Jun-20-22

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

June 20, 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

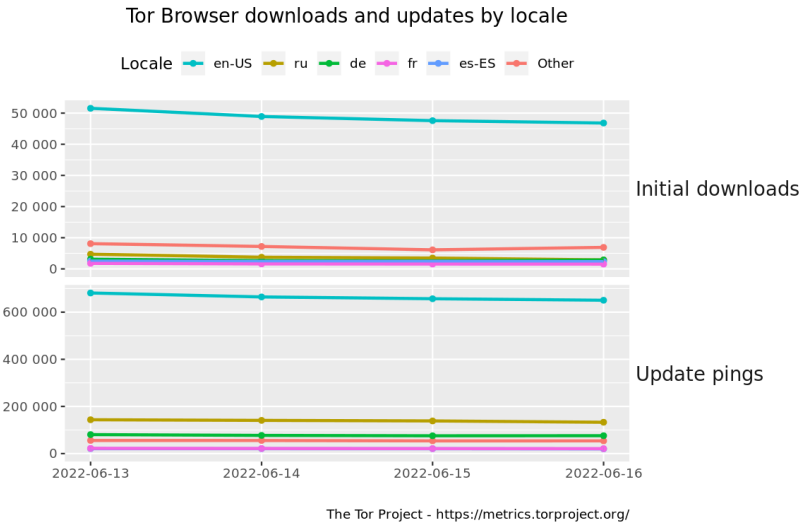
Internet Storm Center Infocon Status

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

* International Operation Takes Down Russian RSOCKS Botnet
* Police Linked To Hacking Campaign To Frame Indian Activists
* Facebook Messenger Scam Duped Millions
* China-Linked APT Flew Under Radar For A Decade
* Linux Botnet Finds Novel Way Of Spreading To New Devices
* U.S. Water Utilities Prime Cyberattack Target, Experts
* Since 2004, The Average American Has Had At Least 7 Data Breaches
* Apple M1 Chip Contains Hardware Vulnerability That Bypasses Memory Defense
* Potent Emotet Variant Spreads Via Stolen Email Credentials
* This Hacking Group Quietly Spied On Their Targets For 10 Years
* NASA To Figure Out How To Get Data On Unexplained Objects In The Sky
* Expect Downtime Next Week For Packet Storm
* Ministry Of Defence Acquires Government's First Quantum Computer
* Optimism Crypto Project Hopes Hacker Will Give Back $15 Million
* Russia Says West Risks Direct Military Clash Over Cyber Attacks
* New Tesla Hack Gives Thieves Their Own Personal Key
* Symantec: More Malware Operators Moving In To Exploit Follina
* 5 Key Questions The Jan. 6 Committee Will Tackle In Its Hearings
* This New Linux Malware Is Almost Impossible To Detect
* Black Basta Ransomware Teams Up With Malware Stalwart Qbot
* Maiar Exchange Taken Offline After Hacker Steals $113m
* Osmosis Blockchain Taken Offline After Hacker Steals $5m
* Data For 2 Million Patients Stolen In Largest Healthcare Breach So Far In 2022
* Feds Raid Dark Web Market Selling Data On 24 Million Americans
* NSA, FBI Warning: Hackers Are Using These Flaws To Target VPNs And Network Devices

Krebs on Security

* Microsoft Patch Tuesday, June 2022 Edition
* Ransomware Group Debuts Searchable Victim Data
* "Downthem" DDoS-for-Hire Boss Gets 2 Years in Prison
* Adconion Execs Plead Guilty in Federal Anti-Spam Case
* KrebsOnSecurity in New Netflix Series on Cybercrime
* What Counts as "Good Faith Security Research?"
* Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions
* Senators Urge FTC to Probe ID.me Over Selfie Data
* When Your Smart ID Card Reader Comes With Malware
* DEA Investigating Breach of Law Enforcement Data Portal

Dark Reading

* Ransomware and Phishing Remain IT's Biggest Concerns
* WordPress Plug-in Ninja Forms Issues Update for Critical Bug
* DeadBolt Ransomware Actively Targets QNAP NAS Devices - Again
* Atlassian Confluence Server Bug Under Active Attack to Distribute Ransomware
* Can We Make a Global Agreement to Halt Attacks on Our Energy Infrastructure?
* Tackling 5 Challenges Facing Critical National Infrastructure Today
* Internet Explorer Now Retired but Still an Attacker Target
* BlastWave Announces Enhancements to Its Zero-Trust Security Software Solution, BlastShield
* Microsoft 365 Function Leaves SharePoint, OneDrive Files Open to Ransomware Attacks
* What We Mean When We Talk About Cyber Insurance
* Android Spyware 'Hermit' Discovered in Targeted Attacks
* Unlocking the Cybersecurity Benefits of Digital Twins
* EU & US Unite to Fight Ransomware
* RSAC Startup Competition Focuses on Post-Cloud IT Infrastructure
* CISOs Gain False Confidence in the Calm After the Storm of the Pandemic
* Are You Hiring Enough Entry-Level Security Pros?
* How Should I Think About Security When Considering Digital Transformation Projects?
* Cisco's Ash Devata on the Future of Secure Access
* 7 Ways to Bring AI to Cybersecurity
* 'Hertzbleed' Side-Channel Attack Threatens Cryptographic Keys for Servers

The Hacker News

* Google Researchers Detail 5-Year-Old Apple Safari Vulnerability Exploited in the Wild
* BRATA Android Malware Gains Advanced Mobile Threat Capabilities
* Over a Dozen Flaws Found in Siemens' Industrial Network Management System
* Learn Cybersecurity with Palo Alto Networks Through this PCCSA Course @ 93% OFF
* Authorities Shut Down Russian RSOCKS Botnet That Hacked Millions of Devices
* Atlassian Confluence Flaw Being Used to Deploy Ransomware and Crypto Miners
* Researchers Uncover 'Hermit' Android Spyware Used in Kazakhstan, Syria, and Italy
* Reimagine Hybrid Work: Same CyberSec in Office and at Home
* Chinese Hackers Exploited Sophos Firewall Zero-Day Flaw to Target South Asian Entity
* Over a Million WordPress Sites Forcibly Updated to Patch a Critical Plugin Vulnerability
* BlackCat Ransomware Gang Targeting Unpatched Microsoft Exchange Servers
* A Microsoft Office 365 Feature Could Help Ransomware Hackers Hold Cloud Files Hostage
* Difference Between Agent-Based and Network-Based Internal Vulnerability Scanning
* High-Severity RCE Vulnerability Reported in Popular Fastjson Library
* MaliBot: A New Android Banking Trojan Spotted in the Wild

Security Week

* Breach at Eye Care Software Vendor Hits Millions of Patients
* Staffing Firm Robert Half Says Hackers Targeted Over 1,000 Customer Accounts
* Now On Demand: SecurityWeek Cloud Security Summit, Presented by Palo Alto Networks
* Hybrid Networks Require an Integrated On-prem and Cloud Security Strategy
* Law Enforcement Dismantle Infrastructure of Russian 'RSOCKS' Botnet
* Details of Twice-Patched Windows RDP Vulnerability Disclosed
* Exploited Vulnerability Patched in WordPress Plugin With Over 1 Million Installations
* Cybersecurity M&A Deals Surge in First Half of June 2022
* Costa Rica Chaos a Warning That Ransomware Threat Remains
* 'MaliBot' Android Malware Steals Financial, Personal Information
* Volexity Blames 'DriftingCloud' APT For Sophos Firewall Zero-Day
* Microsoft Dismisses False Reports About End of Patch Tuesday
* Cisco Patches Critical Vulnerability in Email Security Appliance
* 2,000 People Arrested Worldwide for Social Engineering Schemes
* Sophisticated Android Spyware 'Hermit' Used by Governments
* Researchers Discover Way to Attack SharePoint and OneDrive Files With Ransomware
* Using the Defense Readiness Index to Improve Security Team Skills
* At Second Trial, Ex-CIA Employee Defends Himself in Big Leak
* GreyNoise Attracts Major Investor Interest
* Jit Banks Massive $38.5 Million Seed Round Funding
* Now LIVE: SecurityWeek Cloud Security Summit, Presented by Palo Alto Networks
* Lessons for Better Fraud Decision-Making
* Critical Code Execution Vulnerability Patched in Splunk Enterprise
* So Long, Internet Explorer. The Browser Retires Today
* Small Botnet Launches Record-Breaking 26 Million RPS DDoS Attack
* New 'Hertzbleed' Remote Side-Channel Attack Affects Intel, AMD Processors

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Anna Collard, SVP Content Strategy & Evangelist, KnowBe4 Africa Has Been Acknowledged as a Globa
* A Closer Look at HR Scams: Does Niceness Have a Downside?
* Spear Phishing Campaign Targets Former Israeli Officials
* CyberheistNews Vol 12 #24 [Heads Up] What About the Risks of Your Password Manager?
* Monkeypox Scams Continue to Increase
* Facebook Phishing Scam Steals Millions of Credentials
* Approaching Ransomware Victims Privately
* What About Password Manager Risks?
* Karakurt Adds Irritating Phone Calls to its Crimes
* 40% of CSOs say Their Organization is Not Prepared for Cyberattacks as Phishing is the Top Likely Cau

ISC2.org Blog

* SECURE North America | Apple Stories: How Technology Has Mediated Technology Through History
* ENTRY-LEVEL CYBERSECURITY JOBS KEY TO SOLVING WORKFORCE GAP
* How can mentorship help the cybersecurity workforce gap?
* U.S. State and Federal Funding for Cybersecurity is on the Rise
* (ISC)² Concludes Online Proctored Exams Do Not Meet Exam Security Standards

HackRead

* 9 Years Jail for iCloud Phishing Scam Hacker Who Stole Nude Photos
* New MaliBot Android Malware Found Stealing Personal, Banking Data
* How to configure cPanel and WHM Panel on your VPS
* How Data Landlords Put Their Tenants at Risk
* Play Store Apps Caught Spreading Android Malware to Millions
* Cloudflare Thwarted Largest Ever HTTPS DDoS Attack
* Elasticsearch Database Mess Up Exposed Login, PII Data of 30,000 Students

Koddos

* 9 Years Jail for iCloud Phishing Scam Hacker Who Stole Nude Photos
* New MaliBot Android Malware Found Stealing Personal, Banking Data
* How to configure cPanel and WHM Panel on your VPS
* How Data Landlords Put Their Tenants at Risk
* Play Store Apps Caught Spreading Android Malware to Millions
* Cloudflare Thwarted Largest Ever HTTPS DDoS Attack
* Elasticsearch Database Mess Up Exposed Login, PII Data of 30,000 Students

Naked Security

* S3 Ep87: Follina, AirTags, ID theft and the Law of Big Numbers [Podcast]
* Follina gets fixed - but it's not listed in the Patch Tuesday patches!
* Murder suspect admits she tracked cheating partner with hidden AirTag
* You're invited! Join us for a live walkthrough of the "Follina" story…
* S3 Ep86: The crooks were in our network for HOW long?! [Podcast + Transcript]
* SSNDOB Market domains seized, identity theft "brokerage" shut down
* Know your enemy! Learn how cybercrime adversaries get in…
* Atlassian announces 0-day hole in Confluence Server - update now!
* Yet another zero-day (sort of) in Windows "search URL" handling
* S3 Ep85: Now THAT'S what I call a Microsoft Office exploit! [Podcast]

Threat Post

* China-linked APT Flew Under Radar for Decade
* State-Sponsored Phishing Attack Targeted Israeli Military Officials
* Ransomware Risk in Healthcare Endangers Patients
* Facebook Messenger Scam Duped Millions
* DragonForce Gang Unleash Hacks Against Govt. of India
* Travel-related Cybercrime Takes Off as Industry Rebounds
* In Cybersecurity, What You Can't See Can Hurt You
* Kaiser Permanente Exposes Nearly 70K Medical Records in Data Breach
* Linux Malware Deemed 'Nearly Impossible' to Detect
* Bluetooth Signals Can Be Used to Track Smartphones, Say Researchers

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

IBM Security Intelligence

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

InfoWorld

* Microsoft's complicated dance with open source
* How to create a cloud center of excellence
* Are you ready to automate continuous deployment in CI/CD?
* C# extension for Visual Studio Code set for LSP overhaul
* Migration to the cloud may be slowing down
* What is Podman? The container engine replacing Docker
* Aerospike partners with Starburst to jump on the SQL bandwagon
* Okta's Matt Raible: How I became a Java hipster
* How to implement IP whitelists in ASP.NET Core 6
* Internet Explorer reaches the end of the line

C4ISRNET - Media for the Intelligence Age Military

* Prolonged war may make Russia more cyber aggressive, US official says
* Zero Trust in Zero Gravity: US must commit to stay ahead of rivals in space
* Senators seek boosts for JADC2, cyber mission, hypersonics in defense bill
* US Air Force's 'flying car' coming to an exercise near you
* Space Force seeks a bigger voice in military operations
* How war in Ukraine is informing future US Air Force networks
* Space Development Agency plans for 'enduring' satellite experimentation testbed
* Ukraine to get thousands of secure radios in latest US package
* The Army could take a run at developing a robotic 'Warrior Suit'
* How Russia telegraphed invasion of Ukraine in space and online

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

* An Autopsy on a Zombie In-the-Wild 0-day
* Release of Technical Report into the AMD Security Processor

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.

* Azure Assassin Alliance CTF 2022
* BSidesTLV 2022 CTF
* Google Capture The Flag 2022
* FAUST CTF 2022
* vsCTF 2022
* Crypto CTF 2022
* ImaginaryCTF 2022
* UACTF 2022
* 3kCTF-2022
* RED CTF

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

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

Tools & Techniques

Packet Storm Security Tools Links

Kali Linux Tutorials

* Cliam : Multi Cloud IAM Permissions Enumeration Tool
* LDAPFragger : Command And Control Tool That Enables Attackers To Route Cobalt Strike Beacon Data
* FirmWire : b Full-System Baseband Firmware Emulation Platform
* LeakedHandlesFinder : Leaked Windows Processes Handles Identification Tool
* Pybatfish : Python Client For Batfish (Network Configuration Analysis Tool)
* Moonwalk : Cover Your Tracks During Linux Exploitation By Leaving Zero Traces
* Nanodump : A Crappy LSASS Dumper With No ASCII Art
* BackupOperatorToDA : From An Account Member Of The Group Backup Operators To Domain Admin
* Requests-Ip-Rotator : A Python Library To Utilize AWS API Gateway's Large IP Pool
* Dora : Find Exposed API Keys Based On RegEx And Get Exploitation Methods

GBHackers Analysis

* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3
* Pwn2Own - Windows 11, Microsoft Teams Hacked & Exploiting 16 Zero-day Bugs
* Hackers Exploiting a Critical Vulnerability in Zyxel Firewall & VPN Devices
* Multiple QNAP Flaws Let attackers to Access and Read Sensitive Data
* Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Prevent, Detect, Respond An Intro to Google Workspace Security and Incident Response
* Learning to Combat Ransomware
* FOR509: Cloud Forensics & Incident Response Course - What to Expect
* Hunting Is Sacred, But We Never Do It for Sport! - SANS THIR Summit 2019

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

* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Hacking Apple's M1 Chipsets, Who Hacked The Telcos? - ThreatWire
* FluBot Android Banking Malware Shutdown - ThreatWire

The PC Security Channel [TPSC]

* Malwarebytes: Test vs Ransomware
* Windows Zero Day: MSDT Follina Exploit Demonstration

Eli the Computer Guy

* How Does Computer Discovery and Communication Work
* eBeggar Wednesday - BIDEN LESS POPULAR than TRUMP.... pbbbbb
* What is Ethernet
* SILICON DERBY - Gamepad Giving Inconsistent Results at Neutral Position

Security Now

* The PACMAN Attack - WebAuthn, Passkeys at WWDC, Free Kali Linux Pen Test Course, Proof of Simulation
* Passkeys, Take 2 - ServiceNSW Responds, Follina, Windows Search URL, UNISOC Chip Vulnerability

Troy Hunt

* Weekly Update 300

Intel Techniques: The Privacy, Security, & OSINT Show

* 266-The Sole Proprietorship

* 265-HP Dev One with Pop!_OS

Proof of Concept (PoC) & Exploits

Packet Storm Security

CXSecurity

* Navigate CMS 2.9.4 Server-Side Request Forgery (SSRF) (Authenticated)
* Atlassian Confluence Namespace OGNL Injection
* Microsoft Office Word MSDTJS Code Execution
* Confluence Data Center 7.18.0 Remote Code Execution (RCE)
* dotCMS Shell Upload
* NVIDIA Data Center GPU Manager Remote Memory Corruption
* Telesquare SDT-CW3B1 1.1.0 Command Injection

Proof of Concept (PoC) & Exploits

Exploit Database

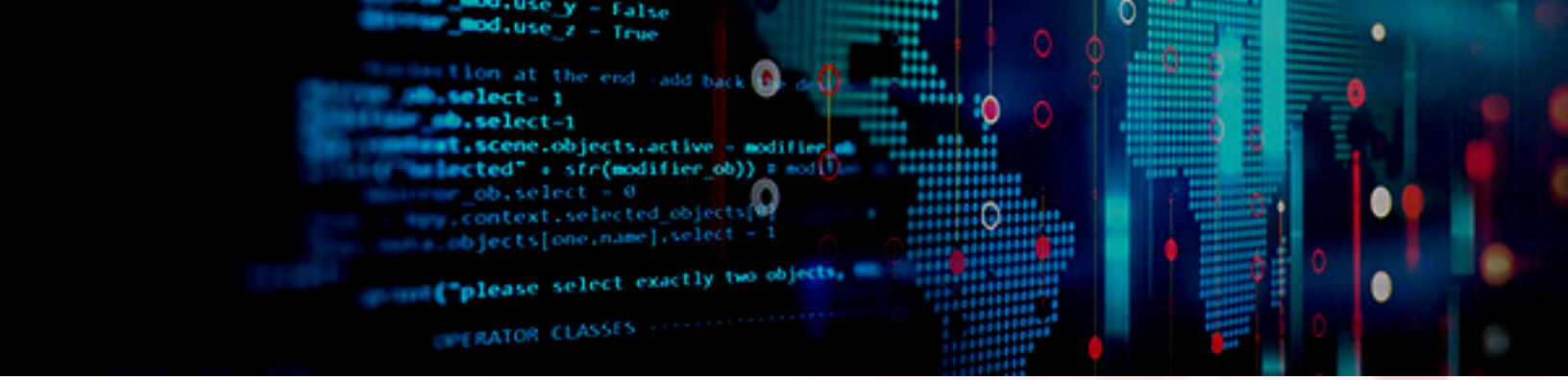
* [webapps] SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)
* [webapps] SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)
* [webapps] Old Age Home Management System 1.0 - SQLi Authentication Bypass
* [webapps] ChurchCRM 4.4.5 - SQLi
* [remote] Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)
* [webapps] phpIPAM 1.4.5 - Remote Code Execution (RCE) (Authenticated)
* [remote] TP-Link Router AX50 firmware 210730 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Pandora FMS v7.0NG.742 - Remote Code Execution (RCE) (Authenticated)
* [remote] Algo 8028 Control Panel - Remote Code Execution (RCE) (Authenticated)
* [local] HP LaserJet Professional M1210 MFP Series Receive Fax Service - Unquoted Service Path
* [remote] Virtua Software Cobranca 12S - SQLi
* [remote] Marval MSM v14.19.0.12476 - Cross-Site Request Forgery (CSRF)
* [remote] Marval MSM v14.19.0.12476 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Avantune Genialcloud ProJ 10 - Cross-Site Scripting (XSS)
* [local] Real Player 16.0.3.51 - 'external::Import()' Directory Traversal to Remote Code Execution (RC
* [local] Real Player v.20.0.8.310 G2 Control - 'DoGoToURL()' Remote Code Execution (RCE)
* [webapps] Confluence Data Center 7.18.0 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)
* [remote] Telesquare SDT-CW3B1 1.1.0 - OS Command Injection
* [webapps] Microweber CMS 1.2.15 - Account Takeover
* [remote] Zyxel USG FLEX 5.21 - OS Command Injection
* [webapps] Contao 4.13.2 - Cross-Site Scripting (XSS)
* [webapps] qdPM 9.1 - Remote Code Execution (RCE) (Authenticated) (v2)

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*

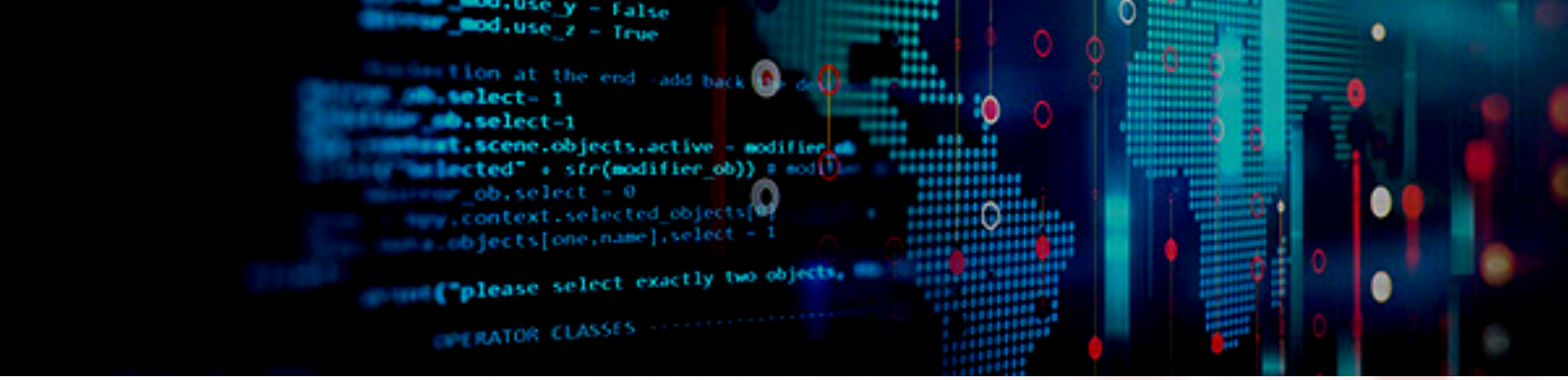
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://blasemarang.kemenag.go.id/readme.html
https://blasemarang.kemenag.go.id/readme.html notified by AnonSec Team
https://bdkpalembang.kemenag.go.id/readme.html
https://bdkpalembang.kemenag.go.id/readme.html notified by AnonSec Team
https://bdksemarang.kemenag.go.id/readme.html
https://bdksemarang.kemenag.go.id/readme.html notified by AnonSec Team
https://bdksurabaya.kemenag.go.id/readme.html
https://bdksurabaya.kemenag.go.id/readme.html notified by AnonSec Team
http://nonedu2.go.th/kz.html
http://nonedu2.go.th/kz.html notified by Mr.Kro0oz.305
https://sakon2.go.th/daka.htm
https://sakon2.go.th/daka.htm notified by telegram@saturaa
http://sop.bppkad.grobogan.go.id/kz.html
http://sop.bppkad.grobogan.go.id/kz.html notified by Mr.Kro0oz.305
https://mesujikab.go.id/br0k3n.htm
https://mesujikab.go.id/br0k3n.htm notified by MR.T1T4N
http://qrayeh.gov.lb/and.html
http://qrayeh.gov.lb/and.html notified by mr.anderson
http://stc.thanhhoa.gov.vn/default.html
http://stc.thanhhoa.gov.vn/default.html notified by RG
http://support.chery.co.il
http://support.chery.co.il notified by -Shahab
http://www7.djop.go.th/index2.html
http://www7.djop.go.th/index2.html notified by ALHOSANE
https://taifnashat.gov.sa/seberia.php
https://taifnashat.gov.sa/seberia.php notified by -X-shadow
http://dinsos.labuhanbatuselatankab.go.id/cek_login.php
http://dinsos.labuhanbatuselatankab.go.id/cek_login.php notified by AnonCoders
http://distanikan.labuhanbatuselatankab.go.id/cek_login.php
http://distanikan.labuhanbatuselatankab.go.id/cek_login.php notified by AnonCoders
http://keckprakyat.labuhanbatuselatankab.go.id/cek_login.php
http://keckprakyat.labuhanbatuselatankab.go.id/cek_login.php notified by AnonCoders
https://apk.tilang.pn-pulaupunjung.go.id/pwn3d.php
https://apk.tilang.pn-pulaupunjung.go.id/pwn3d.php notified by ./KeyzNet



Dark Web News

Darknet Live

UK Home Secretary Approves Assange's Extradition

The U.K. Home Secretary approved the extradition of Julian Assange to the United States. British Home Secretary Priti Patel approved Julian Assange's extradition to the United States. Assange faces 175 years in prison for publishing the material "stolen” by Manning in 2010. Gandalf Assange "The U.K. courts have not found that it would be oppressive, unjust or an abuse of process to extradite Mr. Assange,” the Home Office said. "Nor have they found that extradition would be incompatible with his human rights, including his right to a fair trial and to freedom of expression, and that whilst in the U.S. he will be treated appropriately, including in relation to his health.” Of course, avoiding extradition to the United States was never a real option for Assange. He has 14 days to appeal the decision. Collateral Murder is among the files published by Assange in 2010. "On July 12, 2007, a series of air-to-ground attacks were conducted by a team of two U.S. AH-64 Apache helicopters in Al-Amin al-Thaniyah, New Baghdad, during the Iraqi insurgency which followed the Iraq War. On April 5, 2010, the attacks received worldwide coverage and controversy following the release of 39 minutes of gunsight footage by the Internet whistleblower website WikiLeaks. The footage was portrayed as classified, but the individual who leaked it, U.S. Army soldier Chelsea Manning, testified in 2013 that the video was not classified. The video, which WikiLeaks titled Collateral Murder, showed the crew firing on a group of men and killing several of them, then laughing at some of the casualties, all of whom were civilians, including two Reuters journalists. An anonymous U.S. military official confirmed the authenticity of the footage, which provoked global discussion on the legality and morality of the attacks.” Innocent civilians as well as two Reuters news staff were among those killed in the Collateral Murder video. Assange is not facing charges for the Podesta email dump. WikiLeaks wrote: "This is a dark day for Press freedom and for British democracy. Anyone in this country who cares about freedom of expression should be deeply ashamed that the Home Secretary has approved the extradition of Julian Assange to the United States, the country that plotted his assassination. Julian did nothing wrong. He has committed no crime and is not a criminal. He is a journalist and a publisher, and he is being punished for doing his job. It was in Priti Patel's power to do the right thing. Instead, she will forever be remembered as an accomplice of the United States in its agenda to turn investigative journalism into a criminal enterprise. Foreign laws now determine the limits of press freedom in this country and the journalism that won the industry's most prestigious prizes has been deemed an extraditable offence and worthy of a life sentence. The path to Julian's freedom is long and tortuous. Today is not the end of the fight. It is only the beginning of a new legal battle. We will appeal through the legal system; the next appeal will be before the High Court. We will fight louder and shout harder on the streets, we will organise and we will make Julian's story known to all. Make no mistake, this has always been a political case. Julian published evidence that the country trying to extradite him committed war crimes and covered them up; tortured and rendered; bribed foreign officials; and corrupted judicial inquiries into US wrongdoing. Their revenge is to try to disappear him into the darkest recesses of their prison system for the rest of his life to deter others from holding governments to account. We will not let that happen. Julian's freedom is coupled to all our

freedoms. We will fight to return Julian to his family and to regain freedom of expression for us all”. It seems as if Assange is an enemy of the political class for spilling their secrets. I do not know how Assange's eventual life behind bars fits in with the Umfuld narrative that Assange is a part of the establishment. (via darknetlive.com at https://darknetlive.com/post/uk-retard-approves-assange-extradition/)

Cocaine Vendor Sentenced to Nine Years in Prison

A drug dealer living in Huddersfield was sentenced to prison after pleading guilty to distributing large quantities of drugs through the darkweb. According to a press release by the West Yorkshire Police, the Leeds Crown Court sentenced 41-year-old Simon Barclay to nine years in prison for distributing large quantities of cocaine and heroin through the darkweb. Simon Barclay Barclay was identified following months of investigations into drug trafficking on the darkweb by the Eastern Region Special Operations Unit (ERSOU). After establishing that Barclay was running three darkweb vendor accounts, the ERSOU contacted the Yorkshire and Humber Regional Cyber Crime Unit and Kirklees Police, who launched a joint investigation. During the investigations, investigators allegedly saw Barclay make regular drop-offs of packages to a post office close to his residence. On November 3, 2021, the investigators stopped Barclay on his way to the post office. He was carrying a bag that had several drug packages addressed to different people. The investigators subsequently searched two properties linked to the defendant. The searches resulted in the seizure of cocaine and heroin worth Â£1.2 million. The investigators also seized several electronic devices. Forensic analysis of the seized electronic devices led to the seizure of cryptocurrency worth approximately Â£5.5 million. Barclay pleaded guilty to possession of Class A and B and possession of cryptocurrency linked to a crime. Det Insp Simon Reddington of the Kirklees Police Programme Precision Team: "Barclay has clearly been a significant player in the possession and sale of Class A drugs in Kirklees and nationally this has been reflected in the sentence he has been given today. He was caught as a result of detailed collaborative working between Kirklees Police and partner agencies operating as part of UK DICE. Barclay's use of the dark web proved to be the key to opening the door to his drugs network and this operation truly demonstrates the effectiveness of information sharing between the police and our national and regional partners.” Kirklees Dark Web Criminal Jailed After Â£1-Million Drugs Haul Seized. | archive.is, archive.org, westyorkshire.police.uk (via darknetlive.com at https://darknetlive.com/post/bix-nood-darkweb-vendor-sentenced-to-prison/)

EncroChat: Drug Dealer Sentenced to 14 Years in Prison

A drug dealer who the police identified through EncroChat was sentenced to 14 years in prison at Liverpool Crown Court. Martin Peter Grant, 33, was sentenced to 14 years and six months in prison at Liverpool Crown Court. Grant previously pleaded guilty to conspiracy to supply Class A drugs (heroin and cocaine) and to conspiracy to supply Class B drugs (cannabis and ketamine). Martin Peter Grant and Liam Grant Last month, a court sentenced Grant's younger brother Liam Grant, 25, to four years and six months in prison after he had pleaded guilty to the same charges. According to an announcement from the Merseyside Police, the arrests are a part of Operation Venetic. Police described the operation as "an international operation targeting criminals who used a mobile encryption service, commonly referred to as EncroChat, in an attempt to evade detection.” Police included pictures of drugs in the announcement. Unsure if the pictures are seized products or pictures sent via EncroChat. "Martin led the family enterprise, which involved them both using the dark web in an attempt to conceal their underworld drug dealing. He used the handle Swiftorchid, while younger brother Liam went by the name Beigepalm.” From the article about the arrest of the darkweb MDMA vendor "HundredsUK”: "EncroChat called itself "an end-to-end security solution” that provided customized Android handsets as well as an OTR messaging application. EncroChat usually sold Samsung phones with a modified version of Android. Some units had no functioning GPS, camera, or microphone. The phones came pre-installed with the EncroChat application as well as other applications provided by the company. EncroChat, the application, "routed conversations through a central server based in France.” The service had roughly 60,000 users at the time of its closure.” Merseyside Police have had a lot of Operation Venetic cases lately. "The French National Gendarmerie, assisted by law enforcement in the Netherlands,

installed malware on EncroChat servers in France. "The malware allowed them to read messages before they were sent and record lock screen passwords,” according to a Wikipedia entry on the company. The malware affected more than half the devices in Europe, according to the company. Law enforcement agencies worldwide received access to the data pulled from the hacked EncroChat server.” Merseyside Police detectives identified the brothers by examining "a series of messages and photographs” shared through EncroChat. In one example provided by the police, the brothers discussed ways to travel unmolested by law enforcement during lockdowns. One of the brothers shared a screenshot of an eBay listing for an ambulance and wrote, "buy a ambulance jacket of eBay‚ never get pulled.”

Would have been a lot cooler if the brothers went through with the amber lamps idea! Detective Sergeant Graeme Kehoe: "The fact the Grant brothers pleaded guilty again illustrates the strength of evidence that we have to bring drug dealers who used Encrochat to justice, and prevent them from flooding the streets with drugs. Op Venetic is continuing to expose criminals who thought they could evade detection by using the encrypted devices.” "Bringing the Grant brothers to justice has disrupted not only the serious organised crime they were involved in, but street level drug deals and county lines operations involving vulnerable young people. I hope this sends a clear message to criminals that we'll persist in our pursuit to get them behind bars.” Op Venetic: Liverpool brothers locked up for class A and B drug dealing | merseyside.police.uk (via darknetlive.com at https://darknetlive.com/post/op-venetic-two-brothers-jailed-for-14-years/)

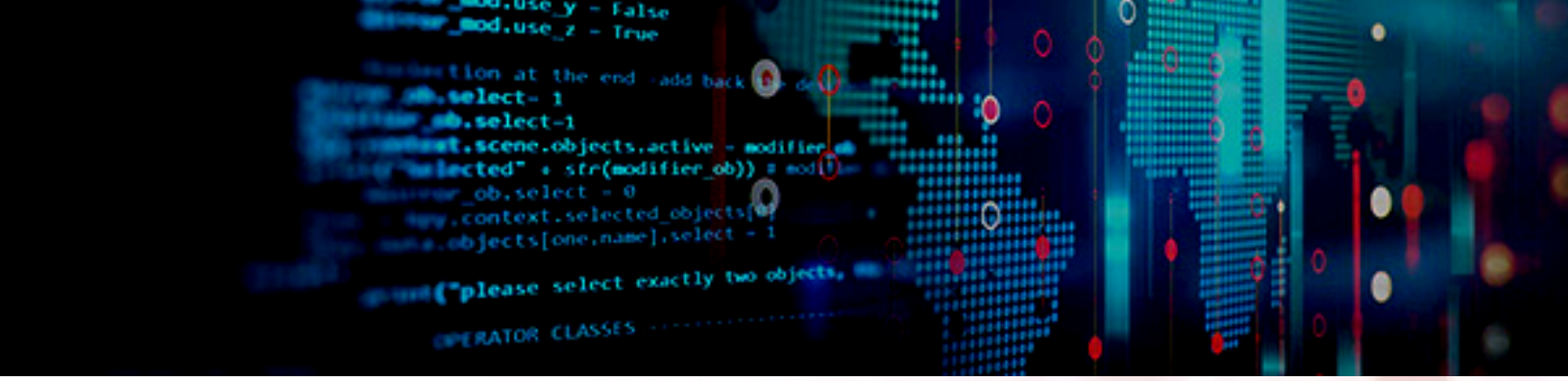
Four Charged for Shipping Kilos of Fentanyl Pills Across the US

A federal grand jury returned a four-count indictment accusing four alleged drug dealers of shipping kilograms of fentanyl pills across the United States. The indictment charges Derrean Wall, Cortez West, Dayareon Crofton, and Floyd Head with conspiracy to possess with intent to distribute a controlled substance. Wall faces three additional counts of possession with intent to distribute a controlled substance. In January 2022, postal inspectors seized a suspicious package en route to Cleveland, Ohio. Later, investigators learned the package contained 2.2 kilograms of fentanyl pills. During the investigation that followed the package seizure, police allegedly identified Crofton, Head, and West as the senders of the package. Over the next three months, police arrested Crofton, Head, and West. Police seized approximately two kilograms of fentanyl pills from each defendant. On April 27, 2022, police executed search warrants at two locations in Ohio. During the execution of the search warrants, officers encountered and arrested Wall, the intended recipient of the intercepted package. Police found "large quantities” of fentanyl pills, heroin, and methamphetamine during the searches.

In the U.S., these charges carry a mandatory minimum sentence of ten years in prison. Fentanyl has been responsible for the majority of fatal overdoses since 2016. According to the NIDA, the number of fatal drug overdoses have increased every year since 1999 with the exception of 2018. The chart below is from the National Institute on Drug Abuse. It appears as if the number of overdoses increased once again in 2021. And 70% of all fatal opioid overdoses occur in males.

Men account for 69% of all fatal drug overdoses. 70% of all opioid overdoses. Four Charged with Trafficking Fentanyl Pills from Southwestern U.S. to Cleveland | archive.is, archive.org, justice.gov. (via darknetlive.com at https://darknetlive.com/post/four-charged-for-shipping-kilos-of-fentanyl-pills/)

Dark Web Link



Trend Micro Anti-Malware Blog

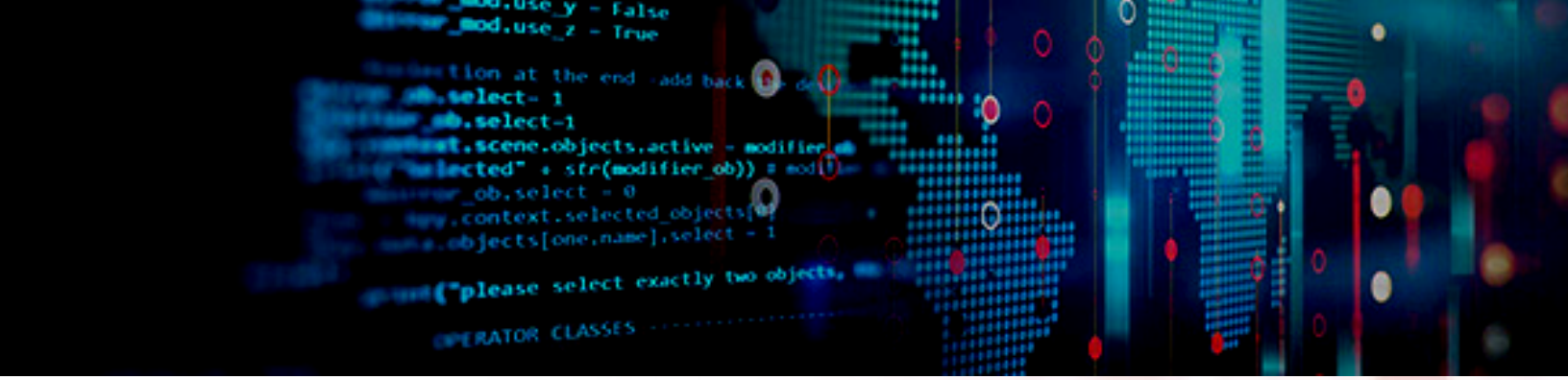
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

Unfortunately, at the time of this report, the RiskIQ resource was not availible.

FireEye

* Metasploit Weekly Wrap-Up
* 4 Strategies to Help Your Cybersecurity Budget Work Harder
* CVE-2022-27511: Citrix ADM Remote Device Takeover
* Security Is Shifting in a Cloud-Native World: Insights From RSAC 2022
* New Report Shows What Data Is Most at Risk to (and Prized by) Ransomware Attackers
* Complimentary GartnerⓇ Report "How to Respond to the 2022 Cyberthreat Landscape": Ransomware Ed
* Patch Tuesday - June 2022
* CVE-2022-32230: Windows SMB Denial-of-Service Vulnerability (FIXED)
* Defending Against Tomorrow's Threats: Insights From RSAC 2022
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Requests Public Comment on CISA's TIC 3.0 Cloud Use Case
* Cisco Releases Security Updates for Multiple Products
* Adobe Releases Security Updates for Multiple Products
* SAP Releases June 2022 Security Updates
* CISA Adds One Known Exploited Vulnerability to Catalog
* Citrix Releases Security Updates for Application Delivery Management
* Microsoft Releases June 2022 Security Updates
* Drupal Releases Security Updates
* AA22-158A: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devi
* AA22-152A: Karakurt Data Extortion Group
* Vulnerability Summary for the Week of June 6, 2022
* Vulnerability Summary for the Week of May 30, 2022

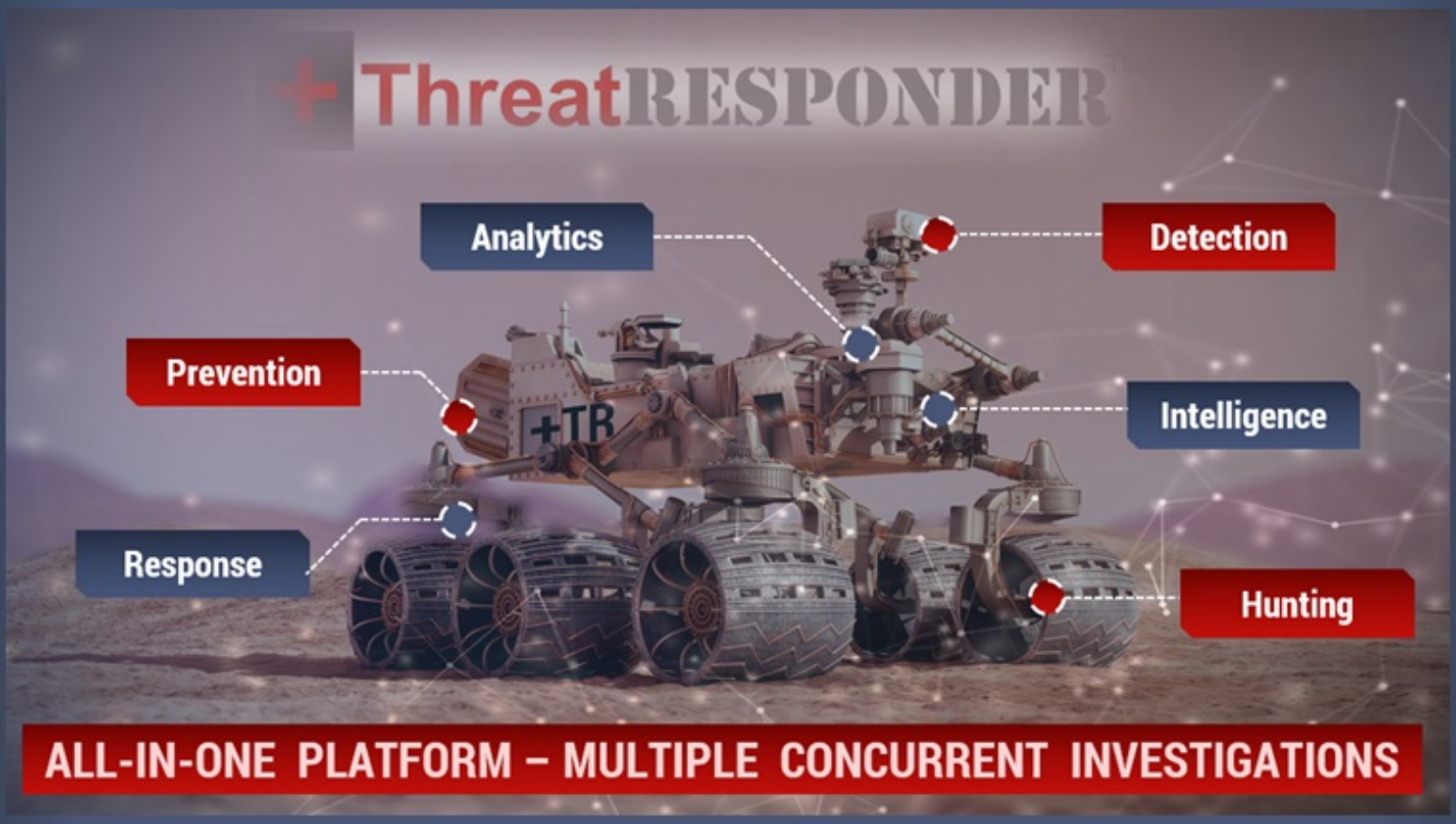
Zero Day Initiative Advisories

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



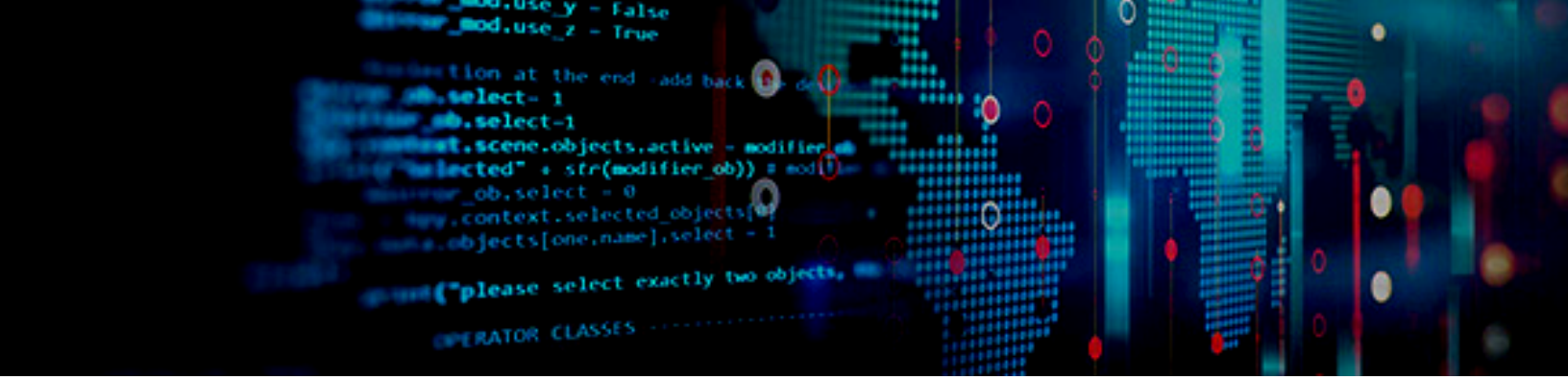
The Solution – ThreatResponder® Platform

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

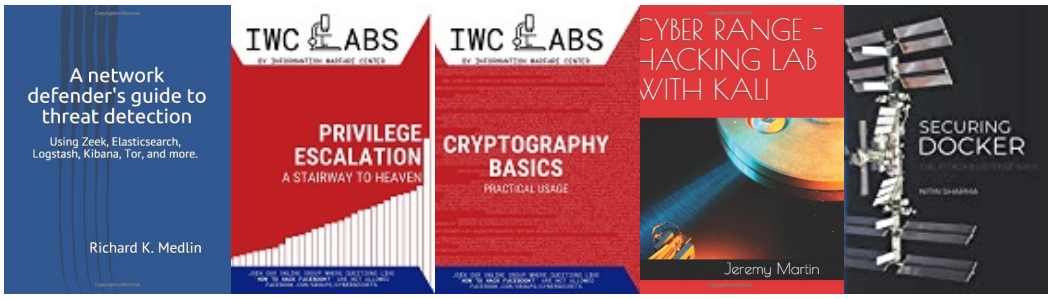


The Cyber Secrets publications on Amazon

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