Aug-29-22

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

August 29, 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

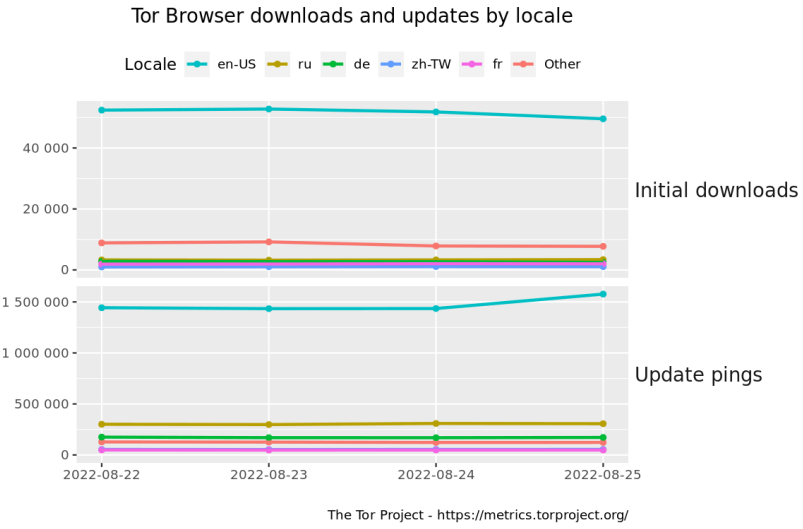
Internet Storm Center Infocon Status

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

* A Massive Hacking Campaign Stole 10,000 Login Credentials From 130 Different Organizations
* LastPass Source Code, Blueprints Stolen By Intruder
* Nato Investigates Hacker Sale Of Missile Firm Data
* Chinese Surveillance Camera Access Is Being Sold
* Hackers Leaked Data Anyways After Company Pays Ransom
* Websites Can Identify If You're Using iPhone's New Lockdown Mode
* Hackers Are Breaking Into And Emptying Cash App Accounts
* Hackers Steal Data For More Than 15 Million Users From Plex
* Firewall Bug Under Active Attack Triggers CISA Warning
* Unix Legend, Who Owes Us Nothing, Keeps Fixing Foundational AWK Code
* Elon Subpoenas Twitter Whistleblower To Testify About Counting Bots
* Hackers Use Deepfakes Of Binance Exec To Scam Multiple Crypto Projects
* Lloyd's To Exclude Certain Nation State Attacks From Cyber Insurance Policies
* Microsoft Finds Critical Hole In OS That For Once Isn't Windows
* If You Haven't Patched Zimbra Holes By Now, Assume You're Toast
* Priti Patel Urges Meta To Give Up On End-To-End Encryption Plans
* Mudge Blows The Whistle On Twitter's Security
* Zoom Patches Make-Me-Root Security Flaw, Patches Patch
* Israeli Spyware Company NSO Group CEO Steps Down
* Why The Pentagon Remains Both The Best And Worst Customer For Tech Innovators
* Fake Reservation Links Prey On Weary Travelers
* Sudden Crypto Drop Sends Bitcoin To Three Week Low
* Apple Security Flaw Actively Exploited By Hackers To Fully Control Devices
* Two Years On, Apple iOS VPNs Still Leak IP Addresses
* About That Draft Law Banning Uncle Sam Buying Insecure Software

Krebs on Security

* PayPal Phishing Scam Uses Invoices Sent Via PayPal
* When Efforts to Contain a Data Breach Backfire
* Sounding the Alarm on Emergency Alert System Flaws
* It Might Be Our Data, But It's Not Our Breach
* The Security Pros and Cons of Using Email Aliases
* Microsoft Patch Tuesday, August 2022 Edition
* Class Action Targets Experian Over Account Security
* Scammers Sent Uber to Take Elderly Lady to the Bank
* No SOCKS, No Shoes, No Malware Proxy Services!
* 911 Proxy Service Implodes After Disclosing Breach

Dark Reading

* Microsoft 365 Empowers Business Users to Shoot Themselves in the Foot
* LastPass Suffers Data Breach, Source Code Stolen
* 'Sliver' Emerges as Cobalt Strike Alternative for Malicious C2
* 'No-Party' Data Architectures Promise More Control, Better Security
* How DevSecOps Empowers Citizen Developers
* Endpoint Protection / Antivirus Products Tested for Malware Protection
* Capital One Joins Open Source Security Foundation
* Twilio Hackers Scarf 10K Okta Credentials in Sprawling Supply-Chain Attack
* ReasonLabs Launches Free Online Security Tool to Power Secure Web Experience for Millions of Global U
* More Bang for the Buck: Cross-Platform Ransomware Is the Next Problem
* Wyden Renews Call to Encrypt Twitter DMs, Secure Americans' Data From Unfriendly Foreign Governments
* Senior-Level Women Leaders in Cybersecurity Form New Nonprofit
* Cyberstarts Closes $60M in Seed Fund III
* The (Nation) State of Cyber: 64% of Businesses Suspect They've Been Targeted or Impacted by Nation-St
* What You Need to Know About the Psychology Behind Cyber Resilience
* Penetration Testing Market Worth $2.7B By 2027: MarketsandMarkets(TM) Report
* Optiv's Annual $40K Scholarship for Black, African-American-Identifying STEM Students Now Open for Ap
* New Exterro FTK Update Accelerates Mobile Digital Forensics
* Thousands of Organizations Remain at Risk From Critical Zero-Click IP Camera Bug
* CISA: Just-Disclosed Palo Alto Networks Firewall Bug Under Active Exploit

The Hacker News

* Twilio Breach Also Compromised Authy Two-Factor Accounts of Some Users
* CISA Adds 10 New Known Actively Exploited Vulnerabilities to its Catalog
* Iranian Hackers Exploiting Unpatched Log4j 2 Bugs to Target Israeli Organizations
* Critical Vulnerability Discovered in Atlassian Bitbucket Server and Data Center
* Hackers Breach LastPass Developer System to Steal Source Code
* Cybercrime Groups Increasingly Adopting Sliver Command-and-Control Framework
* Okta Hackers Behind Twilio and Cloudflare Breach Hit Over 130 Organizations
* Microsoft Uncovers New Post-Compromise Malware Used by Nobelium Hackers
* U.S. Government Spending Billions on Cybersecurity
* Researchers Uncover Kimusky Infra Targeting South Korean Politicians and Diplomats
* PyPI Repository Warns Python Project Maintainers About Ongoing Phishing Attacks
* Crypto Miners Using Tox P2P Messenger as Command and Control Server
* Air-Gapped Devices Can Send Covert Morse Signals via Network Card LEDs
* Guide: How Service Providers can Deliver vCISO Services at Scale
* Hackers Using Fake DDoS Protection Pages to Distribute Malware

Security Week

* Facebook Parent Settles Suit in Cambridge Analytica Scandal
* Montenegro Reports Massive Russian Cyberattack Against Govt
* Atlassian Ships Urgent Patch for Critical Bitbucket Vulnerability
* Twitter, Meta Remove Accounts Linked to US Influence Operations: Report
* DoorDash Discloses Data Breach Related to Attack That Hit Twilio, Others
* Ransomware Operator Abuses Anti-Cheat Driver to Disable Antiviruses
* Crypto Firms Say US Sanctions Limit Use of Privacy Software
* Iranian Government Hackers Exploit Log4Shell in SysAid Apps for Initial Access
* New 'Agenda' Ransomware Customized for Each Victim
* CISA Urges Critical Infrastructure to Prepare for Post-Quantum Cryptography
* CISA: Vulnerability in Delta Electronics ICS Software Exploited in Attacks
* Twitter Ordered to Give Musk Additional Bot Account Data
* LastPass Says Source Code Stolen in Data Breach
* Leaked Docs Show Spyware Firm Offering iOS, Android Hacking Services for $8 Million
* XIoT Vendors Show Progress on Discovering, Fixing Firmware Vulnerabilities
* Cisco Patches High-Severity Vulnerabilities in Business Switches
* BalkanID Adds $2.3M to Seed Funding Round
* Google Open Sources 'Paranoid' Crypto Testing Library
* Cosmetics Giant Sephora Settles Customer Data Privacy Suit
* Twilio, Cloudflare Attacked in Campaign That Hit Over 130 Organizations
* Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird
* How Economic Changes and Crypto's Rise Are Fueling the use of "Cyber Mules"
* Musk Lawyers Seize on Twitter Whistleblower Revelations
* Microsoft Details New Post-Compromise Malware Used by Russian Cyberspies
* Privacy Activists Target Google Over French 'Spam' Emails
* New Air Gap-Jumping Attack Uses Ultrasonic Tones and Smartphone Gyroscope

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Researchers warn of darkverse emerging from the metaverse
* State-Based Cyberattacks to be Excluded from Lloyd's of London Cyber Insurance Policies
* The Crypto Collapse Will Only Add Fuel to the Cyberattack Fire
* BlackByte Ransomware Gang Comes Back to Life with a New Extortion Strategy
* Phishing Remains the Initial Infection Vector in 78% of Attacks Against OT-Heavy Industries
* Report: Deepfakes Used in Scams
* [HEADS UP] Highly Sophisticated Job Offer Scam
* Dueling Clauses, or, not all Fraud is the Same
* [BUDGET AMMO] Companies Are Ditching Cybersecurity Insurance as Premiums Rise, Coverage Shrinks
* Teach Two Things to Decrease Phishing Attack Success

ISC2.org Blog

* Latest Cyberthreats and Advisories - August 26, 2022
* Poll: Cybersecurity Professionals Want Remote Work Options
* The 'Hottest' IT Security Technologies in 2022
* New to Cybersecurity? Use These Career Hacks to Get a Foot in the Door
* Latest Cyberthreats and Advisories - August 19, 2022

HackRead

* NATO Probes Hackers Selling Data from Top Missile Firm MBDA
* 5 Signs your WordPress Site is Hacked (And How to Fix It)
* DoorDash Data Breach -Third Party Vendor Blamed Over Phishing Attack
* Scammers Made Deepfake AI Hologram of Binance Executive
* LastPass Security Breach - Hackers Steal Company's Source Code
* SolarWinds Hackers Using New Post-Exploitation Backdoor 'MagicWeb'
* Plex Breach - Streaming Giant Issues Mass Password Reset to Millions

Koddos

* NATO Probes Hackers Selling Data from Top Missile Firm MBDA
* 5 Signs your WordPress Site is Hacked (And How to Fix It)
* DoorDash Data Breach -Third Party Vendor Blamed Over Phishing Attack
* Scammers Made Deepfake AI Hologram of Binance Executive
* LastPass Security Breach - Hackers Steal Company's Source Code
* SolarWinds Hackers Using New Post-Exploitation Backdoor 'MagicWeb'
* Plex Breach - Streaming Giant Issues Mass Password Reset to Millions

Naked Security

* Firefox 104 is out - no critical bugs, but update anyway
* S3 Ep97: Did your iPhone get pwned? How would you know? [Audio + Text]
* Breaching airgap security: using your phone's compass as a microphone!
* Bitcoin ATMs leeched by attackers who created fake admin accounts
* Laptop denial-of-service via music: the 1980s R&B song with a CVE!
* Apple patches double zero-day in browser and kernel - update now!
* S3 Ep96: Zoom 0-day, AEPIC leak, Conti reward, healthcare security [Audio + Text]
* Chrome browser gets 11 security fixes with 1 zero-day - update now!
* US offers reward "up to $10 million" for information about the Conti gang
* Zoom for Mac patches critical bug - update now!

Threat Post

* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year
* APT Lazarus Targets Engineers with macOS Malware
* U.K. Water Supplier Hit with Clop Ransomware Attack
* Xiaomi Phone Bug Allowed Payment Forgery

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

* Give finops a say over cloud architecture decisions
* What is JSON? The universal data format
* 12 ggplot extensions for snazzier R graphics
* BrandPost: Reduce Time to Decision With the Databricks Lakehouse Platform and Latest Intel 3rd Gen Xe
* Intro to Astro: Clever lazy loading for JavaScript
* Kestrel: The Microsoft web server you should be using
* Tech job market is up this year
* Kissflow review: No code and low code for workflows
* BrandPost: Optimize and Accelerate Cloud Apps for Cost Reduction With IntelÂ® Workload Optimizer
* 3 reasons cloud computing doesn't save money

C4ISRNET - Media for the Intelligence Age Military

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

The Hacker Corner

Conferences

* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021
* Is It Worth Public Speaking?

Google Zero Day Project

* The quantum state of Linux kernel garbage collection CVE-2021-0920 (Part I)
* 2022 0-day In-the-Wild Exploitation…so far

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.

* Balsn CTF 2022
* CakeCTF 2022
* [POSTPONED] CyberSpace CTF
* Winja CTF | Nullcon Goa 2022
* CSAW CTF Qualification Round 2022
* VolgaCTF 2022 Final
* 0CTF/TCTF 2022
* Information and Technology Festival 2022
* DownUnderCTF 2022 (Online)
* SekaiCTF 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

* GNU Privacy Guard 2.2.37
* MIMEDefang Email Scanner 3.1
* I2P 1.9.0
* TOR Virtual Network Tunneling Tool 0.4.7.10
* GNUnet P2P Framework 0.17.4
* Falco 0.32.2
* American Fuzzy Lop plus plus 4.02c
* GNUnet P2P Framework 0.17.3
* Faraday 4.0.4
* Wireshark Analyzer 3.6.7

Kali Linux Tutorials

* Hoaxshell : An Unconventional Windows Reverse Shell, Currently Undetected By Microsoft Defender
* VLANPWN : VLAN Attacks Toolkit
* RedGuard : C2 Front Flow Control Tool, Can Avoid Blue Teams, AVs, EDRs Check
* NimGetSyscallStub : Get Fresh Syscalls From A Fresh Ntdll.Dll Copy
* Chisel-Strike : A .NET XOR Encrypted Cobalt Strike Aggressor Implementation For Chisel To Utilize Fas
* OffensiveVBA : Code Execution And AV Evasion Methods For Macros In Office Documents
* Packj : Large-Scale Security Analysis Platform To Detect Malicious/Risky Open-Source Packages
* MrKaplan : Tool Aimed To Help Red Teamers To Stay Hidden By Clearing Evidence Of Execution
* BlackStone : Pentesting Reporting Tool
* Smap : A Drop-In Replacement For Nmap Powered By Shodan.Io

GBHackers Analysis

* LastPass Developer Account Hacked to Steal the Company's Source Code
* Researchers Hacked SpaceX Operated Starlink Satellite Using $25 Modchip
* Hackers Use Open Redirect Vulnerabilities in Online Services to Deliver Phishing Content
* Hackers Exploiting High-Severity Zimbra Flaw to Steal Email Account Credentials
* 24-Year-Old Australian Hacker Arrested For Creating and Selling Spyware

Weekly Cyber Security Video and Podcasts

SANS DFIR

* The Godfather of Forensics: How to Leverage Your "Year One" to Get an Offer You Cannot Refuse
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown (STAR) | Live Stream
* Introducing the Enterprise Cloud Forensics & Incident Response Poster

Defcon Conference

* DEF CON 30 - The Dark Tangent and MK Factor - Welcome to DEF CON and The Making of the DEF CON Badge
* DEF CON 30 - Perimeter Breached! Hacking an access control system - Sam Quinn Steve Povolny
* DEF CON 30 - Blacks in CyberSecurity Village Interview
* DEF CON 30 - ICS Village Interview

Hak5

* Sneaky Password Exfiltration w/ CanaryTokens & the Nugget!
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Spying On Ring Video - Vulnerability Discovered in Android App - ThreatWire

The PC Security Channel [TPSC]

* Upgrading to Windows XP in 2022
* Tech Support Scam installs RAT (when asked for refund)

Eli the Computer Guy

* Kinda Lame KILLER ROBOTS!!!
* Gender Identity and the Tech Industry - Rethinking Sports and War
* Dojo Derby - PS4 Controller to Python Script for Raspberry Pi
* Investing in LEGO - Is Bitcoin a Currency (Brickville, Asheville)

Security Now

* The Bumblebee Loader - RTL819x Exploit, RubyGems Update, Chrome's Fifth 0-Day of 2022
* TLS Private Key Leakage - BIG patch Tuesday, Facebook E2E encryption, VNC insecurity, Cyotek WebCopy

Troy Hunt

* Weekly Update 310

Intel Techniques: The Privacy, Security, & OSINT Show

* 276-When Google Attacks

* 275-Archived Site Removal & Breaches Galore

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Xalan-J XSLTC Integer Truncation
* Centreon 22.04.0 Cross Site Scripting
* PrestaShop Ap Pagebuilder 2.4.4 SQL Injection
* Arm Mali CSF VMA Split Mishandling
* Zimbra Zip Path Traversal
* Teleport 9.3.6 Command Injection
* 10-Strike Network Inventory Explorer 9.3 Buffer Overflow
* Microsoft Exchange Server ChainedSerializationBinder Remote Code Execution
* Personnel Property Equipment 2015-2022 SQL Injection
* AppleAVD AVC_RBSP::parseSliceHeader ref_pic_list_modification Overflow
* Transposh WordPress Translation 1.0.8.1 Incorrect Authorization
* FLIR AX8 1.46.16 Traversal / Access Control / Command Injection / XSS
* Chrome content::ServiceWorkerVersion::MaybeTimeoutRequest Heap Use-After-Free
* FLIX AX8 1.46.16 Remote Command Execution
* Advantech iView NetworkServlet Command Injection
* Polar Flow Android 5.7.1 Secret Disclosure
* FreeBSD 13.0 aio_aqueue Kernel Refcount Local Privilege Escalation
* Race Against The Sandbox
* TypeORM 0.3.7 Information Disclosure
* Windows Credential Guard Domain-Joined Device Public Key Privilege Escalation
* Win32.Ransom.BlueSky MVID-2022-0632 Code Execution
* Inout RealEstate 2.1.2 SQL Injection
* Inout SiteSearch 2.0.1 Cross Site Scripting
* Gigaland NFT Marketplace 1.9 Shell Upload / Key Disclosure
* Windows sxssrv!BaseSrvActivationContextCacheDuplicateUnicodeString Heap Buffer Overflow

CXSecurity

* WordPress Duplicator 1.4.7.2 Backup Disclosure
* Microsoft Exchange Server ChainedSerializationBinder Remote Code Execution
* FLIX AX8 1.46.16 Remote Command Execution
* Advantech iView NetworkServlet Command Injection
* PAN-OS 10.0 Remote Code Execution
* Webmin Package Updates Command Injection
* Zoho Password Manager Pro XML-RPC Java Deserialization

Proof of Concept (PoC) & Exploits

Exploit Database

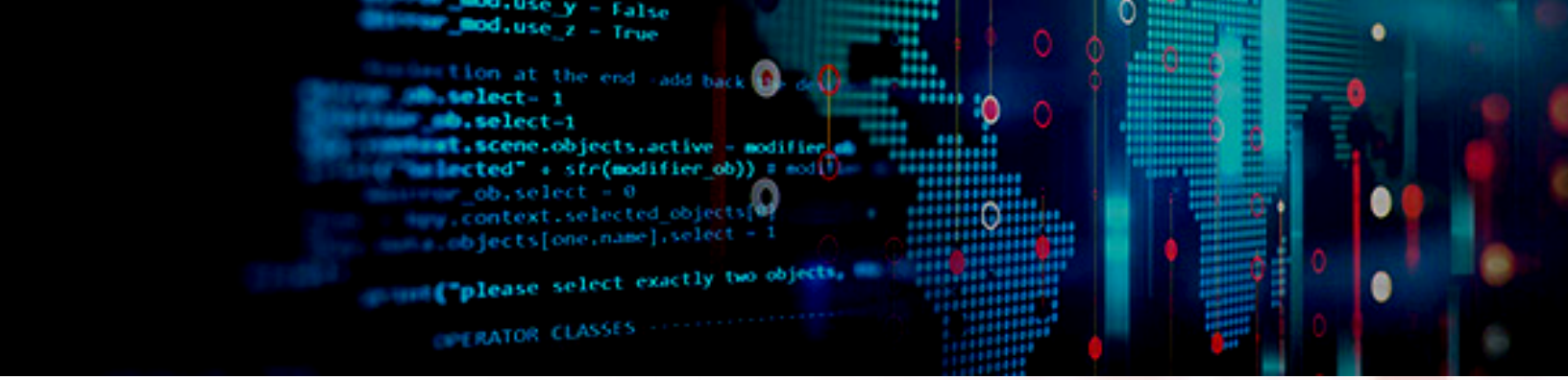
* [remote] PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)
* [webapps] ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)
* [webapps] Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Prestashop blockwishlist module 2.1.0 - SQLi
* [remote] uftpd 2.10 - Directory Traversal (Authenticated)
* [remote] Easy Chat Server 3.1 - Remote Stack Buffer Overflow (SEH)
* [webapps] Webmin 1.996 - Remote Code Execution (RCE) (Authenticated)
* [webapps] NanoCMS v0.4 - Remote Code Execution (RCE) (Authenticated)
* [remote] Omnia MPX 1.5.0+r1 - Path Traversal
* [webapps] mPDF 7.0 - Local File Inclusion
* [webapps] CuteEditor for PHP 6.6 - Directory Traversal
* [webapps] WordPress Plugin Duplicator 1.4.7 - Information Disclosure
* [webapps] WordPress Plugin Duplicator 1.4.6 - Unauthenticated Backup Download
* [webapps] Wavlink WN530HG4 - Password Disclosure
* [webapps] Wavlink WN533A8 - Password Disclosure
* [webapps] Wavlink WN533A8 - Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin WP-UserOnline 2.87.6 - Stored Cross-Site Scripting (XSS)
* [remote] Schneider Electric SpaceLogic C-Bus Home Controller (5200WHC2) - Remote Code Execution
* [webapps] Carel pCOWeb HVAC BACnet Gateway 2.1.0 - Directory Traversal
* [local] Asus GameSDK v1.0.0.4 - 'GameSDK.exe' Unquoted Service Path
* [webapps] Dingtian-DT-R002 3.1.276A - Authentication Bypass
* [remote] rpc.py 0.6.0 - Remote Code Execution (RCE)
* [webapps] Geonetwork 4.2.0 - XML External Entity (XXE)
* [webapps] WordPress Plugin Visual Slide Box Builder 3.2.9 - SQLi

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*

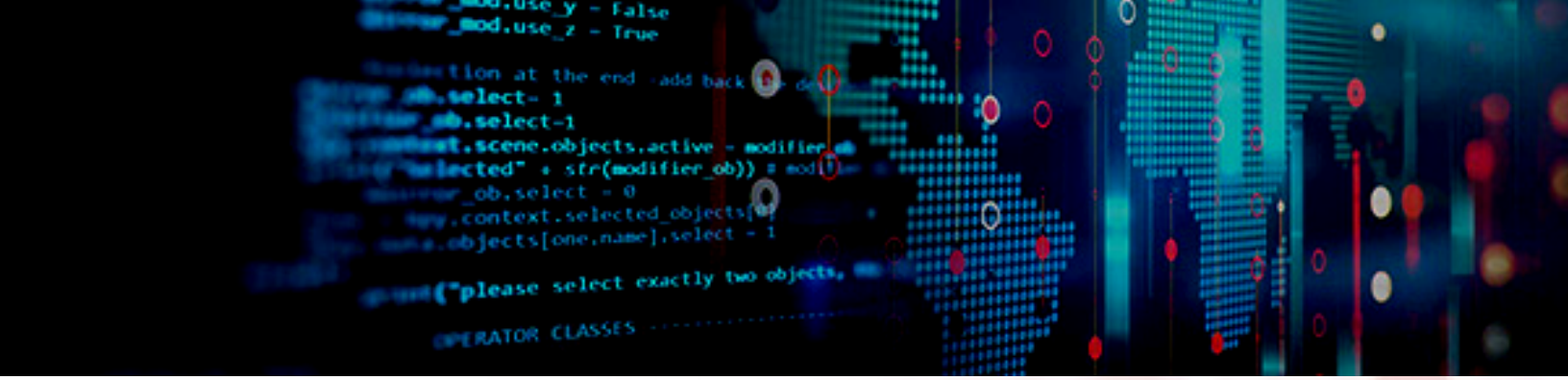
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://akademi.tpe.gov.tr/z.html
https://akademi.tpe.gov.tr/z.html notified by Zer0FauLT
https://akademi.turkpatent.gov.tr/z.html
https://akademi.turkpatent.gov.tr/z.html notified by Zer0FauLT
https://www.ci.gov.tr
https://www.ci.gov.tr notified by Zer0FauLT
http://donmuang-local.go.th/index.php
http://donmuang-local.go.th/index.php notified by ./Niz4r
http://www.khokyanglocal.go.th/index.php
http://www.khokyanglocal.go.th/index.php notified by ./Niz4r
http://tambonbansong.go.th/index.php
http://tambonbansong.go.th/index.php notified by ./Niz4r
http://ss-muni.go.th/index.php
http://ss-muni.go.th/index.php notified by ./Niz4r
http://disperindag.bengkaliskab.go.id/index.php
http://disperindag.bengkaliskab.go.id/index.php notified by 7.htm
http://kesbangpol.bengkaliskab.go.id/index.php
http://kesbangpol.bengkaliskab.go.id/index.php notified by 7.htm
http://kabbengkalis.baznas.go.id/index.php
http://kabbengkalis.baznas.go.id/index.php notified by 7.htm
http://www.sungnoenabt.go.th/read.html
http://www.sungnoenabt.go.th/read.html notified by ./Niz4r
http://alfonsolista.gov.ph
http://alfonsolista.gov.ph notified by Matigan1337
http://benitosoliven-isabela.gov.ph
http://benitosoliven-isabela.gov.ph notified by Matigan1337
http://casiguran-aurora.gov.ph
http://casiguran-aurora.gov.ph notified by Matigan1337
http://cabatuan-isabela.gov.ph
http://cabatuan-isabela.gov.ph notified by Matigan1337
http://bappeda.bengkaliskab.go.id/index.php
http://bappeda.bengkaliskab.go.id/index.php notified by 7.htm
http://biblioteca.comune.montecosaro.mc.it/gootloader.html
http://biblioteca.comune.montecosaro.mc.it/gootloader.html notified by TheInternetJanitor



Dark Web News

Darknet Live

German Man Sentenced for Ordering 100 Grams of Marijuana

A 21-year-old who admitted buying 100 grams of marijuana was sentenced to eight addiction counseling sessions instead of prison. The defendant had ordered 100 grams of marijuana from a supplier on the darkweb. Customs officers intercepted the package. Later, police searched the 21-year-old's apartment in Berchtesgaden and found five more grams of marijuana. They also seized his electronic devices. During a hearing at the Laufen district court, the prosecution admitted that investigators had not found evidence of drug trafficking. However, the defendant had ordered much more than a "personal use” amount of marijuana, the prosecutor told the court. Additionally, if tried as an adult, the defendant would have faced a minimum sentence of one year in prison. Polizei The defendant argued that he had ordered so much marijuana because he could not acquire it locally. He described the 100-gram order as a supply that would last a long time. The presiding judge sentenced the defendant to eight addiction counseling sessions, as many as two drug tests, and a fine of 1,300 euros. Drogenvorrat über »Darknet« bestellt | archive.is, archive.org, www.berchtesgadener-anzeiger.de (via darknetlive.com at https://darknetlive.com/post/german-man-sentenced-to-therapy-for-100-gram-drug-purchase/)

178 Arrested in South Korea for Buying Marijuana on Internet

Police in South Korea arrested 178 people for buying or selling marijuana through the internet. The Seoul Metropolitan Police Agency (SMPA) arrested 178 people for buying or selling marijuana through the darkweb or social media. The arrests are the result of an ongoing crackdown on internet-based drug trafficking. Police seized 12 kilograms of marijuana, 136 grams of synthetic marijuana, and 302 ecstasy pills during the operation. HDR police activities | SMPA Of the 178 suspects, only 12 face drug trafficking charges. The remainder face charges for purchasing or possessing marijuana. Most of the suspects are between the ages of 20 and 30. "Police attributed the demography to more opportunities for younger people to buy and sell drugs through the internet and social media. The SMPA has said it will continue a broad clampdown on drug trafficking on the internet through the end of October.” 178 people nabbed for selling, buying marijuana | archive.is, archive.org, en.yna.co.kr (via darknetlive.com at https://darknetlive.com/post/178-arrested-in-south-korea-buying-marijuana-on-darkweb/)

Police Shut Down 16 Cryptocurrency Exchangers in Afghanistan

Police in Afghanistan shut down 16 cryptocurrency exchangers in the country's Herat province in response to complaints about scams and pyramid schemes. "Da Afghanistan's Bank stated in a letter that digital currency trading has caused lots of problems and is scamming people, therefore they should be closed. We acted and arrested all the exchangers involved in the business and closed their shops,” said Sayed Shah Sa'adat, head of the counter-crime unit of Herat police. Authorities in Afghanistan have been receiving hundreds of complaints every month about fraudulent cryptocurrency exchanges and pyramid schemes. Afghan money changers The local independent outlet Ariana reported that Afghanistan's central bank outlawed cryptocurrency trading in June 2022. Ghulam Mohammad Sohrabi, head of Herat's money

changers' union, said: "Our people are not familiar with digital currencies, their accounts are not the same as bank accounts of dollars, euros and Afghanis; Because there are no documents. On this account, until our people know, don't use it. Digital currency accounts are located outside the country and are purchased from companies; Our people do not know. It would be better if they don't use this money, because this currency has just entered the market and is highly variable. The Herat Currency Exchange Association agreed that digital currencies are reliable in other markets and are in use by other countries. Ariana quoted two residents of Herat who agreed with the government's actions: "Digital currency is a new phenomenon which is not used in Afghanistan, therefore the process should be monitored by the government so that there will be no scamming and people can make better investments,” said Shahram, a resident in Herat. "The government should monitor and prevent digital currency activities, otherwise assets leave Afghanistan. People also suffer losses because syndicates are involved and rates fluctuate daily,” said Mawla Alizada, a Herat resident.

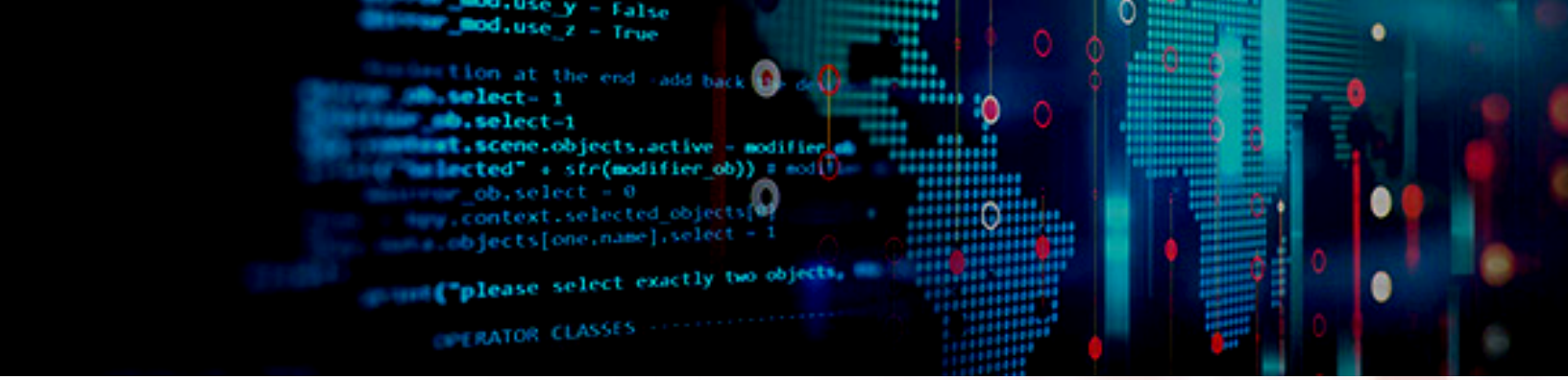
The non-occupation government of Afghanistan holding a mock funeral for the Western 'nation builders' (via darknetlive.com at https://darknetlive.com/post/chad-taliban-vs-scamming-money-changers/)

German Man Allegedly Tried to Hire a Killer on the Darkweb

A 63-year-old from Stuttgart allegedly tried to hire a hitman on the darkweb to kill a relative. Authorities arrested the man in April 2022 in Franconia. The arrest followed a tip from the Federal Criminal Police Office. The Stuttgart public prosecutor's office has now filed charges. There is not much information available about the case. nordbayern.de: "Drugs, weapons or even a contract killer - criminals will find all kinds of things on the dark web. A 63-year-old from Stuttgart, who worked in Uffenheim in the Neustadt/Aisch-Bad Windsheim district, is now accused of attempted incitement to murder. At the end of April, the police arrested the man at his workplace on a tip from the Federal Criminal Police Office.” "But what is the 63-year-old accused of? According to Johannes Steinbach, he is said to have given the order via the Darknet to have his brother poisoned. He probably made the decision to have his brother killed in 2021. Regarding the condition of the suspect, Steinbach explained that he "is said to be suffering from a chronic delusional disorder.” The man is currently temporarily housed in forensic psychiatry.” These are getting old frankly. More interesting news is that the Washington Post is trying to get Tether in trouble for ignoring Tornado Cash sanctions. Imagine contacting the Treasury as well as government-staffed blockchain analytics companies because Tether (based in Hong Kong) is not obeying the U.S. government. Wait until these people learn about Elude or Kilos.

A Tornado Cash developer might still have a Gmail account. Quick! (via darknetlive.com at https://darknetlive.com/post/german-man-tried-to-have-brother-killed-via-darkweb/)

Dark Web Link



Trend Micro Anti-Malware Blog

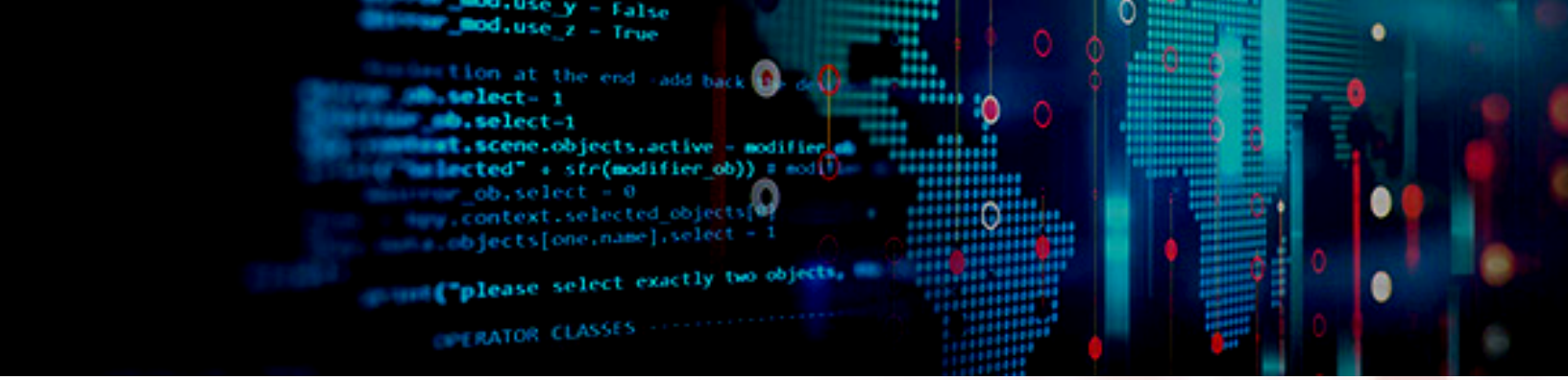
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Wrap-Up
* Incident Reporting Regulations Summary and Chart
* [The Lost Bots] S02E03: Browser-in-Browser Attacks - Don't Get (Cat)-Phished
* Cybersecurity Analysts: Job Stress Is Bad, but Boredom Is Kryptonite
* Avoiding Smash and Grab Under the SEC's Proposed Cyber Rule
* Network Access for Sale: Protect Your Organization Against This Growing Threat
* Metasploit Wrap-Up
* Pushing Open-Source Security Forward: Insights From Black Hat 2022
* 360-Degree XDR and Attack Surface Coverage With Rapid7
* [Security Nation] Jen and Tod on Hacker Summer Camp 2022



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for Multiple Products
* CISA releases 1 Industrial Control Systems Advisory
* CISA Adds Ten Known Exploited Vulnerabilities to Catalog
* Preparing Critical Infrastructure for Post-Quantum Cryptography
* VMware Releases Security Update
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* CISA releases 7 Industrial Control Systems Advisories
* CISA Updates Advisory on Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite
* AA22-228A: Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite
* AA22-223A: #StopRansomware: Zeppelin Ransomware
* Vulnerability Summary for the Week of August 15, 2022
* Vulnerability Summary for the Week of August 8, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5474-2

Ubuntu Security Notice 5474-2 - USN-5474-1 fixed vulnerabilities in Varnish Cache. Unfortunately the fix for CVE-2020-11653 was incomplete. This update fixes the problem. It was discovered that Varnish Cache could have an assertion failure when a TLS termination proxy uses PROXY version 2. A remote attacker could possibly use this issue to restart the daemon and cause a performance loss.

Red Hat Security Advisory 2022-6187-01

Red Hat Security Advisory 2022-6187-01 - This is an updated release of the Node Health Check Operator. You can use the Node Health Check Operator to deploy the Node Health Check controller. The controller identifies unhealthy nodes and uses the Self Node Remediation Operator to remediate the unhealthy nodes.

Red Hat Security Advisory 2022-6184-01

Red Hat Security Advisory 2022-6184-01 - The Self Node Remediation Operator works in conjunction with the Machine Health Check or the Node Health Check Operators to provide automatic remediation of unhealthy nodes by rebooting them. This minimizes downtime for stateful applications and RWO volumes, as well as restoring compute capacity in the event of transient failures.

Ubuntu Security Notice USN-5582-1

Ubuntu Security Notice 5582-1 - Arthur Mongodin discovered that the netfilter subsystem in the Linux kernel did not properly perform data validation. A local attacker could use this to escalate privileges in certain situations. Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5581-1

Ubuntu Security Notice 5581-1 - Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the contents of the addressbar, bypass security restrictions, or execute arbitrary code.

Ubuntu Security Notice USN-5579-1

Ubuntu Security Notice 5579-1 - Roger Pau Monné discovered that the Xen virtual block driver in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information. Roger Pau Monné discovered that the Xen paravirtualization frontend in the Linux kernel did not properly initialize memory pages to be used for shared communication with the backend. A local attacker could use this to expose sensitive information.

Ubuntu Security Notice USN-5578-2

Ubuntu Security Notice 5578-2 - USN-5578-1 fixed a vulnerability in Open VM Tools. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that Open VM Tools incorrectly handled certain requests. An attacker inside the guest could possibly use this issue to gain root privileges inside the virtual machine.

Ubuntu Security Notice USN-5580-1

Ubuntu Security Notice 5580-1 - It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the virtual terminal driver in the Linux kernel did not properly handle VGA console font changes, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2022-6155-01

Red Hat Security Advisory 2022-6155-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Red Hat Security Advisory 2022-6163-01

Red Hat Security Advisory 2022-6163-01 - The systemd packages contain systemd, a system and service

manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6157-01

Red Hat Security Advisory 2022-6157-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6170-01

Red Hat Security Advisory 2022-6170-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

Red Hat Security Advisory 2022-6178-01

Red Hat Security Advisory 2022-6178-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.13.0 ESR. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6165-01

Red Hat Security Advisory 2022-6165-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.13.0. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6158-01

Red Hat Security Advisory 2022-6158-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Red Hat Security Advisory 2022-6160-01

Red Hat Security Advisory 2022-6160-01 - The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6180-01

Red Hat Security Advisory 2022-6180-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

Red Hat Security Advisory 2022-6175-01

Red Hat Security Advisory 2022-6175-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.13.0 ESR. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6169-01

Red Hat Security Advisory 2022-6169-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.13.0. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6168-01

Red Hat Security Advisory 2022-6168-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.13.0. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6161-01

Red Hat Security Advisory 2022-6161-01 - The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6179-01

Red Hat Security Advisory 2022-6179-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.13.0 ESR. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6166-01

Red Hat Security Advisory 2022-6166-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.13.0. Issues addressed include spoofing and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-6171-01

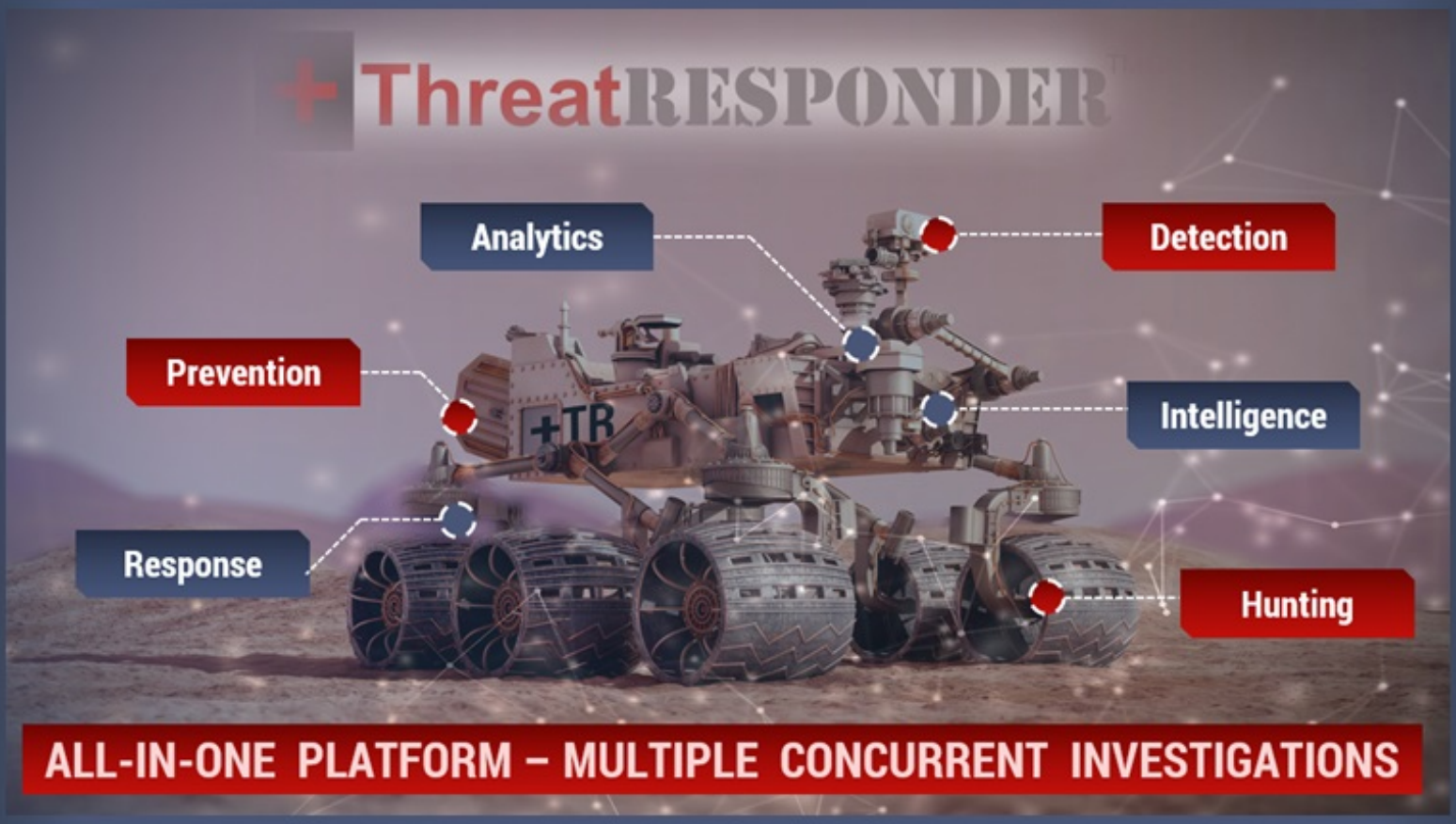
Red Hat Security Advisory 2022-6171-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

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



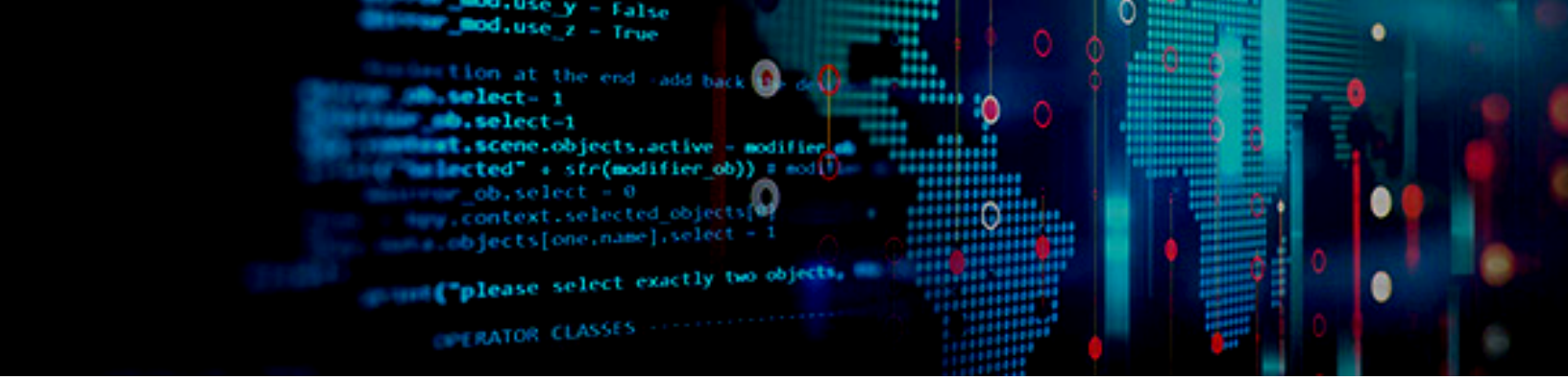
The Solution – ThreatResponder® Platform

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

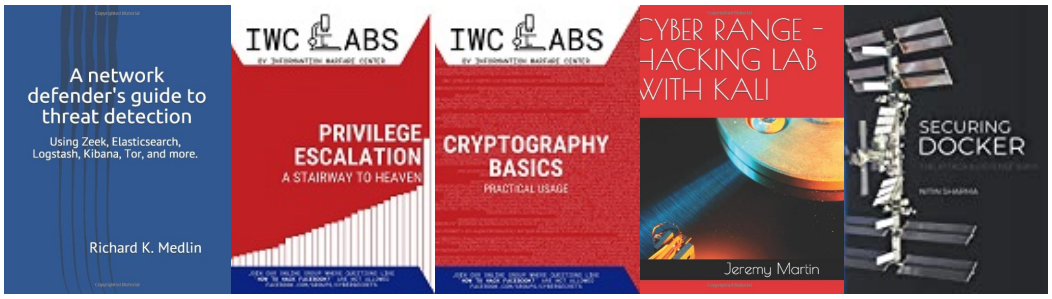


The Cyber Secrets publications on Amazon

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