Jun-27-22

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 27, 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

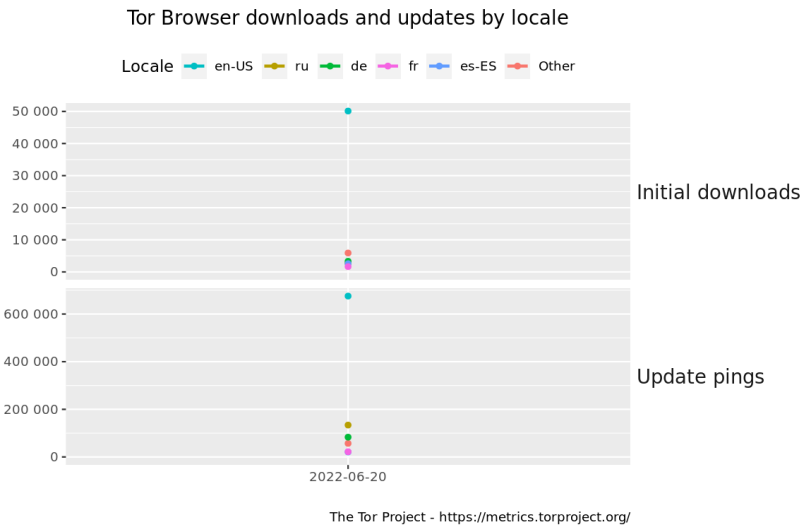
Internet Storm Center Infocon Status

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

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:
* Security Conferences
* Google Zero Day Project

Cyber Range Content
* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques
* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week
* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified
* CyberCrime-Tracker

Advisories
* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products
* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

Packet Storm Security

* Russia's Killnet Hacker Group Says It Attacked Lithuania
* Contractor Loses Entire Japanese City's Personal Data In USB Fail
* Beijing Probes Security At Academic Journal Database
* UK Security Services Must Seek Approval To Access Telecoms Data, Judge Rules
* NSO Claims More Than 5 EU States Use Pegasus Spyware
* Beijing-Backed Attackers Use Ransomware As Decoy While They Conduct Espionage
* Google Warns Spyware Being Deployed Against Android, iOS
* Microsoft Compares Russian Hacks Of Ukraine To Assassination That Started World War I
* Fancy Bear Uses Nuke Threat Lure To Exploit 1-Click Bug
* CISA Warns Over Software Flaws In Industrial Control Systems
* Questions Over Cyber Command Support, Operations Raised In Defense Authorization Bill
* NSA, CISA Say: Don't Block PowerShell, Here's What To Do Instead
* Yodel Becomes Latest Victim Of A Cyber Incident
* Elusive ToddyCat APT Targets Microsoft Exchange Servers
* Mega Says It Can't Decrypt Your Files. New POC Exploit Shows Different
* Apple's iOS 16 Will Give You An Alternative To Irritating CAPTCHAs
* 1.5 Million Customers Impacted By Flagstar Bank Data Breach
* Hidden Anti-Cryptography Provisions In Internet Anti-Trust Bills
* Hartzbleed: A New Side-Channel Attack
* Office 365 Config Loophole Opens OneDrive, SharePoint Data To Ransomware Attack
* How Refactoring Code In Safari's WebKit Resurrected Zombie Security Bug
* There Are 24.6 Billion Sets Of Credentials Up For Sale On The Dark Web
* This Phone-Wiping Android Banking Trojan Is Getting Nastier
* Capital One: Convicted Techie Got In Via Misconfigured AWS Buckets
* International Operation Takes Down Russian RSOCKS Botnet

Krebs on Security

* Meet the Administrators of the RSOCKS Proxy Botnet
* Why Paper Receipts are Money at the Drive-Thru
* 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

Dark Reading

* Thrive Acquires DSM
* It's a Race to Secure the Software Supply Chain - Have You Already Stumbled?
* Threat Intelligence Services Are Universally Valued by IT Staff
* Why We're Getting Vulnerability Management Wrong
* APT Groups Swarming on VMware Servers with Log4Shell
* Only 3% of Open Source Software Bugs Are Actually Attackable, Researchers Say
* 7 Steps to Stronger SaaS Security
* The Cybersecurity Talent Shortage Is a Myth
* Without Conti on the Scene, LockBit 2.0 Leads Ransomware Attacks
* Chinese APT Group Likely Using Ransomware Attacks as Cover for IP Theft
* Johnson Controls Acquires Tempered Networks to Bring Zero Trust Cybersecurity to Connected Buildings
* ShiftLeft: Focus On 'Attackability' To Better Prioritize Vulnerabilities
* Pair of Brand-New Cybersecurity Bills Become Law
* The Rise, Fall, and Rebirth of the Presumption of Compromise
* Reinventing How Farming Equipment Is Remotely Controlled and Tracked
* Cyberattackers Abuse QuickBooks Cloud Service in 'Double-Spear' Campaign
* Palo Alto Networks Bolsters Its Cloud Native Security Offerings With Out-of-Band WAAS
* How APTs Are Achieving Persistence Through IoT, OT, and Network Devices
* 80% of Legacy MSSP Users Planning MDR Upgrade
* MetaMask Crypto-Wallet Theft Skates Past Microsoft 365 Security

The Hacker News

* Cybersecurity Experts Warn of Emerging Threat of "Black Basta" Ransomware
* Critical Security Flaws Identified in CODESYS ICS Automation Software
* What Are Shadow IDs, and How Are They Crucial in 2022?
* Italy Data Protection Authority Warns Websites Against Use of Google Analytics
* Researchers Warn of 'Matanbuchus' Malware Campaign Dropping Cobalt Strike Beacons
* Learn NIST Inside Out With 21 Hours of Training @ 86% OFF
* Hackers Exploit Mitel VoIP Zero-Day in Likely Ransomware Attack
* Google Says ISPs Helped Attackers Infect Targeted Smartphones with Hermit Spyware
* Multiple Backdoored Python Libraries Caught Stealing AWS Secrets and Keys
* State-Backed Hackers Using Ransomware as a Decoy for Cyber Espionage Attacks
* New 'Quantum' Builder Lets Attackers Easily Create Malicious Windows Shortcuts
* Log4Shell Still Being Exploited to Hack VMWare Servers to Exfiltrate Sensitive Data
* NSO Confirms Pegasus Spyware Used by at least 5 European Countries
* Manual vs. SSPM: Research on What Streamlines SaaS Security Detection & Remediation
* Chinese Hackers Distributing SMS Bomber Tool with Malware Hidden Inside

Security Week

* NIST Releases New macOS Security Guidance for Organizations
* House Passes ICS Cybersecurity Training Bill
* Cerby Emerges From Stealth With Security Platform for Unmanageable Apps
* FTC Takes Action Against CafePress Over Massive Data Breach, Cover-Up
* Netsec Goggle Customizes Brave Search Results to Show Only Cybersecurity Websites
* Cyberattack Forces Iran Steel Company to Halt Production
* Researchers: Oracle Took 6 Months to Patch 'Mega' Vulnerability Affecting Many Systems
* CrowdStrike: Ransomware Actor Caught Exploiting Mitel VOIP Zero-Day
* Black Basta Ransomware Becomes Major Threat in Two Months
* Hadrian Raises $11 Million for Offensive Security Platform
* Codesys Patches 11 Flaws Likely Affecting Controllers From Several ICS Vendors
* US Agencies Warn Organizations of Log4Shell Attacks Against VMware Products
* US, UK, New Zealand Issue PowerShell Security Guidance
* Apple, Android Phones Targeted by Italian Spyware: Google
* A Year After Death, McAfee's Corpse Still in Spanish Morgue
* Biden Signs Two Cybersecurity Bills Into Law
* Security Orchestration: Beware of the Hidden Financial Costs
* Top Cryptographers Flag 'Devastating' Flaws in MEGA Cloud Storage
* Chinese APT 'Bronze Starlight' Uses Ransomware to Disguise Cyberespionage
* ICS Vendors Respond to OT:Icefall Vulnerabilities Impacting Critical Infrastructure
* Johnson Controls Acquires Tempered Networks to Shield Buildings From Cyberattacks
* MCG Health Faces Lawsuit Over Data Breach Impacting 1.1 Million Individuals
* US Subsidiary of Automotive Hose Maker Nichirin Hit by Ransomware
* Firmware Security Startup Binarly Raises $3.6 Million in Seed Funding
* Microsoft: Russian Cyber Spying Targets 42 Ukraine Allies
* SMA Technologies Patches Critical Security Issue in Workload Automation Solution

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* MetaMask Crypto Wallet Phishing
* Amazon Prime Day 2022 is Coming: Here are Quick Cybersecurity Tips to Help You Stay Safe
* Technology, Microlearning, and its Impact on Users and Cybersecurity
* Pre-Hijacking of Online Accounts are the Latest Method for Attackers to Impersonate and Target
* "Failure to Authenticate" Wire Transaction at the Heart of a Cyber Insurance Appeal Case
* Phishing Scammers Leverage Telegraph's Loose Governance to Host Crypto and Credential Scams
* Vendor Impersonation Competing with CEO Fraud
* [Heads Up] Russia has increased the cyber attacks against countries that help Ukraine
* Spear Phishing Campaign Targets the US Military
* FBI Warns of Fraudsters on LinkedIn

ISC2.org Blog

* Infosecurity Europe: A show so secure a train strike couldn't break it!
* Unconscious Bias: How to Understand, Identify and Manage It
* SECURE North America | Users Aren't the Weakest Link, They're Your Allies
* How can your organization find and develop the next generation of cybersecurity?
* SECURE North America | Apple Stories: How Technology Has Mediated Technology Through History

HackRead

* Scammer Who Used Info of Riot Games' Co-Founder to Mine Crypto is Jailed
* Hackers Exploit Harmony's Horizon Blockchain Bridge to Steal $100 Million
* Prepare for Your Salesforce Certified OmniStudio-Developer Exam
* ISPs Helping Attackers Install Hermit Spyware on Smartphones- Google
* Chinese Hackers Distributing Nim language Malware in SMS Bomber Tool
* Flaws in Smart Jacuzzi App Could Be Exploited To Extract Users' Data
* 5 Tips for Protecting Your Phone from Malware

Koddos

* Scammer Who Used Info of Riot Games' Co-Founder to Mine Crypto is Jailed
* Hackers Exploit Harmony's Horizon Blockchain Bridge to Steal $100 Million
* Prepare for Your Salesforce Certified OmniStudio-Developer Exam
* ISPs Helping Attackers Install Hermit Spyware on Smartphones- Google
* Chinese Hackers Distributing Nim language Malware in SMS Bomber Tool
* Flaws in Smart Jacuzzi App Could Be Exploited To Extract Users' Data
* 5 Tips for Protecting Your Phone from Malware

Naked Security

* FTC warns of LGBTQ+ extortion scams - be aware before you share!
* OpenSSL issues a bugfix for the previous bugfix
* S3 Ep88: Phone scammers, hacking bust, and data breach fines [Podcast + Transcript]
* Capital One identity theft hacker finally gets convicted
* Interpol busts 2000 suspects in phone scamming takedown
* 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]

Threat Post

* Google Warns Spyware Being Deployed Against Android, iOS Users
* Fancy Bear Uses Nuke Threat Lure to Exploit 1-Click Bug
* Gamification of Ethical Hacking and Hacking Esports
* Discovery of 56 OT Device Flaws Blamed on Lackluster Security Culture
* Elusive ToddyCat APT Targets Microsoft Exchange Servers
* Kazakh Govt. Used Spyware Against Protesters
* Office 365 Config Loophole Opens OneDrive, SharePoint Data to Ransomware Attack
* Voicemail Scam Steals Microsoft Credentials
* China-linked APT Flew Under Radar for Decade
* State-Sponsored Phishing Attack Targeted Israeli Military Officials

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

* Security survives the budget axe
* 7 devops practices to improve application performance
* 8 Java frameworks for a cloud-native world
* Apache Doris just 'graduated': Why care about this SQL data warehouse
* Making application modernization pragmatic and useful
* What is NoSQL? Databases for a cloud-scale future
* Rust is most popular WebAssembly language, survey says
* IaaS, PaaS, drive public cloud ecosystem revenue to $126 billion in Q1
* TypeScript 4.8 fixes file watching on Linux, macOS
* How to work with trace listeners in ASP.NET Core 6

C4ISRNET - Media for the Intelligence Age Military

* Kennedy confirmed as Air Force cyber boss
* South Korea develops robot for autonomous tunnel exploration
* US Air Force mints program to hone command and control
* US must prepare for proliferation of cyber warfare
* What the Cyber Workforce bill means for federal IT professionals
* US Air Force seeks tech sweet spot for Advanced Battle Management System
* Parsons' chief executive talks acquisitions, Ukraine and the defense budget
* Battlefield robots getting 'common sense' training before deployment
* How the cloud saved Ukraine's data from Russian attacks
* Viasat to test 5G networking for Marine Corps operations

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

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.

* Codeguru eXtreme
* US Cyber Open CTF: Season II
* Google Capture The Flag 2022
* Hacky Holidays - Unlock the City
* FAUST CTF 2022
* vsCTF 2022
* HTB Business CTF 2022: Dirty Money
* Crypto CTF 2022
* ImaginaryCTF 2022
* UACTF 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

* OpenSSL Toolkit 1.1.1p
* Wireshark Analyzer 3.6.6
* TOR Virtual Network Tunneling Tool 0.4.7.8
* Zeek 4.2.2
* Falco 0.32.0
* GRR 3.4.6.0
* I2P 1.8.0
* Deliverance 0.018-daf9452 File Descriptor Fuzzer
* TP-Link Backup Decryption Utility
* Lynis Auditing Tool 3.0.8

Kali Linux Tutorials

* PowerProxy : PowerShell SOCKS Proxy With Reverse Proxy Capabilities
* Cyph : Cryptographically Secure Messaging And Social Networking Service
* ShadowClone : Unleash The Power Of Cloud
* Vaas Verdict-as-a-Service SDKs: Analyze Files For Malicious Content
* BirDuster : A Multi Threaded Python Script Designed To Brute Force Directories
* DuplicateDump : Dumping LSASS With A Duplicated Handle From Custom LSA Plugin
* Chlonium : Chromium Cookie Import / Export Tool
* NodeSecurityShield : A Developer And Security Engineer Friendly Package For Securing NodeJS Applicati
* BWASP : BoB Web Application Security Project
* RogueAssemblyHunter : Rogue Assembly Hunter Is A Utility For Discovering 'Interesting' .NET CLR Modul

GBHackers Analysis

* Critical PHP Flaws Allows Attackers to Execute Remote Code on QNAP NAS Devices
* Critical Flaws in MEGA Cloud Storage Let Attacker Decrypt User Data
* A 5-Year-Old Bug in Apple Safari Exploited in the Wild - Google Project Zero
* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3
* Pwn2Own - Windows 11, Microsoft Teams Hacked & Exploiting 16 Zero-day Bugs

Weekly Cyber Security Video and Podcasts

SANS DFIR

* FOR509: Cloud Forensics & Incident Response Course - What to Expect
* Learning to Combat Ransomware
* Learning to Combat Ransomware
* Prevent, Detect, Respond An Intro to Google Workspace Security and Incident Response

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

* Create Your First O.MG Payload ft. MG
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Another Record Breaking DDoS Attack; Stealing Crypto Keys from AMD and Intel CPUs - ThreatWire

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* What is a Subnet Mask
* eBeggar Wednesday - BITCOIN FAILING
* What is TCP/IP Version 4
* How Does Computer Discovery and Communication Work

Security Now

* Microsoft's Patchy Patches - 3rd Party Authenticators, MS-DFSNM, Safari Regression, Firefox Cookies
* The PACMAN Attack - WebAuthn, Passkeys at WWDC, Free Kali Linux Pen Test Course, Proof of Simulation

Troy Hunt

* Weekly Update 301

Intel Techniques: The Privacy, Security, & OSINT Show

* 267-macOS Privacy & Security Revisited

* 266-The Sole Proprietorship

Proof of Concept (PoC) & Exploits

Packet Storm Security

* WordPress Simple Page Transition 1.4.1 Cross Site Scripting
* Mailhog 1.0.1 Cross Site Scripting
* WordPress W-DALIL 2.0 Cross Site Scripting
* WordPress Weblizar 8.9 Code Execution
* Coffee Shop Cashiering System 1.0 SQL Injection
* Library Management System With QR Code 1.0 SQL Injection
* Library Management System With QR Code 1.0 Cross Site Scripting
* Library Management System With QR Code 1.0 Shell Upload
* WSO2 Management Console Cross Site Scripting
* Backdoor.Win32.InfecDoor.17.c MVID-2022-0614 Insecure Permissions
* Trojan-Mailfinder.Win32.VB.p MVID-2022-0616 Insecure Permissions
* Backdoor.Win32.Shark.btu MVID-2022-0615 Insecure Permissions
* Yashma Ransomware Builder 1.2 MVID-2022-0613 Insecure Permissions
* WordPress Download Manager 3.2.43 Cross Site Scripting
* Zoo Management System 1.0 Cross Site Scripting
* SAP FRUN Simple Diagnostics Agent 1.0 Directory Traversal
* SAP Fiori Launchpad Cross Site Scripting
* SAP FRUN Simple Diagnostics Agent 1.0 Missing Authentication
* SAP FRUN 2.00 / 3.00 Cross Site Scripting
* SIEMENS-SINEMA Remote Connect 3.0.1.0-01.01.00.02 Cross Site Scripting
* Nexans FTTO GigaSwitch Outdated Components / Hardcoded Backdoor
* Lepin EP-KP001 KP001_V19 Authentication Bypass
* Mitel 6800/6900 Series SIP Phones Backdoor Access
* SoftGuard SNMP Network Management Extension HTML Injection / File Download
* Gentics CMS 5.36.29 Cross Site Scripting / Deserialization

CXSecurity

* Kitty 0.76.0.8 Stack Buffer Overflow
* phpIPAM 1.4.5 Remote Code Execution
* Pandora FMS 7.0NG.742 Remote Code Execution
* 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)

Proof of Concept (PoC) & Exploits

Exploit Database

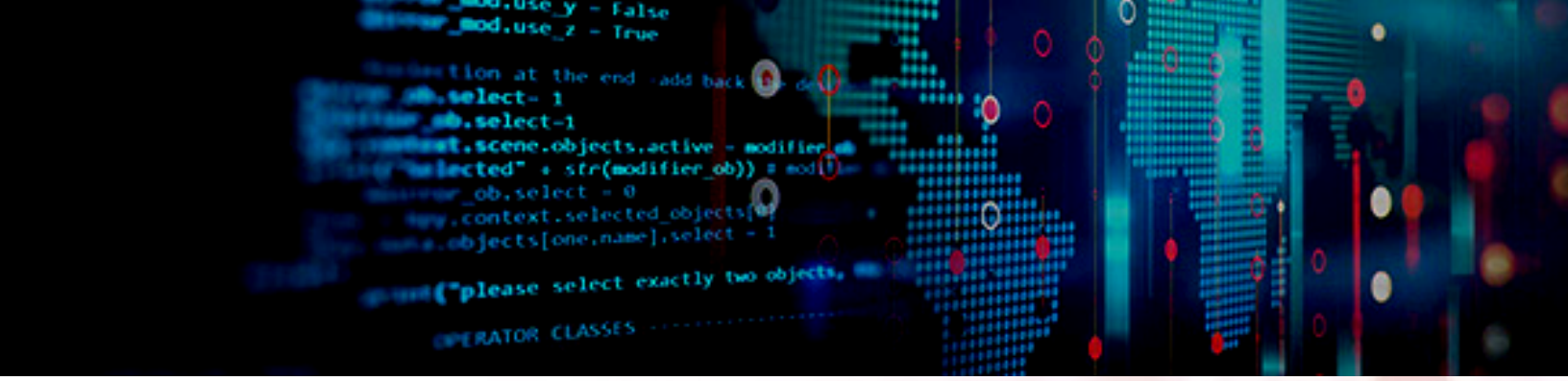
* [webapps] SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)
* [webapps] SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)
* [webapps] Old Age Home Management System 1.0 - SQLi Authentication Bypass
* [webapps] ChurchCRM 4.4.5 - SQLi
* [remote] Sourcegraph Gitserver 3.36.3 - Remote 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*

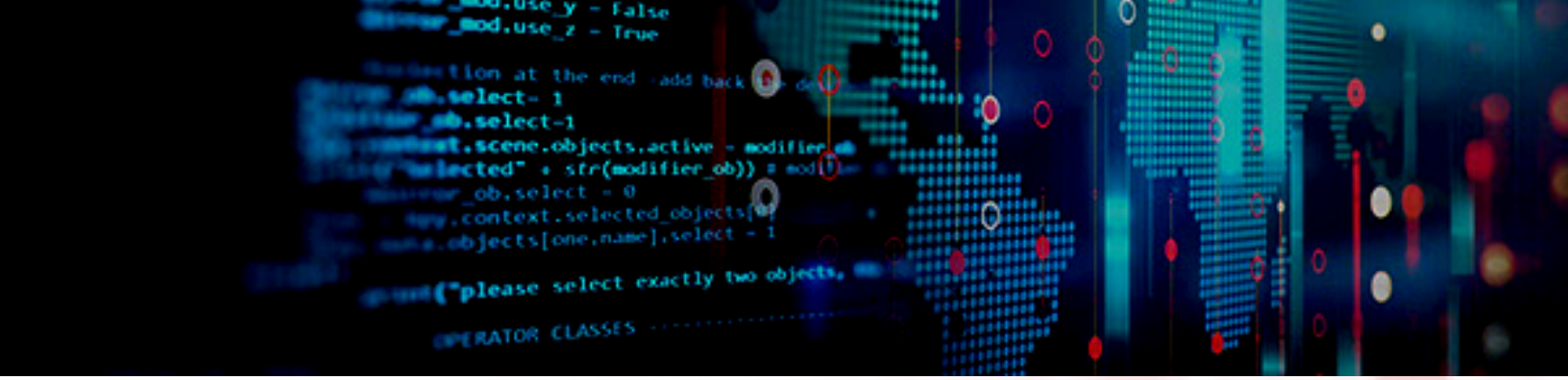
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://acehtamiangkab.go.id/readme.php
https://acehtamiangkab.go.id/readme.php notified by AnonSec Team
http://siechd.nic.in
http://siechd.nic.in notified by Hunter Gujjar
http://quran.gov.bh/1877.html
http://quran.gov.bh/1877.html notified by CodeBoy1877
http://comingo.gov.vn
http://comingo.gov.vn notified by CodeBoy1877
https://cs.pmo.gov.ps/1877.html
https://cs.pmo.gov.ps/1877.html notified by CodeBoy1877
http://uyd.yb.gov.ng/xxx.txt
http://uyd.yb.gov.ng/xxx.txt notified by Imam
http://fpis.gov.ng/xxx.txt
http://fpis.gov.ng/xxx.txt notified by Imam
http://kel-sawahgede.cianjurkab.go.id
http://kel-sawahgede.cianjurkab.go.id notified by CodeBoy1877
http://banyuwangipekon.pringsewukab.go.id
http://banyuwangipekon.pringsewukab.go.id notified by CodeBoy1877
http://cmchacao.gob.ve/kz.html
http://cmchacao.gob.ve/kz.html notified by Mr.Kro0oz.305
http://xnzoms.barishalcity.gov.bd/adritod.txt
http://xnzoms.barishalcity.gov.bd/adritod.txt notified by ./unn0rmaL
https://bid.barishalcity.gov.bd/adritod.txt
https://bid.barishalcity.gov.bd/adritod.txt notified by ./unn0rmaL
https://birth.barishalcity.gov.bd/adritod.txt
https://birth.barishalcity.gov.bd/adritod.txt notified by ./unn0rmaL
http://terminalmanta.gob.ec/cl.html
http://terminalmanta.gob.ec/cl.html notified by Clash Hackers
https://iraqnla.gov.iq/v3n.html
https://iraqnla.gov.iq/v3n.html notified by v3n0m
https://aporo.gob.mx/Freak.html
https://aporo.gob.mx/Freak.html notified by T-Freak
http://urdu.fbr.gov.pk/Moroccohack.html
http://urdu.fbr.gov.pk/Moroccohack.html notified by Moroccan Revolution



Dark Web News

Darknet Live

Dealer Who Identified Himself on EncroChat Sentenced to Prison

An EncroChat-using drug dealer was sentenced to 25 years in prison for selling Class A and Class B drugs. During a hearing at Liverpool Crown Court, John Digweed, 33, of Harlech Road, Crosby, was sentenced to prison for 25 years for drug distribution and money laundering. John Digweed in his mugshot. A jury convicted Digweed of conspiring to supply Class A drugs, including heroin, cocaine, ecstasy powder, and 2CB, and Class B drugs cannabis, ketamine, and amphetamine. The jury also convicted him of money laundering. During the trial, prosecutors showed the jury evidence of Digweed's involvement in the supply of 12.5kg of heroin, 30-35kg of cocaine, 80kg of cannabis, 4kg of ketamine, and 3kg of amphetamine. Merseyside Police arrested Digweed in March 2021 as a part of Operation Venetic. Operation Venetic was "an international operation targeting criminals who used a mobile encryption service, commonly referred to as EncroChat, in an attempt to evade detection when dealing drugs.”

A picture of a block of marijuana sent to Digweed on EncroChat After law enforcement agencies had hacked EncroChat, investigators examined messages sent and received by a drug dealer under the username "Diorpaw.” Investigators said Digweed identified himself in his messages to other EncroChat users. In one example provided by police, one of Digweed's contacts sent him a picture of a block of marijuana labeled "Johnny Weed.” Digweed responded, "HaHaHaHa lad who's done that, its only missing dig out the name” My names Johnny Digweed init.” Digweed then sent the image to other EncroChat users. "His messages on the dark web revealed that he supplied drugs across the northwest and managed the supply of crack cocaine and heroin to Devon and Cornwall,” police said. Digweed referenced Cornwall, Bristol, Middlesbrough, London, Weston-Super-Mare, and Wales in other messages. Superintendent Graeme Robson: "Digweed's covert messages via EncroChat revealed his clear involvement as a leading figure in drug conspiracies that could have caused immense suffering to families and residents in our community. In one message sent to other handles he brazenly identified himself in messages. The messages he sent also revealed that he operated a sophisticated and organised criminal enterprise.” "We know the destruction that drugs cause and Merseyside Police remains relentless in our pursuit of these criminals and to bring down serious and organised criminal groups. I hope this result shows that Merseyside Police, will leave no stone unturned in our pursuit of these people who think they are above the law, and we will continue to target criminals like Digweed by thoroughly examining any evidence, messages and images we find.” Drug dealer jailed for 25 years after identifying himself on 'Dark Web' | merseyside.police.uk (via darknetlive.com at https://darknetlive.com/post/another-encrochat-drug-dealer-sentenced-to-prison/)

Elliptic: Illicit Use of Dogecoin Increasing

The blockchain analysis firm Elliptic identified Dogecoin as a cryptocurrency increasingly linked to criminal activity, including darknet market usage. Elliptic, which offers blockchain intelligence solutions similar to Chainalysis, published a report identifying an increase in the use of Dogecoin for illicit activity on the internet. The report demonstrates that Dogecoin is rarely used for illegal purposes. According to the company, the meme coin's criminal uses include fraud, scams, ponzi schemes, terrorism financing, malware, transactions on

darkweb markets, and the child sexual abuse material (CSAM) industry. Elliptic also identified so-called "far-right extremism” as one form of the "illicit use of Doge.” __ Theft, scams, and ponzi schemes are the most common illicit activities involving Doge. Terrorism Financing _ The government in Israel seized Dogecoin worth $40,235 from wallets allegedly linked to the Islamic Resistance Movement in July 2021. This is the only example provided by Elliptic. __ Israel seized money from a Palestinian political party. "While a small sum compared to Bitcoin and Tether, this example demonstrates the awareness, and increasing adoption, of a wide variety of cryptoassets by groups such as Hamas. It also reinforces the importance of blockchain analytics solutions in a compliance toolkit to enable financial institutions and law enforcement agencies to screen for risk beyond just the most popular cryptoassets.” Child Sexual Abuse Material _ Elliptic monitors child sexual abuse material (CSAM) vendors on the darknet and clearnet. The majority of cryptocurrency payments to CSAM vendors are in Bitcoin. "A small and growing number of these vendors accept other crypto assets - including Dogecoin,” the report claims. Elliptic explains that there has been $3,000 worth of Doge payments to CSAM vendors to date. __ A screenshot of a CSAM-flagged address in Elliptic Lens. Darkweb Markets _ The report includes two examples of darkweb marketplaces that either accept Doge payments or accepted them in the past. Just-Kill, a "call & email flood service,” allows users to deposit funds using Dogecoin, among other cryptocurrencies. __ Just Kill The report claims that Doge "is accepted "on some popular darknet drug markets.” Archetyp Market is one example of a darkweb drug market that accepts Doge payments. The market "previously used a coin swap service to allow users to deposit funds in a range of other cryptoassets - including Doge.” Archetyp currently only accepts Monero. __ Archetyp Market no longer allows users to conduct transactions with Dogecoin. Another example of "the importance of blockchain analytics solutions” is the now-defunct Doge Road Market. Doge Road existed briefly in 2014 before exit scamming. Malware _ The report highlighted two malware campaigns that involved Dogecoin. Cliptomaner, identified by Kaspersky in October 2020, hijacks a user's clipboard to swap cryptocurrency addresses for addresses controlled by the attackers. Cliptomaner hijacks Doge addresses, among other cryptocurrencies, and has received almost $29,000 in Doge. In July 2020, Intezer identified the "Doki” malware campaign, which used: "a previously undocumented method to contact its operator by abusing the Dogecoin cryptocurrency blockchain in a unique way in order to dynamically generate its C2 domain address. The malware has managed to stay under the radar for over six months despite samples being publicly available in VirusTotal.” "Far-Right Extremism” _ Elliptic laments that when "payments companies such as PayPal, Visa and Mastercard” freeze accounts owned by nominally right-wing people, they "turn instead to cryptocurrencies such as Bitcoin.” By attempting to raise funds without using mainstream payment platforms, these targets of financial censorship have "increasingly exploited the internet,” Elliptic claims. According to the report, the basic CivNat news outlet Infowars ("leftists are the real racists”) is an example of an extremist right-wing group embracing cryptocurrency. To date, Infowars has raised "over $1,700 in Doge alone.” __ Infowars accepts donations in the form of several cryptocurrencies. Thefts, Scams, and Ponzi Schemes _ Elliptic highlighted the hack of the Dogecoin wallet Dogewallet which resulted in the loss of $14,000 in Doge. "Additional notable examples include the Plus Token ponzi scheme, which resulted in the seizure of over $20 million in Doge by Chinese authorities, and an alleged theft of $119 million of Dogecoin connected to a Turkish ponzi scheme in 2021.” The report seems accurate in that Dogecoin use has increased since its launch. I am skeptical that illicit Doge use is worth consideration. When I had a Twitter account, I saw countless scams involving Elon Musk imposters and various cryptocurrencies, including Doge. The total earnings of cryptocurrency scammers on Twitter dwarf the examples of illicit cryptocurrency use provided by Elliptic. For instance, during one weekend in February 2021, scammers earned more than $145,000 in cryptocurrency through fake giveaways on Twitter, including $26,004.94 worth of Doge. Dogecoin Gaining Traction for Illicit use | archive.is, archive.org, hub.elliptic.co (via darknetlive.com at https://darknetlive.com/post/retarded-firm-publishes-dogecoin-hitpiece/)

Fraudster Charged for Using Stolen Credit Card to Buy Jewelry

A man who purchased a diamond necklace with a credit card from the darkweb is facing 15 years in prison. An affidavit filed by a special agent with Homeland Security Investigations accuses Demonn Chadwick Jenkins II, 27, of fraudulent use of credit card information. On June 16, 2022, Jenkins used a Capital One Platinum Mastercard in someone else's name to purchase a diamond necklace for $9990 and a Rolex watch for $10,800 at a jewelry store on Main Street in St. Thomas. __ The red pins are jewelry stores on Main Street, St. Thomas. The next day, Customs and Border Protection (CBP) Officers at the Cyril E. King Airport searched Jenkins' bag and discovered the necklace and watch. According to the affidavit, Jenkins "failed to declare the purchases of the jewelry on his Customs and Border Protection Declaration form.” Jenkins had planned to return to Atlanta, Georgia, on June 17, 2022. "He was later identified as the purchaser of the jewelry using footage taken from the jewelry store's security cameras,” according to a press release from the United States Attorney's Office for the District of Virgin Islands. Based on that information, Jenkins likely told CBP officers that he had not purchased the jewelry in St. Thomas. If he had the jewelry before arriving on the island and did not alter it while on the island, he would not need to pay the Customs Duties for those purchases. __ Jenkins filed for bankrupcy in May 2022 When questioned by CBP officers, "Jenkins admitted that he purchased the Mastercard on the Dark Web for approximately $15.” Assistant U.S. Attorney Adam Sleeper filed a motion to detain Jenkins until his trial because he "has previously been arrested for committing similar crimes.” On June 21, 2022, U.S. Magistrate Ruth Miller released Jenkins to a third-party custodian. If convicted, Jenkins faces 15 years in prison. GEORGIA MAN CHARGED WITH CREDIT CARD FRAUD | archive.is, archive.org, justice.gov (via darknetlive.com at https://darknetlive.com/post/future-doctor-charged-with-credit-card-fraud/)

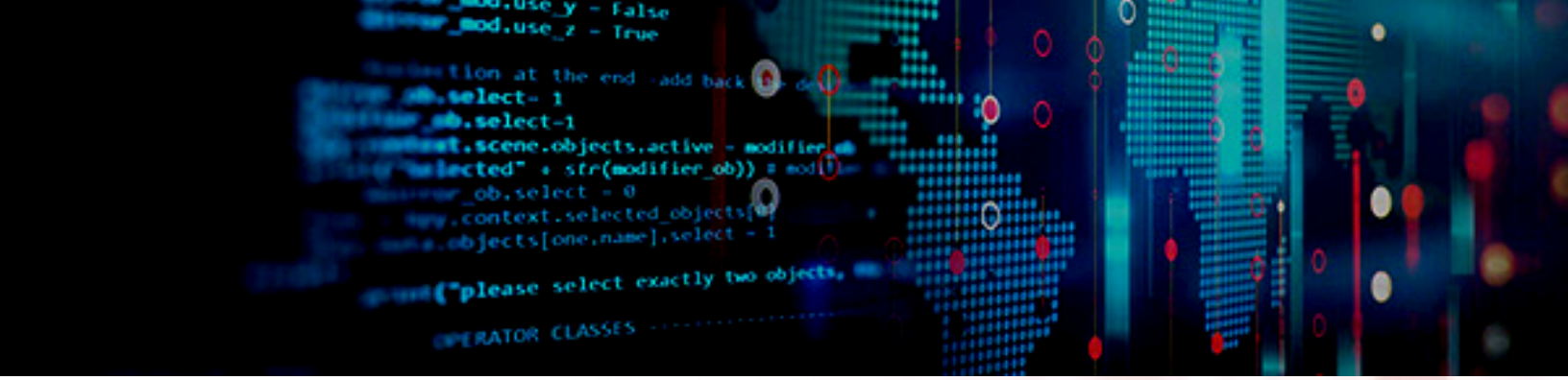
Seven Sentenced in South Wales Drug Trafficking Case

Seven people were sentenced to a total of 54 years in prison for selling drugs and buying firearms on the darkweb. __ Naisha Hembury A press release from the Tarian Regional Organised Crime Unit in Southern Wales highlighted the sentencing of members of an organized crime group. EncroChat? _ Investigators had the evidence they needed to dismantle the group after its "encrypted drug deal chats were cracked.” Although the announcement does not identify the source of the decrypted chats, I suspect they came from EncroChat. Law enforcement agencies in Wales have arrested several so-called "organised crime gangs” operating in Wales, including at least one other case involving illegal firearm deals. __ Max Smith "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.” __ Ryan Hales Firearms and Silencers _ During the investigation into the organized crime group, "detectives uncovered chats on the dark web about purchasing and importing firearms and silencers.” Some of the defendants possessed firearms and ammunition. I suspect the firearms possessed by defendants originated from firearms sellers in the real world; as with murder-for-hire cases, firearm sellers on the darkweb are scammers or feds. __ Marc Harris Police seized Â£4,942,800 worth of Class A & B drugs during the investigation, including 70 kilos of Cocaine, 30 kilos of Heroin, 96 kilos of Amphetamine, and 19 kilos of Cannabis. Sentencing _ One defendant faced drug and firearms charges: Jay Abdul, 39, was sentenced to 19 years and six months for conspiracy to supply Class A & B drugs and possessing a Section 5 prohibited firearm. The remaining defendants faced charges for conspiracy to supply Class A & B drugs: Aysha Ali, 36, was sentenced to four years and six months; Neesha Ali, 40, was sentenced to three years and nine months; Ryan Hales, 28, was sentenced to 11 years and three months; Marc Harris, 31, was sentenced to seven years and four months; Naisha Hembury, 35, was sentenced to 22 months suspended for 18 months; and Max Smith, 25, was sentenced to five years and three months in prison. __ Jay Abdul Tarian Detective Inspector Gareth Grant said: "The safeguarding of our communities will always be our priority. Whilst the seizure of the firearms during this investigation is very disturbing I want to reassure people that guns like this are, thankfully, very unusual here in

south Wales. Such was the weight of evidence against the majority of these defendants that he had no option but to enter guilty pleas. This is down to the hard work and dedication of my investigation team. The success of this investigation demonstrates that we will relentlessly pursue those involved in large scale criminality to ensure effective justice is sought against such individuals and they are brought to justice.”

Aysha Ali and Neesha Ali SEVEN PEOPLE JAILED FOR PART IN DRUG GANG | archive.is, tarianrocu.org.uk (via darknetlive.com at https://darknetlive.com/post/sentences-for-south-wales-drug-gang/)

Dark Web Link



Trend Micro Anti-Malware Blog

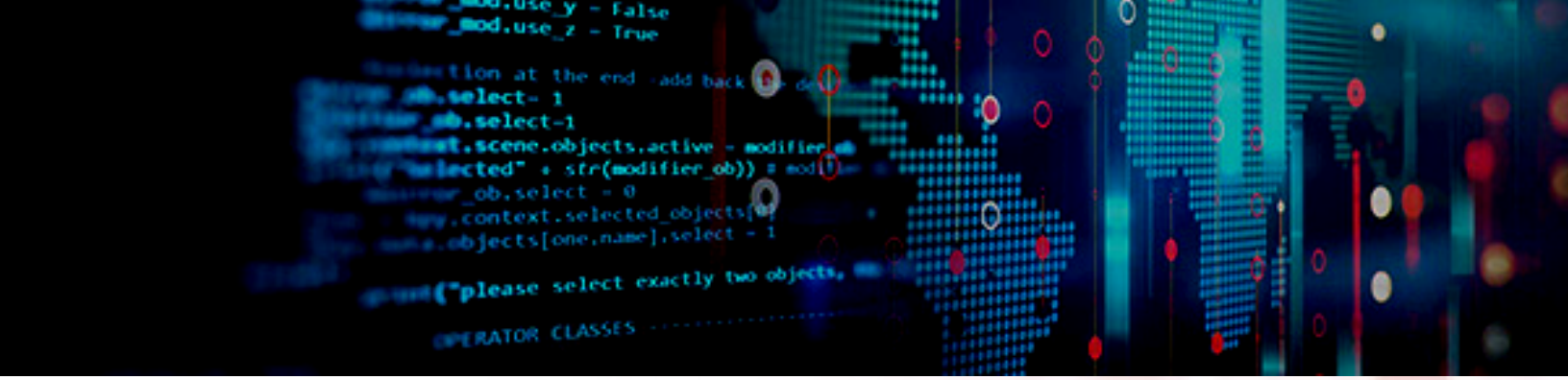
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* API Security: Best Practices for a Changing Attack Surface
* Metasploit Weekly Wrap-Up
* Velociraptor Version 0.6.5: Table Transformations, Multi-Lingual Support, and Better VQL Error-Handli
* CVE-2022-31749: WatchGuard Authenticated Arbitrary File Read/Write (Fixed)
* Two Rapid7 Solutions Take Top Honors at SC Awards Europe
* Rapid7 MDR Delivered 549% ROI via Headcount Avoidance, Time Savings, and Breach Risk Reduction
* [Security Nation] Steve Micallef of SpiderFoot on Open-Source Intelligence
* How to Secure App Development in the Cloud, With Tips From Gartner
* Metasploit Weekly Wrap-Up
* 4 Strategies to Help Your Cybersecurity Budget Work Harder



Advisories

US-Cert Alerts & bulletins

* CISA Adds Eight Known Exploited Vulnerabilities to Catalog
* Citrix Releases Security Updates for Hypervisor
* Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
* CISA Releases Cloud Security Technical Reference Architecture
* Google Releases Security Updates for Chrome
* CISA Releases Security Advisories Related to OT:ICEFALL (Insecure by Design) Report
* Keeping PowerShell: Measures to Use and Embrace
* CISA Requests Public Comment on CISA's TIC 3.0 Cloud Use Case
* AA22-174A: Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
* AA22-158A: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devi
* Vulnerability Summary for the Week of June 13, 2022
* Vulnerability Summary for the Week of June 6, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-5189-01
Red Hat Security Advisory 2022-5189-01 - Updated images are now available for Red Hat Advanced Cluster Security for Kubernetes (RHACS). The updated image includes bug and security fixes.
Ubuntu Security Notice USN-5493-1
Ubuntu Security Notice 5493-1 - It was discovered that the 8 Devices USB2CAN interface implementation in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service.
Red Hat Security Advisory 2022-5187-01
Red Hat Security Advisory 2022-5187-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a cross site scripting vulnerability.
Red Hat Security Advisory 2022-5188-01
Red Hat Security Advisory 2022-5188-01 - Updated images are now available for Red Hat Advanced Cluster Security for Kubernetes (RHACS). The updated image includes bug and security fixes.
Red Hat Security Advisory 2022-5192-01
Red Hat Security Advisory 2022-5192-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a cross site scripting vulnerability.
Ubuntu Security Notice USN-5492-1
Ubuntu Security Notice 5492-1 - It was discovered that Vim incorrectly handled memory when opening and searching the contents of certain files. If an attacker could trick a user into opening a specially crafted file, it could cause Vim to crash.
Ubuntu Security Notice USN-5487-3
Ubuntu Security Notice 5487-3 - USN-5487-1 fixed several vulnerabilities in Apache HTTP Server. Unfortunately it caused regressions. USN-5487-2 reverted the patches that caused the regression in Ubuntu 14.04 ESM for further investigation. This update re-adds the security fixes for Ubuntu 14.04 ESM and fixes two different regressions: one affecting mod_proxy only in Ubuntu 14.04 ESM and another in mod_sed affecting also Ubuntu 16.04 ESM and Ubuntu 18.04 LTS.
Red Hat Security Advisory 2022-5029-01
Red Hat Security Advisory 2022-5029-01 - This release of Red Hat build of Eclipse Vert.x 4.2.7 GA includes security updates. Issues addressed include denial of service and deserialization vulnerabilities.
Ubuntu Security Notice USN-5487-2
Ubuntu Security Notice 5487-2 - USN-5487-1 fixed a vulnerabilities in Apache. Unfortunately, that update introduced a regression when proxying balancer manager connections in some configurations on Ubuntu 14.04 ESM. This update reverts those changes till further fix. It was discovered that Apache HTTP Server mod_proxy_ajp incorrectly handled certain crafted request. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash or expose sensitive information. Multiple other issues were also originally addressed.
Red Hat Security Advisory 2022-5115-01
Red Hat Security Advisory 2022-5115-01 - An update for python-django20 is now available for Red Hat OpenStack Platform 16.2.3 (Train). Issues addressed include a remote SQL injection vulnerability.
Red Hat Security Advisory 2022-5116-01
Red Hat Security Advisory 2022-5116-01 - An update for puppet-firewall is now available for Red Hat OpenStack Platform 16.2.3 (Train). An issue was address where unmanaged rules could leave the system in an unsafe state via duplicate a comment.
Red Hat Security Advisory 2022-5114-01

Red Hat Security Advisory 2022-5114-01 - Barbican is a ReST API designed for the secure storage, provisioning and management of secrets, including in OpenStack environments.

Ubuntu Security Notice USN-5491-1

Ubuntu Security Notice 5491-1 - Joshua Rogers discovered that Squid incorrectly handled the Gopher protocol. A remote attacker could possibly use this issue to cause Squid to crash, resulting in a denial of service.

Red Hat Security Advisory 2022-5162-01

Red Hat Security Advisory 2022-5162-01 - PostgreSQL is an advanced object-relational database management system.

Red Hat Security Advisory 2022-5157-01

Red Hat Security Advisory 2022-5157-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2022-5163-01

Red Hat Security Advisory 2022-5163-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2022-5152-01

Red Hat Security Advisory 2022-5152-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2022-4999-01

Red Hat Security Advisory 2022-4999-01 - 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 3.11.715. Issues addressed include a memory exhaustion vulnerability.

Ubuntu Security Notice USN-5489-1

Ubuntu Security Notice 5489-1 - Alexander Bulekov discovered that QEMU incorrectly handled floppy disk emulation. A privileged attacker inside the guest could use this issue to cause QEMU to crash, resulting in a denial of service, or possibly leak sensitive information. It was discovered that QEMU incorrectly handled NVME controller emulation. An attacker inside the guest could use this issue to cause QEMU to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.04 LTS.

Ubuntu Security Notice USN-5488-1

Ubuntu Security Notice 5488-1 - Chancen and Daniel Fiala discovered that OpenSSL incorrectly handled the c_rehash script. A local attacker could possibly use this issue to execute arbitrary commands when c_rehash is run.

SAP FRUN Simple Diagnostics Agent 1.0 Information Disclosure

SAP Focused Run Simple Diagnostics Agent version 1.0 suffers from an information disclosure vulnerability.

Ubuntu Security Notice USN-5487-1

Ubuntu Security Notice 5487-1 - It was discovered that Apache HTTP Server mod_proxy_ajp incorrectly handled certain crafted request. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a denial of service. It was discovered that Apache HTTP Server incorrectly handled certain request. An attacker could possibly use this issue to cause a crash or expose sensitive information.

Red Hat Security Advisory 2022-5132-01

Red Hat Security Advisory 2022-5132-01 - Updated images are now available for Red Hat Advanced Cluster Security for Kubernetes (RHACS). The updated image includes bug and security fixes.

Ubuntu Security Notice USN-5486-1

Ubuntu Security Notice 5486-1 - It was discovered that some Intel processors did not implement sufficient control flow management. A local attacker could use this to cause a denial of service. Joseph Nuzman discovered that some Intel processors did not properly initialise shared resources. A local attacker could use

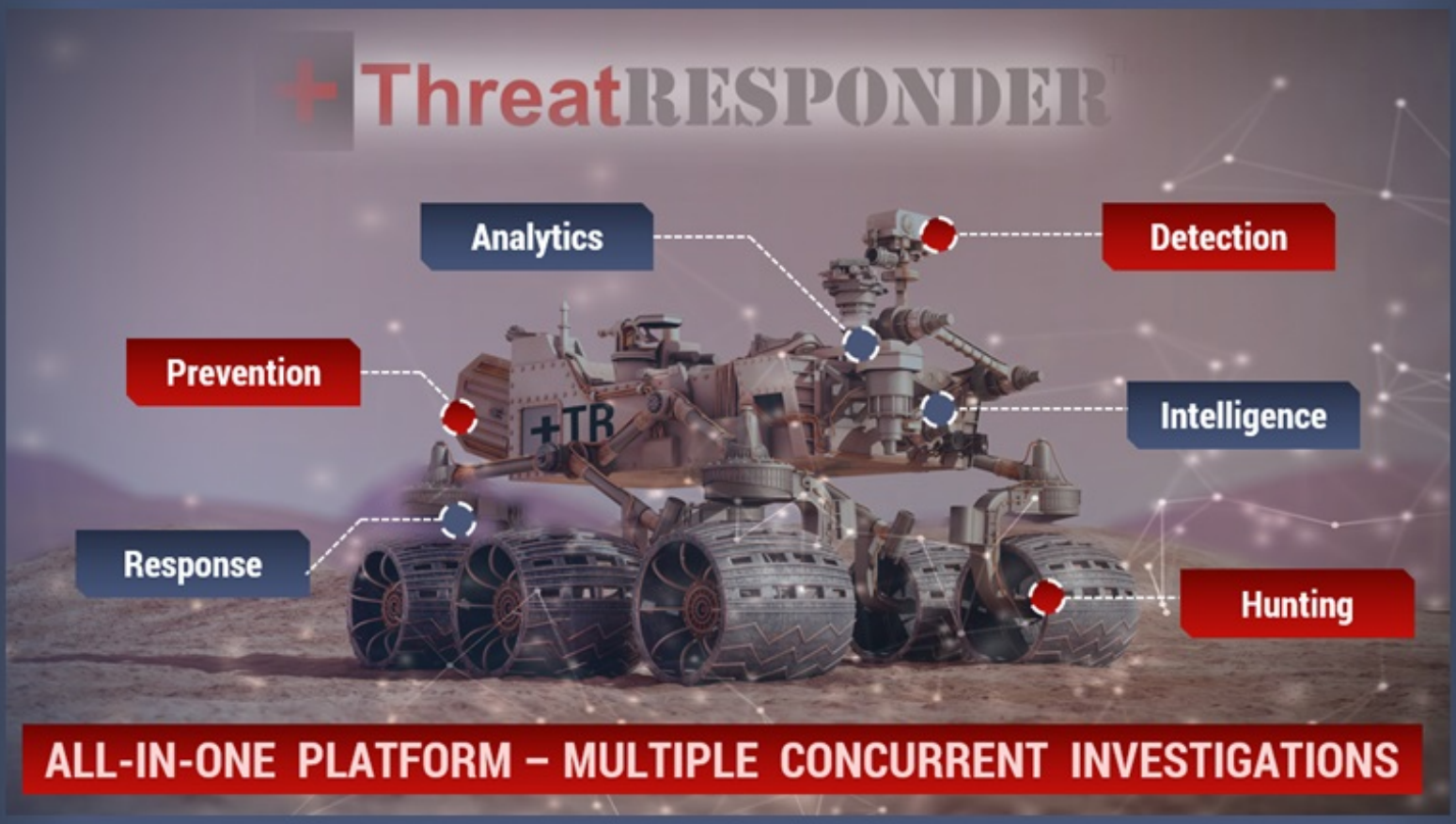
this to obtain sensitive information. Mark Ermolov, Dmitry Sklyarov and Maxim Goryachy discovered that some Intel processors did not prevent test and debug logic from being activated at runtime. A local attacker could use this to escalate privileges.

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



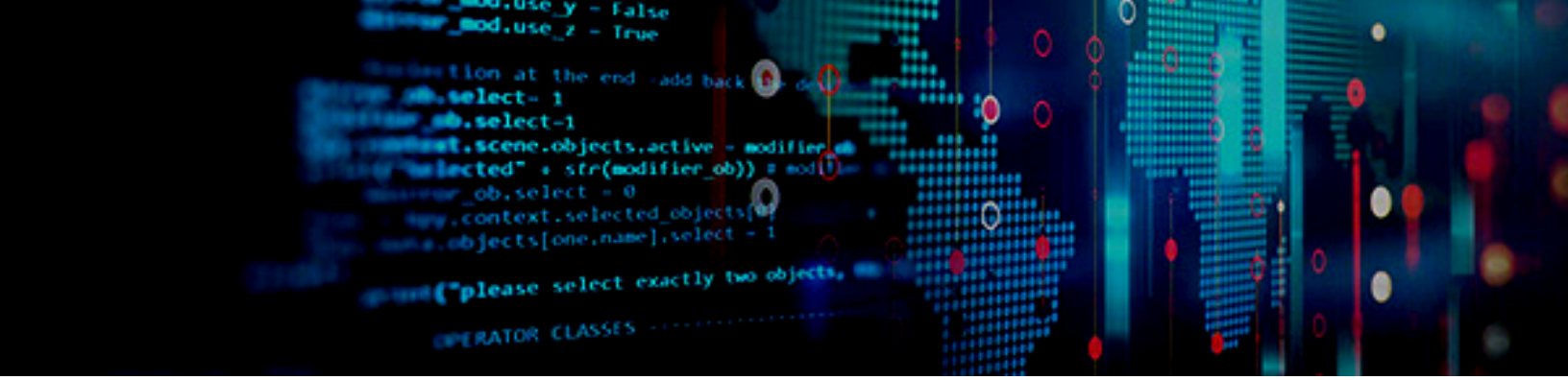
The Solution – ThreatResponder® Platform

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

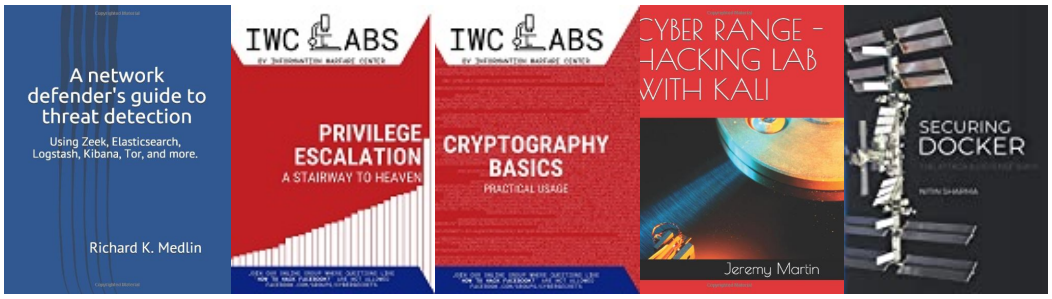


The Cyber Secrets publications on Amazon

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