noname.html notified by K4TSUY4-GH05T
https://humbanghasundutankab.go.id/heked.html
https://humbanghasundutankab.go.id/heked.html notified by Mr.spongebob
https://mygovuc.gov.my
https://mygovuc.gov.my notified by eRRoR 7rB
http://ogp.gouv.ci/404.php
http://ogp.gouv.ci/404.php notified by 0x1998
http://keeromkab.go.id/index.html
http://keeromkab.go.id/index.html notified by AnonyKs_xD
https://www.tanzaniatourism.go.tz/kurd.htm
https://www.tanzaniatourism.go.tz/kurd.htm notified by 0x1998
https://sanandrestuxtla.gob.mx/Ahd404.html
https://sanandrestuxtla.gob.mx/Ahd404.html notified by Ahd404
https://sugarcane.icar.gov.in/images/president.txt
https://sugarcane.icar.gov.in/images/president.txt notified by ./W4D3R



Dark Web News

Darknet Live

UK: Darkweb Drug Trafficker Sentenced to Prison

A member of a "global darkweb organized crime group” has been sentenced to nine years in prison for shipping kilograms of drugs to buyers around the globe. Mubinar Rahman, 26, mailed more than 104 packages of MDMA to global destinations as a part of an organized darkweb drug trafficking operation, according to the National Crime Agency (NCA). The defendant pleaded guilty at Newcastle Crown Court in October 2020 to trafficking drugs and possession of Class A drugs with intent to supply.

Mubinar Rahman is an "accountancy student” living in South Shields. Between June 29, 2020, and July 27, 2020, the NCA and Border Force intercepted 39 packages shipped by Rahman. Rahman had addressed the packages to buyers in the UK, United States, Israel, Norway, Thailand, Hong Kong, and elsewhere. The investigation resulted in seizures of 90 kilograms of MDMA, 134 kilograms of amphetamine, and more than 6,000 Valium and Xanax pills. In total, the value of the drugs shipped by Rahman was $1,036,025 (or 6,590,367 CNY/59,694,066 INR). The investigation involved cooperation with the United States Homeland Security Investigations (HSI). On 28 July 2020, NCA officers watched Rahman park his 2010 BMW outside a house associated with the drug trafficking operation. Officers arrested Rahman after he had returned to his car. During a search of the BMW, officers found ten packages addressed to international customers. A subsequent search of the house resulted in the discovery of 25 kilograms of MDMA, 134 kilograms of amphetamine sulfate, packaging equipment, and other materials often used by drug traffickers.

The court called Rahman the "warehouse and distribution hub manager.” Rahman refused to answer questions asked by NCA officers. However, according to the NCA, messages shared on EncroChat, the encrypted communications network hacked by law enforcement during Operation Venetic "helped officers identify other suspects involved in the darkweb drugs network.” Law enforcement arrested two additional suspects in April 2021 on suspicion of importing and supplying Class A, B, and C drugs. Investigators identified two more suspects who are allegedly on the run at the time of publication. NCA Branch Commander Martin Clarke: "Rahman was working for a well-established criminal network which exploited the fast parcel system to move illegal drugs. Working with key partners at home such as Border Force and abroad with HSI, we have removed a significant amount of Class A from circulation and denied Rahman's organized crime group the chance to plough profits from those drugs into more criminality. We are determined to do all we can to disrupt all drugs supply routes in and out of the UK.” Tim Hemker, attache at the US Homeland Security Investigations: "Homeland Security Investigations is proud of our strong partnership with the National Crime Agency. "Today's sentencing is the result of our agencies' exemplary collaboration to hold criminals on the dark web accountable for illegally selling and shipping narcotics overseas and putting countless individuals in danger. "We will continue to work together to keep drugs off our streets and our communities safe.” archive.is/archive.org If this guy is a part of a large-scale DTO that operated on markets with the kind of weight described in the article, I think somebody will know the vendor username. (via darknetlive.com at https://darknetlive.com/post/uk-darkweb-drug-trafficker-sentenced-to-prison/)

Three Arrested in Austria for Selling Ecstasy and Marijuana

Police in Braunau arrested three people for allegedly buying drugs on the darkweb and reselling them to local customers. Police in Braunau arrested a 29-year-old Romanian, a 40-year-old Croatian citizen, and a 35-year-old Hungarian citizen for selling drugs to people in Braunau. The suspects allegedly distributed "almost 1,000 ecstasy tablets, 700 grams of marijuana in the last six months.” Investigators believe that the 29-year-old has been ordering drugs from vendors on the darkweb since the summer of 2021. In two instances that the police are aware of, the suspect imported 1.5 kilograms of cocaine from a supplier in Germany. The 29-year-old, using a fake identity, worked as a waiter in Braunau. The suspects allegedly sold drugs to people around a "trendy bar” in the area. polizei.gv.at: He is also accused of selling a large part of the drugs to mentally disabled, underage buyers and of having received sexual favors in return. Those allegations seem like quite the jackpot for a prosecutor. Are they saying that mentally disabled 15-year-olds, possibly at a bar, had sex with one or more defendants? Is there a concentration of underage drug buyers with mental disabilities in the area? Surely the crime would be the "sexual relations with a minor” part. Otherwise, wouldn't the customer be just as guilty of exchanging sex for drugs? What is the implication here? The State Criminal Police Office of Upper Austria, the police in Vöcklabruck, and the police in Steyr arrested the defendants after the trio had received a shipment of amphetamines. During the execution of search warrants, the police found drugs intended for sale. All three suspects made full confessions. Police are now investigating the trio's customers. archive.is/archive.org (via darknetlive.com at https://darknetlive.com/post/three-arrested-in-austria-for-selling-ecstasy-and-marijuana/)

National Crime Agency Wants to Regulate Bitcoin Mixers

The UK's National Crime Agency is calling for the regulation of cryptocurrency mixers. Gary Cathcart, head of financial investigation at the National Crime Agency, said that mixers "can be used to provide a 'layering' service, churning criminal cash, obscuring its origins and audit trail, similar to how a cash business might be used by criminals to legitimize cash through the banking system.” According to the NCA, "regulation would force mixers to comply with money laundering laws, with an obligation to carry out customer checks and audit trails of currencies passing through the platforms.” The NCA said that law enforcement needs to be able to investigate "what is often serious criminal activity.” Per Bitcoin Wiki The Financial Times first covered the story. The FT piece includes very few NCA quotes but identifies Wasabi Wallet, Samourai Wallet, and Helix as "three well-known services.” Helix's creator, Larry Dean Harmon, pleaded guilty to money laundering in 2021, leaving only Wasabi and Samourai as the current services named in the article. The piece focused on non-custodial CoinJoin which might be difficult to regulate. Samourai Wallet In the Financial Times piece, the author provided examples of the illegal use of mixers. The author wrote that the NCA is concerned about "ransomware attacks, fraud, state-sponsored crime, and terrorism.” Helpfully, the author also included statements from "the world's oldest and the UK's leading defense and security think tank,” the Royal United Services Institute. "However, free and open-source software algorithms in which there is no entity that takes custody of funds cannot be effectively regulated.” Allison Owen, an analyst who leads the Royal United Services Institute's work on cryptocurrencies and financial crime, said mixers could be used by governments to evade sanctions. "People argue the blockchain has so much transparency when it comes to transactions monitoring, but you still need to make sure the monitoring is taking place,” she added. A reporter with the Financial Times reached out to Samourai about the NCA's call to regulate mixers. Samourai responded with a solid 500+ word email that provided appropriate context to the Financial Times piece. The published article, though, included only one sentence from Samourai. The email sent from Financial Times to Samourai devs. Europol also highlighted Samourai Wallet as an emerging "top threat” in 2020 due to its decentralized nature. Samourai said it believes the "vast majority” of users who use this type of CoinJoin software are law-abiding. "We agree that the use of centralized mixers that take possession and custody of funds should be scrutinized and avoided,” the company added in a statement. I refuse to respond to requests for comment from any mainstream media outlet. In my opinion, the Financial Times running a piece critical of Bitcoin mixers is akin to the Wall Street Journal running their article critical of WallStreetBets. Most of you know the reasons for this, so there is no need to go into that.

/r/wallstreetbets Since the Financial Times only published such a small part of Samourai's response, I included their complete response below. There must be a distinction made between what the NCA has labelled 'crypto mixers' and the open source software algorithms that are used in Samourai Wallet, known as CoinJoin. A "mixer” implies a custodial system where crypto is sent into the control of a third party custodian who promises to send back crypto that is unrelated to the deposit. The software that Samourai Wallet produces is fundamentally different. In the Samourai software, users individually collaborate with each other to compose what are known as CoinJoin transactions to themselves. The user retains custody of their bitcoin at all times and a transmission of funds to any third party never occurs. While it is true that Bitcoin is a pseudonymous system at the protocol level, the vast majority of crypto on-ramps and off-ramps are the custodians of vast amounts of personally identifiable information about their users — to comply with KYC and AML guidelines and regulations. Several of these custodians have had serious data breaches where this sensitive information is now in the hands of criminals and other bad actors putting innocent users at increased risk of being the target of serious crime like fraud, kidnapping, or worse. With transparent ledgers like the Bitcoin blockchain every transaction is publicly recorded and viewable by anyone indefinitely, a situation no normal person would tolerate in the existing financial system. The existing system has several legislative mechanisms built in that ensure basic privacy (your bank doesn't share your account balance and transaction history with the barista at the coffee shop for example). The blockchain doesn't have the luxury of legislative power to solve these problems, therefore software solutions such as CoinJoin are used to obtain these basic protections. The argument that crypto users identity is obscured on the blockchain so users shouldn't need to worry themselves with basic financial privacy is not only bad advice, it is a feeble attempt to justify an unprecedented encroachment into the financial privacy of law abiding citizens. The NCA's remit is to stop serious and organized crime not regulate the behaviour of law abiding citizens. Elliptic doesn't provide the underlying data they use to produce these unverifiable numbers. Their methodolgy is often a black box, where headline numbers and charts are presented in lieu of data. Likewise, government contracts play an important part of for profit businesses like Elliptic. It is our contention that these figures are likely overstated. For H1 2021, FINCEN estiamted ransomware, by far the largest illicit use volume of bitcoin, to mixer flows at only 1% (source). Elliptic's and FINCEN's estimates are an order of magnitude apart, which implies one of them is wrong. We believe the vast majority of users who are using non custodial CoinJoin software are law abiding and simply trying to obtain a basic level of financial privacy when using a transparent and public blockchain. Businesses that take custody of funds on behalf of customers are already heavily regulated. We agree that the use of centralized mixers that take possession and custody of funds should be scrutinized and avoided. However, free and open source software algorithms in which there is no entity that takes custody of funds cannot be effectively regulated. We believe the NCA should instead focus on more productive methods to prevent serious crime and catch criminals. I hate that I feel the need to point this out but it do be like that. I am not endorsing Bitcoin mixers at all. I like CoinJoin and appreciate Wasabi and Samourai. CoinJoin is not a replacement for Monero (and there is at least one of you who claims Monero is not a replacement for cash or Runescape coins or something). And for all I know, Samourai is a fed op. Also, I am aware that it is not feasible for a publication such as the Financial Times to publish Samourai's entire response. Also, also, "we want to regulate cryptocurrency mixers” sounds like the response to an unprompted question from a journalist asking, "does the NCA want to regulate cryptocurrency mixers?” Do you have a license for that satoshi, mate? Criddle, Cristina. "NCA Calls for Regulation of Crypto Mixers Used in 'Churning Criminal Cash'.” Financial Times, Financial Times, 15 Mar. 2022, https://www.ft.com/content/c6df2b68-a244-4560-9911-88cc1fa61576. archive.ph/archive.org (via darknetlive.com at https://darknetlive.com/post/national-crime-agency-wants-to-regulate-bitcoin-mixers/)

Simple OPSEC Failure: Harvard Bomb Hoax

In 2013, a Harvard University student sent a bomb threat to university faculty members. Although the student had used the Tor Browser and an anonymous email address, law enforcement identified him hours after sending the threats. I remembered this case after seeing a post by a user on Dread who asked about the "best way to safely hide tor usage.” Most people will probably remember this case.

A good question to ask. The Bomb Threat _ On December 16, 2013, "Eldo Kim, 20, of Cambridge, emailed several bomb threats to offices associated with Harvard University, including the Harvard University Police Department and the Harvard Crimson, the student-run daily newspaper.” The emails had the subject line "bombs placed around campus” and contained the following message: shrapnel bombs placed in:
science center
sever hall
emerson hall
thayer hall
2/4. guess correctly.
be quick for they will go off soon __ a Harvard alert concerning the bomb hoax. The Harvard University Police Department notified the Federal Bureau of Investigation (FBI) in response to the emails. The FBI immediately began an investigation on the campus, in coordination with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE), the United States Secret Service (USSS), the Harvard University Police Department, the Cambridge Police Department, the Boston Police Department; and the Massachusetts State Police. Officers evacuated the buildings specified in the emails and searched them for explosives. __ Police evacuated the listed buildings and searched for bombs X-Originating-IP _ The FBI investigated the origin of the emails. They learned that someone had used Guerrilla Mail, a disposable email service, to send the threats. Guerrilla Mail attaches the header X-Originating-IP:[the user's IP address] to every outgoing email. The FBI saw that the person responsible for sending the emails had accessed Guerrilla Mail through Tor. The criminal complaint does not explain how the FBI learned that the suspect had used Tor. However, the simplest explanation is that Guerrilla Mail embedded the IP address of the Tor exit node Kim had used. As The Privacy Blog pointed out, "even if they had not embedded the IP, GuerrillaMail keep logs which would have been available to the FBI with a warrant.” __ Guerrilla Mail is an anti-spam service When investigating the IP address, the FBI saw that it matched an IP address of an exit node. Investigators and Harvard University employees analyzed the logs for the University's wireless network. The logs revealed that Kim had been using Tor in the hours leading up to receipt of the emails. The rest is history. Confession _ The FBI and an officer of the Harvard University Police Department questioned Kim. They advised Kim of his rights under Miranda. Then Kim confessed to sending the emails in an attempt to avoid taking an exam. Kim then stated that he authored the bomb threat emails described above. Kim stated that he acted alone. He further stated that he sent the emails to "five or six Harvard University email addresses” that he picked randomly from the University's web page. According to Kim, he was motivated by a desire to avoid a final exam scheduled to be held on December 16, 2013. Kim further stated that he sent all of the threatening emails at about 8:30 a.m. and that he used TOR to create a "guerrillamail.com” email address for each of the emails. Kim explained that he sent all the bomb-threat emails from his MacBook Pro Laptop. Kim stated he chose the word "shrapnel” because it sounded more dangerous and wrote, "2/4. guess correctly,” so that it would take more time for the Harvard Police Department to clear the area. Kim was scheduled to take a final exam in Emerson Hall, a building on the Harvard campus, at 9:00 a.m. on December 16, 2013. Kim stated that he was in Emerson Hall at 9:00 a.m. when the fire alarm sounded and the building was evacuated. According to Kim, upon hearing the alarm, he knew that his plan had worked. To be clear, Tor did not fail. Kim was one of very few, if any, university students using Tor in time before the bomb threats were received. Also, Kim's plan was a success, I think. Affidavit pdf archive.org (DOJ Announcement) (via darknetlive.com at https://darknetlive.com/post/simple-opsec-failure-harvard-bomb-hoax/)

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

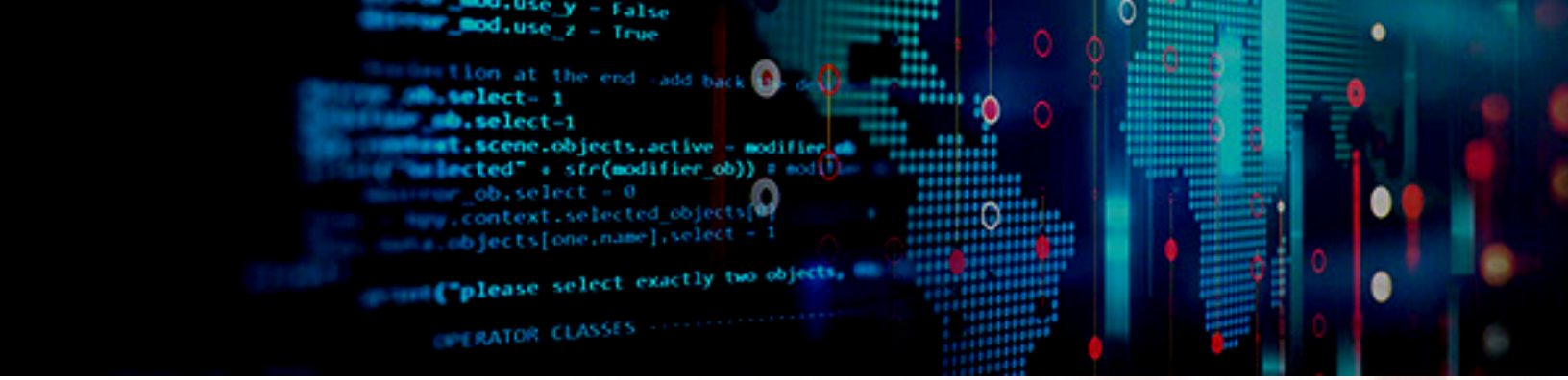
Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

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

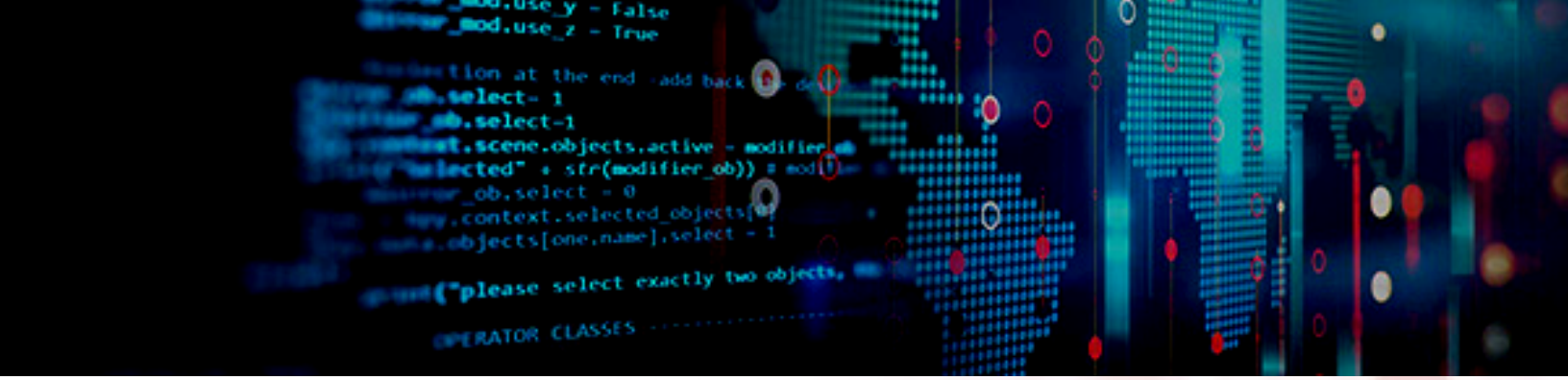
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* 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

FireEye

* Metasploit Weekly Wrap-Up
* 3 Ways InsightIDR Customers Leverage the MITRE ATT&CK Framework
* [Security Nation] Bob Lord on Securing the DNC
* The VM Lifecycle: How We Got Here, and Where We're Going
* Cybercriminals' Recruiting Effort Highlights Need for Proper User Access Controls
* InsightVM Scanning: Demystifying SSH Credential Elevation
* An Inside Look at CISA's Supply Chain Task Force
* Metasploit Weekly Wrap-Up
* Run Faster Log Searches With InsightIDR
* 7Rapid Questions: Growing From BDR to Commercial Sales Manager With Maria Loughrey



Advisories

US-Cert Alerts & bulletins

* CRI-O Security Update for Kubernetes
* WordPress Releases Security Update
* ISC Releases Security Advisories for BIND
* Strengthening Cybersecurity of SATCOM Network Providers and Customers
* OpenSSL Releases Security Updates
* Drupal Releases Security Updates
* Apple Releases Security Updates for Multiple Products
* Google Releases Security Updates for Chrome
* AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers
* AA22-074A: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor
* Vulnerability Summary for the Week of March 7, 2022
* Vulnerability Summary for the Week of February 28, 2022

Zero Day Initiative Advisories

ZDI-CAN-16710: DevExpress
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Markus Wulftange (@mwulftange)' was reported to the affected vendor on: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16872: 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: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16887: Autodesk
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16882: Autodesk
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16874: 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: 2022-03-16, 5 days ago. The vendor is

given until 2022-07-14 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-16871: 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: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16875: 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: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16873: 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: 2022-03-16, 5 days ago. The vendor is given until 2022-07-14 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-16821: 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, 10 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-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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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, 10 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.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5333-2

Ubuntu Security Notice 5333-2 - USN-5333-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Chamal De Silva discovered that the Apache HTTP Server mod_lua module incorrectly handled certain crafted request bodies. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service.

Ubuntu Security Notice USN-5332-2

Ubuntu Security Notice 5332-2 - USN-5332-1 fixed a vulnerability in Bind. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Xiang Li, Baojun Liu, Chaoyi Lu, and Changgen Zou discovered that Bind incorrectly handled certain bogus NS records when using forwarders. A remote attacker could possibly use this issue to manipulate cache results.

Ubuntu Security Notice USN-5333-1

Ubuntu Security Notice 5333-1 - Chamal De Silva discovered that the Apache HTTP Server mod_lua module incorrectly handled certain crafted request bodies. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. James Kettle discovered that the Apache HTTP Server incorrectly closed inbound connection when certain errors are encountered. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Ubuntu Security Notice USN-5332-1

Ubuntu Security Notice 5332-1 - Xiang Li, Baojun Liu, Chaoyi Lu, and Changgen Zou discovered that Bind incorrectly handled certain bogus NS records when using forwarders. A remote attacker could possibly use this issue to manipulate cache results. It was discovered that Bind incorrectly handled certain crafted TCP streams. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. This issue only affected Ubuntu 21.10.

Ubuntu Security Notice USN-5321-2

Ubuntu Security Notice 5321-2 - USN-5321-1 fixed vulnerabilities in Firefox. The update didn't include arm64 because of a regression. This update provides the corresponding update for arm64. This update also removes Yandex and Mail.ru as optional search providers in the drop-down search menu.

Ubuntu Security Notice USN-5334-1

Ubuntu Security Notice 5334-1 - It was discovered that man-db incorrectly handled permission changing operations in its daily cron job, and was therefore affected by a race condition. An attacker could possibly use this issue to escalate privileges and execute arbitrary code.

Ubuntu Security Notice USN-5326-1

Ubuntu Security Notice 5326-1 - It was discovered that FUSE is susceptible to a restriction bypass flaw on a system that has SELinux active. A local attacker with non-root privileges could mount a FUSE file system that is accessible to other users and trick them into accessing files on that file system, which could result in a Denial of Service or other unspecified conditions.

Red Hat Security Advisory 2022-0947-01

Red Hat Security Advisory 2022-0947-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains the RHEL-8-CNV-4.10 OpenShift Virtualization 4.10.0 image.

Red Hat Security Advisory 2022-0952-01

Red Hat Security Advisory 2022-0952-01 - Red Hat Directory Server is an LDAPv3-compliant directory server. The suite of packages includes the Lightweight Directory Access Protocol server, as well as command-line utilities and Web UI packages for server administration. Issues addressed include double free and null pointer vulnerabilities.

Red Hat Security Advisory 2022-0951-01

Red Hat Security Advisory 2022-0951-01 - Expat is a C library for parsing XML documents. Issues addressed include code execution and integer overflow vulnerabilities.

Red Hat Security Advisory 2022-0949-01

Red Hat Security Advisory 2022-0949-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include a privilege escalation vulnerability.

Ubuntu Security Notice USN-5331-1

Ubuntu Security Notice 5331-1 - It was discovered that tcpdump incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code. It was discovered that tcpdump incorrectly handled certain captured data. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2022-0810-01

Red Hat Security Advisory 2022-0810-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.4. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5329-1

Ubuntu Security Notice 5329-1 - It was discovered that tar incorrectly handled certain files. An attacker could possibly use this issue to cause tar to crash, resulting in a denial of service.

Red Hat Security Advisory 2022-0889-01

Red Hat Security Advisory 2022-0889-01 - 389 Directory Server is an LDAP version 3 compliant server. The base packages include the Lightweight Directory Access Protocol server and command-line utilities for server administration. Issues addressed include a double free vulnerability.

Ubuntu Security Notice USN-5330-1

Ubuntu Security Notice 5330-1 - It was discovered that LibreOffice incorrectly handled digital signatures. An attacker could possibly use this issue to create a specially crafted document that would display a validly signed indicator, contrary to expectations.

Red Hat Security Advisory 2022-0896-01

Red Hat Security Advisory 2022-0896-01 - The glibc packages provide the standard C libraries, POSIX thread libraries, standard math libraries, and the name service cache daemon used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-5328-2

Ubuntu Security Notice 5328-2 - USN-5328-1 fixed a vulnerability in OpenSSL. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Tavis Ormandy discovered that OpenSSL incorrectly parsed certain certificates. A remote attacker could possibly use this issue to cause OpenSSH to stop responding, resulting in a denial of service.

Ubuntu Security Notice USN-5328-1

Ubuntu Security Notice 5328-1 - Tavis Ormandy discovered that OpenSSL incorrectly parsed certain certificates. A remote attacker could possibly use this issue to cause OpenSSH to stop responding, resulting in a denial of service.

Ubuntu Security Notice USN-5327-1

Ubuntu Security Notice 5327-1 - Hiroyuki Yamamori discovered that rsh incorrectly handled certain filenames. If a user or automated system were tricked into connecting to a malicious rsh server, a remote attacker could possibly use this issue to modify directory permissions.

Red Hat Security Advisory 2022-0899-01

Red Hat Security Advisory 2022-0899-01 - The libxml2 library is a development toolbox providing the implementation of various XML standards. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-0892-01

Red Hat Security Advisory 2022-0892-01 - The libarchive programming library can create and read several different streaming archive formats, including GNU tar, cpio, and ISO 9660 CD-ROM images. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several popular

desktop file managers.

Red Hat Security Advisory 2022-0925-01

Red Hat Security Advisory 2022-0925-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0894-01

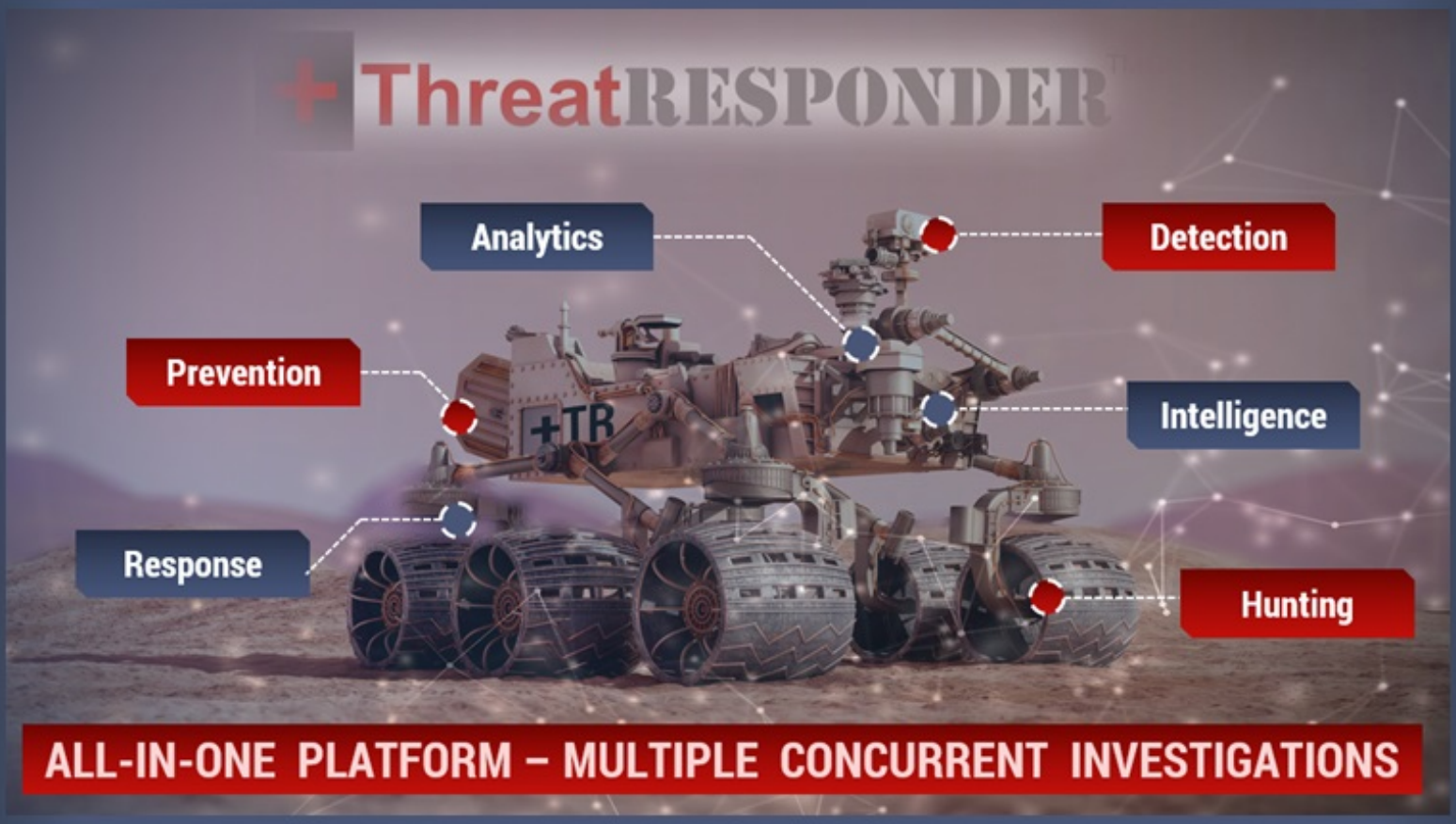
Red Hat Security Advisory 2022-0894-01 - Vim is an updated and improved version of the vi editor. Issues addressed include buffer overflow and use-after-free vulnerabilities.

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



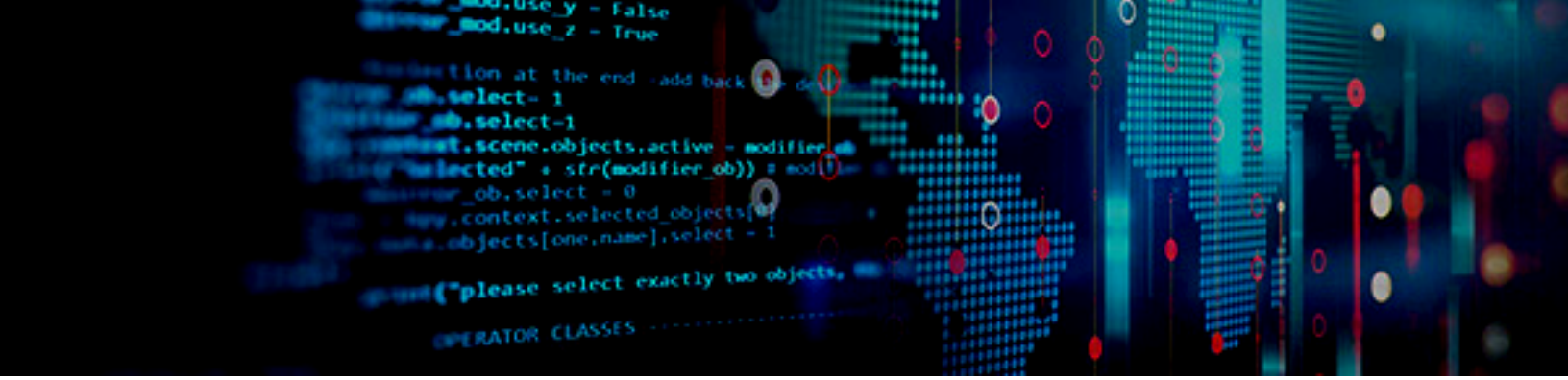
The Solution – ThreatResponder® Platform

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

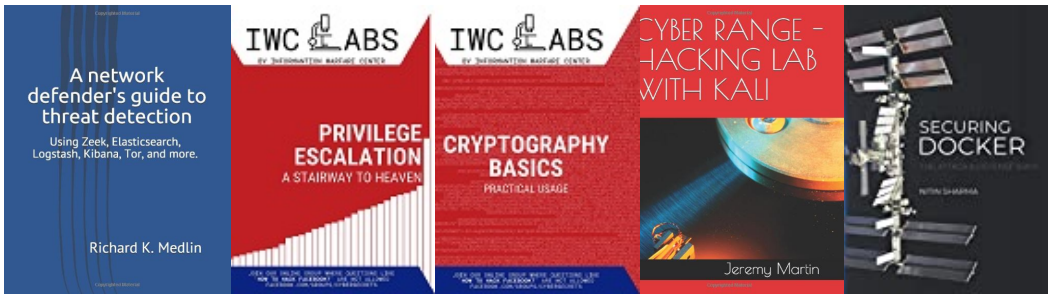


The Cyber Secrets publications on Amazon

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