Jun-06-22

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®

CYBER WEEKLY AWARENESS REPORT

June 6, 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

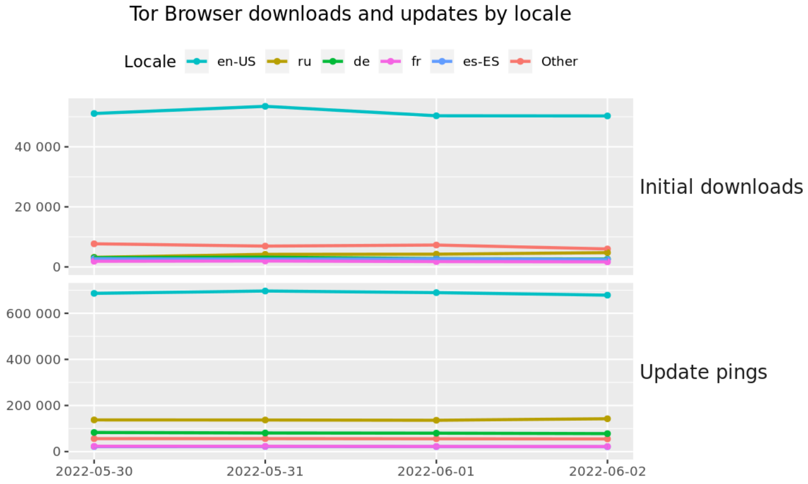
Internet Storm Center Infocon Status

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.



The Tor Project - https://metrics.torproject.org/

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

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* FDA Urges Patch Of Illumina Devices
* Clipminer Rakes In $1.7m In Crypto Hijacking Scam
* Evil Corp Pivots LockBit To Dodge U.S. Sanctions
* Zero-Day Exploitation Of Atlassian Confluence
* Scammers Target NFT Discord Channel
* Here's Why The World's Most Infamous Spyware Maker Is Broke
* International Authorities Take Down Flubot Malware Network
* US Ran Offensive Cyber Ops To Support Ukraine, Says General
* Tim Horton's App Tracked Movement In Violation Of Privacy Laws
* EnemyBot Malware Adds Enterprise Flaws To Exploit Arsenal
* Industrial IoT Ransomware Attacks Control Systems Directly
* Microsoft Releases Workaround For 1-Click 0-Day Under Active Attack
* Bad News: The Cybersecurity Skills Crisis Is About To Get Even Worse
* Germany Issues Fresh Warning To Banks Of Cyber Attacks Due To Ukraine War
* The Underground Company That Hacks iPhones For Ordinary Consumers
* ChromeLoader Browser Hijacker Provides Gateway To Bigger Threats
* Guardian Launches Tor Onion Service
* Australian Digital Driving Licenses Can Be Defaced In Minutes
* Russia Nixes US Charges Against REvil As Cooperation Fizzles
* Ransomware Attack Sends US County Back To 1977
* Global Tech Industry Objects To India's New Infosec Reporting Regime
* The Mystery Of China's Sudden Warnings About US Hackers
* CISA Adds 75 Actively Exploited Bugs To Its Must-Patch List In Just A Week
* Surveillance Tech Didn't Stop The Uvalde Massacre
* Critical Flaws In Popular ICS Platform Can Trigger RCE

Krebs on Security

* 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
* Microsoft Patch Tuesday, May 2022 Edition
* Your Phone May Soon Replace Many of Your Passwords
* Russia to Rent Tech-Savvy Prisoners to Corporate IT?
* You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
* Fighting Fake EDRs With 'Credit Ratings' for Police

LATEST NEWS

Dark Reading

* FDA: Patch Illumina DNA Sequencing Instruments, Stat
* YourCyanide Ransomware Propagates With PasteBin, Discord, Microsoft Links
* Iconium Software Releases DataLenz v1.3 for IBM zSystems
* Microsoft Disables Iran-Linked Lebanese Hacking Group Polonium
* Actively Exploited Atlassian Zero-Day Bug Allows Full System Takeover
* Why Network Object Management Is Critical for Managing Multicloud Network Security
* For Ransomware, Speed Matters
* Cerberus Sentinel Completes Acquisition of Creatrix, Inc.
* Research Reveals 75% of CISOs Are Worried Too Many Application Vulnerabilities Leak Into Production,
* Intel Chipset Firmware Actively Targeted by Conti Group
* Gurucul Launches Cloud-Native SOC Platform Pushing the Boundaries of Next-Gen SIEM and XDR with Ident
* Phishers Having a Field Day on WhatsApp, Telegraph
* New Cloud Pricing and Products Proof of RSA's Transformation
* Microsoft Philanthropies Collaborates With WiCyS to Help Close the Cybersecurity Skills Gap
* US Sanctions Force Evil Corp to Change Tactics
* CyberQ Technologies Inc. Launches Managed AI for Splunk UBA Customers
* Neosec Introduces Expert Managed Threat Hunting Service for Detecting and Investigating API Abuse and
* Turbulent Cyber Insurance Market Sees Rising Prices and Sinking Coverage
* Building America's Cybersecurity Infrastructure
* 'Clipminer' Malware Actors Steal $1.7 Million Using Clipboard Hijacking

The Hacker News

* State-Backed Hackers Exploit Microsoft 'Follina' Bug to Target Entities in Europe and U.S
* Atlassian Releases Patch for Confluence Zero-Day Flaw Exploited in the Wild
* GitLab Issues Security Patch for Critical Account Takeover Vulnerability
* Chinese LuoYu Hackers Using Man-on-the-Side Attacks to Deploy WinDealer Backdoor
* Researchers Uncover Malware Controlling Thousands of Sites in Parrot TDS Network
* Microsoft Blocks Iran-linked Lebanese Hackers Targeting Israeli Companies
* Hackers Exploiting Unpatched Critical Atlassian Confluence Zero-Day Vulnerability
* Threat Detection Software: A Deep Dive
* Conti Leaks Reveal Ransomware Gang's Interest in Firmware-based Attacks
* Researchers Demonstrate Ransomware for IoT Devices That Targets IT and OT Networks
* ExpressVPN Removes Servers in India After Refusing to Comply with Government Order
* Critical UNISOC Chip Vulnerability Affects Millions of Android Smartphones
* SideWinder Hackers Use Fake Android VPN Apps to Target Pakistani Entities
* DOJ Seizes 3 Web Domains Used to Sell Stolen Data and DDoS Services
* New Unpatched Horde Webmail Bug Lets Hackers Take Over Server by Sending Email

LATEST NEWS

Security Week

* Critical U-Boot Vulnerability Allows Rooting of Embedded Systems
* Atlassian Patches Confluence Zero-Day as Exploitation Attempts Surge
* Activists Say Cyber Agency Weakens Voting Tech Advisory
* Foxconn Confirms Ransomware Hit Factory in Mexico
* Ten Eleven Ventures Raises $600M Fund for Cybersecurity Investments
* Digital Experience Monitoring: More Important Than Ever
* Chainguard Bags Massive $50M Series A for Supply Chain Security
* Deadly Secret: Electronic Warfare Shapes Russia-Ukraine War
* CISA Warns of Critical Vulnerabilities in Illumina Genetic Analysis Devices
* Lebanese Threat Actor 'Polonium' Targets Israeli Organizations
* TXOne Unveils New OT Network Security Appliance for SMB Manufacturers
* Atlassian Confluence Servers Hacked via Zero-Day Vulnerability
* Report: Clipminer Botnet Operators Rake in $1.7 Million
* Exiled Iran Group Claims Tehran Hacking Attack
* Logging and Security Analytics Firm Devo Banks New $100 Million Investment
* Millions of Budget Smartphones With UNISOC Chips Vulnerable to Remote DoS Attacks
* Dutch Used Pegasus Spyware on Most-Wanted Criminal: Report
* Cloud Data Security Startup Laminar Raises $30 Million
* US Authorities Seize Domains Selling Stolen Data, DDoS Services
* Leaks Show Conti Ransomware Group Working on Firmware Exploits
* US Warns Organizations of 'Karakurt' Cyber Extortion Group
* Cloud Security Startup JupiterOne Lands $70 Million at 'Unicorn' Valuation
* Coralogix Raises $142 Million for Data Observability Platform
* Automation. Where do We Go from Here?
* Access Brokers and Ransomware-as-a-Service Gangs Tighten Relationships
* Cybercriminals Hold 1,200 Unsecured Elasticsearch Databases for Ransom

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Why We Recommend Your Passwords Be Over 20-Characters Long
* Introducing KnowBe4's Password Policy E-Book
* Your KnowBe4 Fresh Content Updates from May 2022
* Smishing and Home Delivery
* SideWinder Targets Pakistani Entities With Phishing Attacks
* U.K.'s National Health Service Becomes the Latest Victim of a Credential Harvesting Phishing Operatio
* Phishing Attacks Rise 54% as the Initial Attack Vector Across All Threat Incidents
* The Business (and Success) of Ransomware Explained as a Simple Funnel
* CyberheistNews Vol 12 #22 [Heads Up] The New Verizon 2022 Data Breach Investigation Report Shows Shar
* Phishing Campaign Targets QuickBooks Users

ISC2.org Blog

* Update on (ISC)&sup2; Entry-Level Cybersecurity Certification Pilot
* The United States Department of Justice Will no Longer Prosecute Ethical Hackers
* Journey Into Cybersecurity - Conversations with Cyber Newcomers, Part 2
* (ISC)2 Supports Members with Thoughtful Response to SEC Proposed Rule on Cybersecurity Reporting
* Journey Into Cybersecurity - Conversations with Cyber Newcomers, Part 1

HackRead

* Anonymous Hacktivists Leak 1TB of Top Russian Law Firm Data
* Scoop: Australian Trading Giant ACY Securities Exposed 60GB of User Data
* Fake Updates Continue To Be A Digital Risk: What To Do?
* Authorities Take Down SMS-based FluBot Android Spyware
* FBI Seizes WeLeakInfo, IPStress and OVH-Booter Cybercrime Portals
* ExpressVPN Removes VPN Servers in India Rejecting Data Collection Law
* Types of Web Hosting and How Much Does It Cost To Host A Website?

Koddos

* Anonymous Hacktivists Leak 1TB of Top Russian Law Firm Data
* Scoop: Australian Trading Giant ACY Securities Exposed 60GB of User Data
* Fake Updates Continue To Be A Digital Risk: What To Do?
* Authorities Take Down SMS-based FluBot Android Spyware
* FBI Seizes WeLeakInfo, IPStress and OVH-Booter Cybercrime Portals
* ExpressVPN Removes VPN Servers in India Rejecting Data Collection Law
* Types of Web Hosting and How Much Does It Cost To Host A Website?

LATEST NEWS

Naked Security

* Atlassian announces 0-day hole in Confluence Server - update soon!
* Yet another zero-day (sort of) in Windows "search URL" handling
* S3 Ep85: Now THAT'S what I call a Microsoft Office exploit! [Podcast]
* Firefox 101 is out, this time with no 0-day scares (but update anyway!)
* Mysterious "Follina" zero-day hole in Office - here's what to do!
* Beware the Smish! Home delivery scams with a professional feel&hellip;
* S3 Ep84: Government demand, Mozilla velocity, and Clearview fine [Podcast]
* Who's watching your webcam? The Screencastify Chrome extension story&hellip;
* Poisoned Python and PHP packages purloin passwords for AWS access
* Clearview AI face-matching service fined a lot less than expected

Threat Post

* Old Hacks Die Hard: Ransomware, Social Engineering Top Verizon DBIR Threats - Again
* Evil Corp Pivots LockBit to Dodge U.S. Sanctions
* Cybercriminals Expand Attack Radius and Ransomware Pain Points
* Scammers Target NFT Discord Channel
* International Authorities Take Down Flubot Malware Network
* Being Prepared for Adversarial Attacks - Podcast
* Microsoft Releases Workaround for 'One-Click' 0Day Under Active Attack
* EnemyBot Malware Targets Web Servers, CMS Tools and Android OS
* ChromeLoader Browser Hijacker Provides Gateway to Bigger Threats
* Zero-Day 'Follina' Bug Lays Microsoft Office Open to Attack

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

LATEST NEWS

IBM Security Intelligence

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

InfoWorld

* Maximize your cloud security with isolation zones
* Cloud complicates everything, but supergraphs offer hope
* 12 programming tricks to cut your cloud bill
* Deno Deploy moves toward GA, adds paid plan
* GitHub Enterprise Server adds code security, automation features
* Legacy systems should be part of a multicloud strategy
* What is TensorFlow? The machine learning library explained
* C++ 23 to introduce module support
* Use logging and DI in minimal APIs in ASP.NET Core 6
* Better Java: JDK Enhancement Proposals explained

C4ISRNET - Media for the Intelligence Age Military

* Unlocking airborne ISR can help achieve regional security in Indo-Pacific
* Special operations forces need AI that can explain its decisions, says military data chief
* Strategic review to guide US approach to space weapons, classification, Liquori says
* Palantir's Karp is first western CEO to visit Zelenskyy amid invasion
* To maximize cybersecurity dollars, lean on Zero Trust
* Government watchdog finds major flaws in US Space Command basing process
* Pentagon's AI, data office fully operational as leadership posts filled
* US military may need innovation overhaul to fight future wars, Milley says
* Space Development Agency chooses satellite ground segment provider
* Ukraine war shows danger of unencrypted communications, says US Army secretary

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

* Release of Technical Report into the AMD Security Processor
* The More You Know, The More You Know You Don't Know

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.

* Grey Cat The Flag 2022
* Tenable CTF 2022
* Access Denied CTF 2022
* usd Hacking Night
* justCTF 2022
* Imperial CTF 22 Finals
* WeCTF 2022
* STANDCON CTF 2022
* TyphoonCon CTF 2022
* BSidesTLV 2022 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

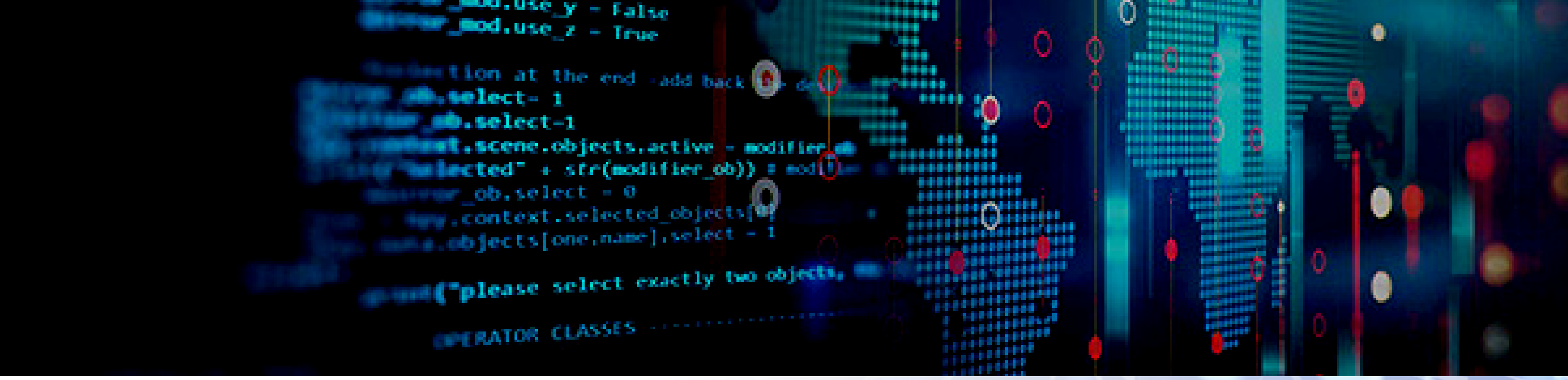
* GRR 3.4.6.0
* I2P 1.8.0
* Deliverance 0.018-daf9452 File Descriptor Fuzzer
* TP-Link Backup Decryption Utility
* Lynis Auditing Tool 3.0.8
* COOPER Analysis Tool
* Aircrack-ng Wireless Network Tools 1.7
* Samhain File Integrity Checker 4.4.9
* Adversary3 2.0
* Wireshark Analyzer 3.6.5

Kali Linux Tutorials

* Smap : A Drop-In Replacement For Nmap Powered By Shodan.Io
* ADReaper : A Fast Enumeration Tool For Windows Active Directory Pentesting Written In Go
* KrbRelay : Framework For Kerberos Relaying
* Zircolite : A Standalone SIGMA-based Detection Tool For EVTX, Auditd And Sysmon For Linux Logs
* linWinPwn : A Bash Script That Automates A Number Of Active Directory Enumeration And Vulnerability C
* OWASP Coraza WAF : A Golang Modsecurity Compatible Web Application Firewall Library
* Kraken : A Multi-Platform Distributed Brute-Force Password Cracking System
* vAPI : Vulnerable Adversely Programmed Interface Which Is Self-Hostable API
* EDRSandblast : Tool That Weaponize A Vulnerable Signed Driver To Bypass EDR Detections And LSASS Prot
* 365Inspect : A PowerShell Script That Automates The Security Assessment Of Microsoft Office 365 Envir

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

* SANS Threat Analysis Rundown
* 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

* How Hackers Use DNS Spoofing to Phish Passwords (WiFi Pineapple Demo)
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Assembling and Soldering Our DIY 3D Printed Drone

The PC Security Channel [TPSC]

* Windows Defender Bypassed
* Android Malware: SharkBot

Eli the Computer Guy

* How to DESTROY a YOUTUBE CHANNEL
* APPLE SUPPORTS CHINESE REPRESSION
* ELON MUSK WANTS RECESSION - survival of the fittest... meme's...
* ELON MUSK SUED by TWITTER SHAREHOLDERS

Security Now

* DuckDuckGone? - Digital Driver's License, MS Office 0-day, GhostTouch, Vodafone TrustPiD
* Dis-CONTI-nued: The End of Conti? - Clearview AI in Ukraine, Vancouver Pwn2Own, Voyager 1

Troy Hunt

* Weekly Update 298

Intel Techniques: The Privacy, Security, & OSINT Show

* 264-Back to Basics-Linux I
* 263-Proton Changes & New Breach Lessons

Proof of Concept (PoC) & Exploits

Packet Storm Security

* NVIDIA Data Center GPU Manager Remote Memory Corruption
* Real Player 20.1.0.312 / 20.0.3.317 DLL Hijacking
* IIPImage Remote Memory Corruption
* Telesquare SDT-CW3B1 1.1.0 Command Injection
* SolarView Compact 6.00 Directory Traversal
* Contao 4.13.2 Cross Site Scripting
* Microweber CMS 1.2.15 Account Takeover
* Zyxel USG FLEX 5.21 Command Injection
* libMeshb Buffer Overflow
* Product Show Room Site 1.0 Cross Site Scripting
* dotCMS Shell Upload
* GtkRadiant 1.6.6 Buffer Overflow
* Packet Storm New Exploits For May, 2022
* libxml2 xmlBufAdd Heap Buffer Overflow
* OpenSSL 1.0.2 / 1.1.1 / 3.0 BN_mod_sqrt() Infinite Loop
* Avantune Genialcloud ProJ 10 Cross Site Scripting
* Real Player 16.0.3.51 / Cloud 17.0.9.17 / 20.0.7.309 DCP URI Remote Code Execution
* Real Player 16.00.282 / 16.0.3.51 / Cloud 17.0.9.17 / 20.0.7.309 Remote Code Execution
* Real Player 20.0.8.310 G2 Control DoGoToURL() Remote Code Execution
* MyBB Admin Control Remote Code Execution
* Microsoft Office MSDT Follina Proof Of Concept
* Microsoft Follina Proof Of Concept
* Fast Food Ordering System 1.0 Cross Site Scripting
* Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 Remote Root
* WordPress User Meta Lite / Pro 2.4.3 Path Traversal

CXSecurity

* dotCMS Shell Upload
* NVIDIA Data Center GPU Manager Remote Memory Corruption
* Telesquare SDT-CW3B1 1.1.0 Command Injection
* IIPImage Remote Memory Corruption
* Microsoft Office MSDT Follina Proof Of Concept
* Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 Remote Root
* qdPM 9.1 Remote Code Execution (RCE) (Authenticated) (v2)

Proof of Concept (PoC) & Exploits

Exploit Database

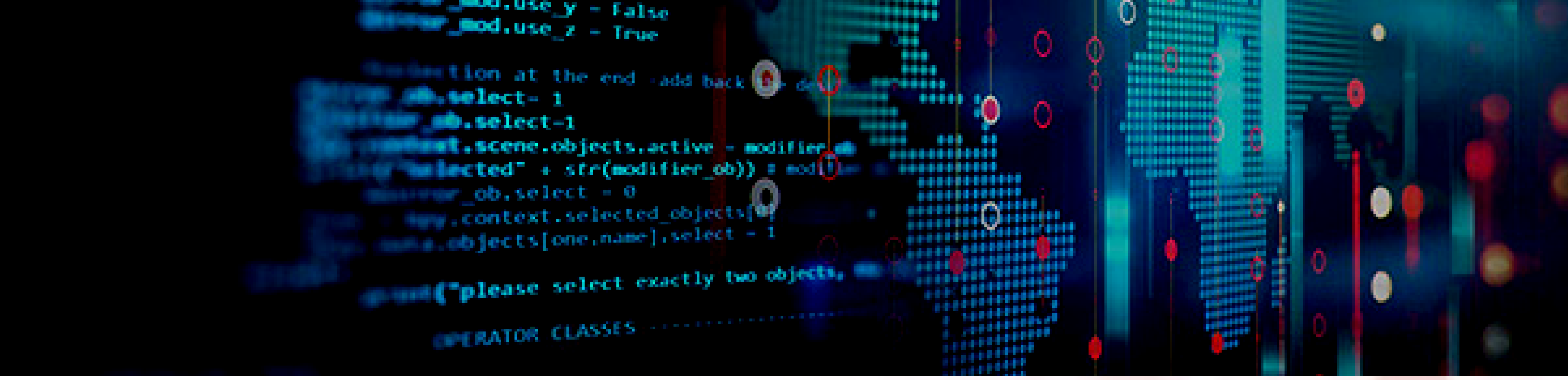
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)
* [remote] Telesquare SDT-CW3B1 1.1.0 - OS Command Injection
* [webapps] Microweber CMS 1.2.15 - Account Takeover
* [remote] Zyxel USG FLEX 5.21 - OS Command Injection
* [webapps] Contao 4.13.2 - Cross-Site Scripting (XSS)
* [webapps] qdPM 9.1 - Remote Code Execution (RCE) (Authenticated) (v2)
* [webapps] m1k1o's Blog v.10 - Remote Code Execution (RCE) (Authenticated)
* [webapps] OpenCart v3.x Newsletter Module - Blind SQLi
* [webapps] Showdoc 2.10.3 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.0 - OS Command Injection
* [webapps] T-Soft E-Commerce 4 - SQLi (Authenticated)
* [webapps] T-Soft E-Commerce 4 - 'UrunAdi' Stored Cross-Site Scripting (XSS)
* [webapps] Survey Sparrow Enterprise Survey Software 2022 - Stored Cross-Site Scripting (XSS)
* [remote] SDT-CW3B1 1.1.0 - OS Command Injection
* [webapps] TLR-2005KSH - Arbitrary File Delete
* [webapps] Royal Event Management System 1.0 - 'todate' SQL Injection (Authenticated)
* [webapps] College Management System 1.0 - 'course_code' SQL Injection (Authenticated)
* [remote] F5 BIG-IP 16.0.x - Remote Code Execution (RCE)
* [webapps] TLR-2005KSH - Arbitrary File Upload
* [remote] Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)
* [webapps] Joomla Plugin SexyPolling 2.1.7 - SQLi
* [webapps] WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)
* [webapps] MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE) (Authenticated)

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
```

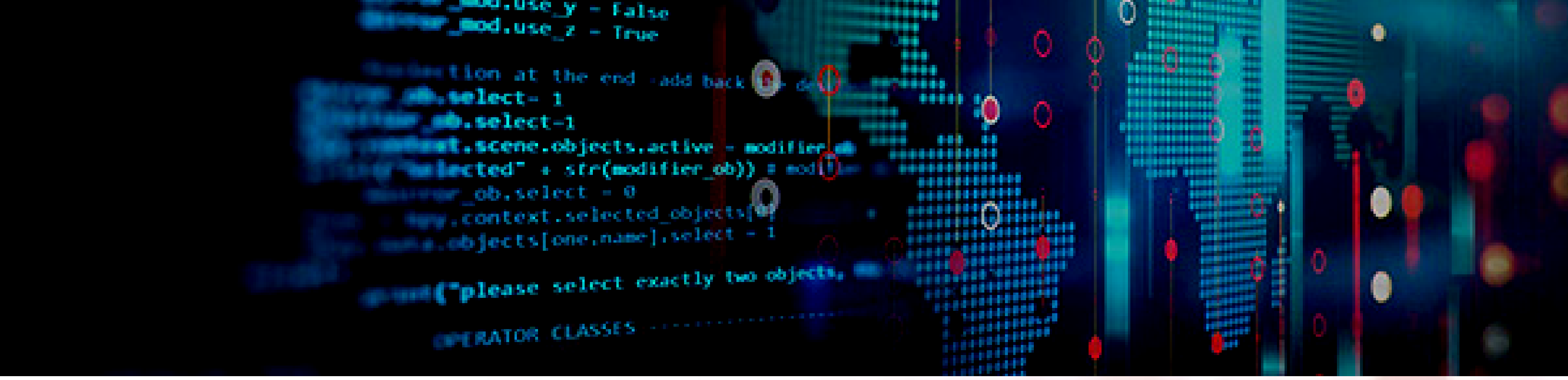
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
t.scene.objects.active = modifier_ob
"Selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Latest Hacked Websites

Published on Zone-h.org

https://hma.gob.pe/xaad.html
https://hma.gob.pe/xaad.html notified by Mr.XaaD
https://inmujerguadalupe.gob.mx/1975.html
https://inmujerguadalupe.gob.mx/1975.html notified by 1975 Team
https://apizaco.gob.mx/abcd.html
https://apizaco.gob.mx/abcd.html notified by ./KeyzNet
http://mag.gov.py/1975.html
http://mag.gov.py/1975.html notified by 1975 Team
https://munichinautla.gob.gt/vz.txt
https://munichinautla.gob.gt/vz.txt notified by aDriv4
http://spb3.go.th/rz.php
http://spb3.go.th/rz.php notified by AnonCoders
https://mains.gov.my/readme.html
https://mains.gov.my/readme.html notified by AnonSec Team
https://malakakab.go.id/index.html
https://malakakab.go.id/index.html notified by Approve1337
http://morong.gov.ph/dz.php
http://morong.gov.ph/dz.php notified by djebbaranon
http://dinalupihan.gov.ph/dz.php
http://dinalupihan.gov.ph/dz.php notified by djebbaranon
http://pilarbataan.gov.ph/dz.php
http://pilarbataan.gov.ph/dz.php notified by djebbaranon
https://hospitalsanandreschiriguana.gov.co/1975.html
https://hospitalsanandreschiriguana.gov.co/1975.html notified by 1975 Team
https://pupr.padangpariamankab.go.id/lovv.html
https://pupr.padangpariamankab.go.id/lovv.html notified by /Rayzky_
http://yala.nfe.go.th/betong/web1/file_editor/0x.txt
http://yala.nfe.go.th/betong/web1/file_editor/0x.txt notified by L4663R666H05T
http://phuket.nfe.go.th/kathu/web1/file_editor/0x.txt
http://phuket.nfe.go.th/kathu/web1/file_editor/0x.txt notified by L4663R666H05T
https://virtualshowroom.nissan.com.eg/a.txt
https://virtualshowroom.nissan.com.eg/a.txt notified by Trenggalek Cyber Army
https://virtual360.nissan-saudiarabia.com/a.txt
https://virtual360.nissan-saudiarabia.com/a.txt notified by Trenggalek Cyber Army



Dark Web News

Darknet Live

Man Admits Exchanging Crypto Without Government Approval

A 49-year-old man admitted exchanging cryptocurrency through Paxful and LocalBitcoins. According to an announcement from the U.S. Attorney's Office for the Southern District of Texas, 49-year-old Hien Ngoc Vo admitted to operating an unlicensed money transmitting business. Between March 16, 2016, and June 8, 2016, the defendant processed $515,147.19 in Bitcoin on Paxful and LocalBitcoins. "Vo received funds in the form of cash, direct bank deposits, American Express credit cards as well as Amazon and generic gift cards. He used several bank accounts to conduct his business, but the banks shut down the accounts after inquiring about the origination of the funds.&rdquo; U.S. Attorney Jennifer B. Lowery announced the guilty plea. Vo collected between 5 and 30% of every transaction he conducted. Additionally, Vo did not require any form of identification from his clients, nor did he ask "the purpose for which they were purchasing the cryptocurrency.&rdquo; Chief U.S. District Judge Lee H. Rosenthal will sentence Vo on September 5, 2020. Vo faces a maximum sentence of five years in prison. He will serve much less time behind bars if any. Houston area unlicensed cryptocurrency business results in conviction | archive.is, justice.gov Apparently this is something they are regularly prosecuting now? (via darknetlive.com at https://darknetlive.com/post/mommy-government-strikes-again-for-faiulure-to-register-crypto-exchange/)

FBI Seized weleakinfo.to and "Two Related Domains"

The FBI and the U.S. Department of Justice announced the seizure of three domains as part of an international cybercrime investigation. "Today, the FBI and the Department stopped two distressingly common threats: websites trafficking in stolen personal information and sites which attack and disrupt legitimate internet businesses,&rdquo; said U.S. Attorney Graves. "Cyber crime often crosses national borders. Using strong working relationships with our international law enforcement partners, we will address crimes like these that threaten privacy, security, and commerce around the globe.&rdquo; Visitors of the websites are met with a seizure banner. Three domains are now in the custody of the Department of Justice: weleakinfo.to, ipstress.in, and ovh-booter.com. "These seizures are prime examples of the ongoing actions the FBI and our international partners are undertaking to disrupt malicious cyber activity,&rdquo; said Special Agent in Charge Jacobs. "Disrupting malicious DDoS operations and dismantling websites that facilitate the theft and sale of stolen personal information is a priority for the FBI.&rdquo; The search feature on WeLeakInfo.to. Weleakinfo.to hosted a database of seven billion indexed records, including names, email addresses, usernames, phone numbers, and passwords for online accounts. Customers could pay for a subscription that allowed them to search for records for the duration of the subscription. The site offered several different subscriptions ranging from $2 to $70 per month. In January 2020, the FBI announced the seizure of weleakinfo.com. ipstress.in and ovh-booter.com, as indicated by their addresses, allowed paying customers to launch Distributed Denial of Service attacks with the site's infrastructure. The Netherlands National Police Corps and the Belgium Federal Police assisted in the investigation. The FBI's international partners arrested one suspect, executed search warrants, and seized server infrastructure. "Trusted by governments...&rdquo;

WeLeakInfo.to and Related Domain Names Seized | archive.is, justice.gov (via darknetlive.com at https://darknetlive.com/post/fbi-seized-weleakinfo-and-other-sites/)

Two Indicted for Selling Fent Analogues in "Canada1" Case

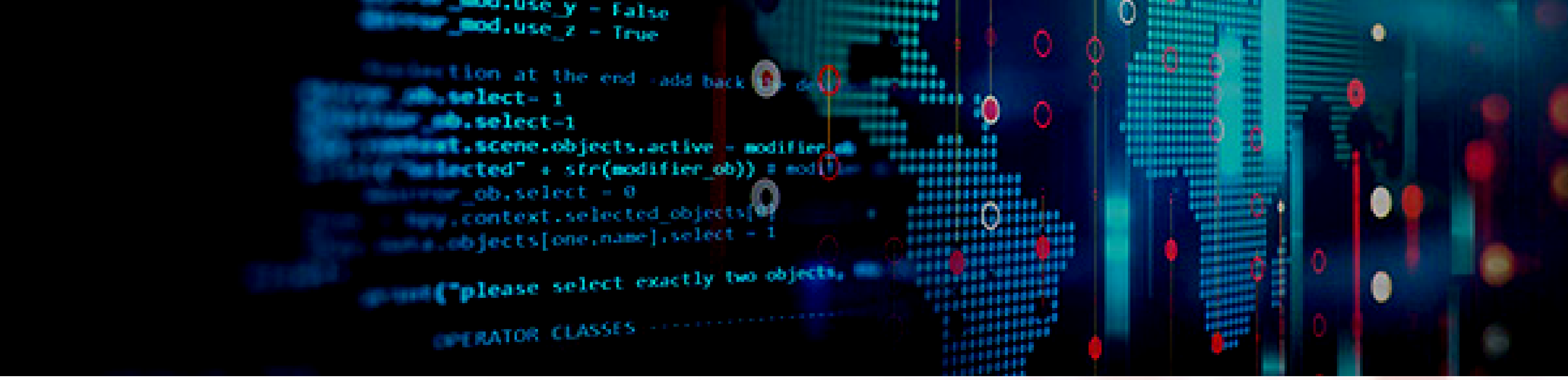
A recently unsealed indictment accuses two people of selling fentanyl analogues on Dream Market under the username "Canada1.&rdquo; Thomas Michael Federuik, 59, of Vancouver, British Columbia, Canada, and Paul Anthony Nicholls, 44, of Surrey, England, have been indicted in the Southern District of Georgia on drug distribution and money laundering charges. The indictment charges both defendants with one count of Conspiracy to Import Controlled Substances, Conspiracy to Distribute Controlled Substances, and Money Laundering Conspiracy. "Pills in the underground drug market and on the Dark Web are often diluted with dangerous and deadly substances like fentanyl, as was the case in this investigation,&rdquo; said Robert J. Murphy, the Special Agent in Charge of the DEA. Atlanta Field Division. "There is no quality control in the process, so there's a high chance that users will receive a deadly dose of fentanyl. The success of this investigation was made possible because of the collaborative efforts between all law enforcement agencies involved.&rdquo; _ Robert J. Murphy, the Special Agent in Charge of the DEA. Atlanta Field Division According to the indictment, the defendants sold U-47700 and U-49900 through Dream Market under the username "Canada1.&rdquo; _ Nobody is able to find sites on the darknet. They are just that hidden. The investigation into Canada1 began in October 2017 after two U.S. Navy petty officers in Kingsland, Ga., fatally overdosed on a fentanyl analogue. Investigators learned that the two people who had overdosed-referred to in the indictment as B.J.T. and T.L.B.-had ordered the analogue from Canada1. They also learned that the vendor had shipped the drugs in packages labeled "East Van Eco Tours&rdquo; and "Bridge City Consulting L.L.P.&rdquo; "The U.S. Postal Inspection Service's objectives are to preserve the integrity of the nation's mail system from criminal misuse, rid the mail of illicit drugs, and to keep our communities safe,&rdquo; said Juan A. Vargas, Acting Inspector in Charge of the U.S. Postal Inspection Service Miami Division. "Postal Inspectors will work with our law enforcement partners to combine resources and expertise to achieve a common goal, which is to combat the perils of illegal and dangerous drug distribution and ensure perpetrators of such attempts are brought to justice.&rdquo; The Royal Canadian Mounted Police (RCMP) determined that the defendants had created or used those companies. The indictment accuses both suspected drug dealers of creating companies to facilitate the importation of fentanyl analogues from dealers overseas. Both defendants are in custody pending extradition hearings. The court documents do not reveal much about the case. The press release from the U.S. Attorney's Office for the Southern District of Georgia just regurgitates the same limited information. If convicted of the charges, both defendants face a mandatory minimum sentence of 10 years in prison, up to life. "The case is being investigated in Canada by U.S. Homeland Security Investigations, Vancouver; the Royal Canadian Mounted Police and its Online Undercover Operations Unit and Federal Serious and Organized Crime Unit, Cybercrime Operations Group; Calgary Police Service; and the Canada Border Service Agency. "In the United Kingdom, assistance was provided by the National Extradition Unit with the Metropolitan Police and the Staffordshire Police. "And in the United States, by the U.S. Food and Drug Administration Office of Criminal Investigations; the U.S. Naval Criminal Investigative Service; Homeland Security Investigations Savannah; the U.S. Drug Enforcement Administration; and the U.S. Postal Inspection Service, with assistance from the U.S. Marshals Service. The U.S. Department of Justice's Office of International Affairs is providing significant assistance.&rdquo; Two men indicted for international conspiracy to ship Fentanyl, other drugs into United States through Dark Web connections | archive.is, justice.gov Indictment: pdf (via darknetlive.com at https://darknetlive.com/post/two-arrested-in-canada1-case/)

Two Marijuana Dealers Sentenced for Laundering Bitcoin

A father and son were sentenced to five years in prison for marijuana distribution and money laundering. U.S. District Judge John C. Coughenour sentenced Kenneth Warren Rhule (K. H. Rhule), 28, to five years in prison for conspiracy to manufacture and distribute marijuana and laundering monetary instruments. The judge sentenced Kenneth John Rule (K. J. Rhule), 47, to five years in prison for conspiracy to manufacture and distribute marijuana. "Not only did this pair produce and distribute marijuana products on the dark web, in violation of the state's regulatory scheme, they also illegally laundered immense amounts of bitcoin that their enterprise earned,&rdquo; said U.S. Attorney Nick Brown. "When law enforcement moved in there were more than a dozen firearms - some loaded and ready to be used to protect their drug trade.&rdquo; __ Altogether, Rhule exchanged $142,000 worth of bitcoin for cash with the undercover agent. LocalBitcoins _ In April 2018, federal investigators started meeting with the localbitcoins.com user "Gimacut93&rdquo; to exchange cash for Bitcoin. "Through their conversations the undercover agent made it seem they were laundering money related to human trafficking activities,&rdquo; according to the announcement from the U.S. Attorney's Office for the Western District of Washington. The criminal complaint detailed the investigation into the money laundering activities. Investigators contacted Gimacut93 on localbitcoins.com and asked to meet to exchange $12,000 in cash for Bitcoin. Kenneth Warren Rhule met the undercover law enforcement officer at a Starbucks. While waiting for confirmations, K.W. Rhule told the undercover agent that he worked in the CBD industry, filling "5, 10, or 20,000-kilo orders.&rdquo; He also told the agent that he was not charging a fee because he had a lot of Bitcoin he needed to move, and he usually needed to exchange $100,000 worth every month. __ "CBD industry&rdquo; "In completing these transactions, the undercover agent represented the cash to be the proceeds of specified unlawful activity, as defined in 18 U.S.C. &sect; 1956(c)(7), and K. W. Rhule acted with the intent to avoid a transaction reporting requirement under state or federal law, including those under the Bank Secrecy Act, 31 U.S.C. &sect;&sect; 5313-26, and its implementing regulations. K. W. Rhule did not ask the undercover agent for any personally identifying information (such as full name, Social Security number, or taxpayer identification number) prior to, during, or after the transactions.&rdquo; At the next meeting, the undercover L.E.O. asked K. W. Rhule about anonymous transactions with cryptocurrency. The defendant then advised the L.E.O. to use Monero, Tails, and the Tor Browser. The L.E.O. told K. W. Rhule that he needed an anonymous way to accept payment from prostitutes in the Ukraine (this is what the press release described as "human trafficking&rdquo;). __ Investigators linked the company "HerbinArtisans&rdquo; to the Rhule defendants. After exchanging more than $120,000 in Bitcoin with the feds, Gimacut93 stopped responding to their text messages and ignored them on LocalBitcoins. Instagram _ The phone number K. W. Rhule had given the undercover fed through LocalBitcoins was the same phone number used by the Instagram account "HerbinArtisans.&rdquo; Although the account is now private and does not mention cannabis sales, investigators believe that K. W. Rhule used to reach customers through the account. The description for the account previously included "Bitcoin and crypto-friendly. D.M. for inquiries.&rdquo; __ On February 10, 2015, K. W. Rhule registered for an enterprise account with Google, using the domain name herbinartisans.com. The defendant used a herbinartisans.com email address with the HerbinArtisans Instagram account. __ Investigators obtained access to the Google account. They examined emails sent by both Rhule defendants, incriminating pictures stored in Google Drive, and SMS conversations between the father and son. Google Drive _ The HerbinArtisans' Google Drive also contained an organizational chart, created on January 18, 2016, which listed "Ken&rdquo; as the "C.E.O.,&rdquo; while "Kenny&rdquo;&mdash;a name used by K. W. Rhule&mdash;was listed as the "C.O.O.&rdquo; of the organization. Other individuals, also known to be associated with HerbinArtisans, were listed in subordinate roles with the titles "Garden technician,&rdquo; "Processing lead,&rdquo; "Processor,&rdquo; and "V.P.&rdquo; on the same chart. __ The organization chart stored in Google Drive identified the defendants. The defendants purchased a Cessna P210N, which they stored in Snohomish, Washington. The plea agreement indicates that the defendants used the plane to transport marijuana. __ On April 24, 2015, K. J. Rhule texted K. W. Rhule, "Also, I have some KILLER deep web locations for selling&hellip;&rdquo; Similarly, on May 16, 2015, K. J. Rhule texted K. W. Rhule, "Also, online deep web&hellip; Setup a couple order takers&hellip; The proceeds go into a bitcoin account we control&hellip; They send in the orders each day, we ship them, and we pay out the commission when the Bitcoin escrow is released&hellip;&rdquo; __ According to an Income Statement saved in the HerbinArtisans account, from 2015 until 2019, HerbinArtisans earned a "Total [Gross] Income&rdquo; of $13,710,069.27 and a "Net Income&rdquo; of

$2,574,850.33. _ Search Warrants _ On March 10, 2020, law enforcement officers executed a search warrant at properties associated with the defendants, including a warehouse in Monroe, Washington. _ The Monroe, Washington, warehouse used by the Rhule duo. "Inside a warehouse located on the property, agents found processing equipment and materials dedicated to the extraction and concentration of marijuana including: various types of industrial-grade machinery, steel tables, industrial amounts of dry ice, dry-ice storage bin coolers, metal cylinders of various sizes, flexible metal hoses, pressure cylinders, various pumps, industrial scales, stainless steel pressure cylinders, pressure covers, vacuum pumps, electric motors, a mini dryer, a terpene trap, tube racks, mixers, chemistry mixers, multiple ovens and drying racks containing marijuana distillate products.&rdquo; "agents also found approximately 29 large garbage bags filled with marijuana plant material and multiple glass jars containing refined marijuana distillate products. Agents further found a large rotary evaporator with multiple large glass flasks, a heavy-duty press, and a 50-gallon tank of pressurized butane.&rdquo; Law enforcement officers found approximately 1,000 kilograms of bulk marijuana or marijuana extracts, including packaging, when they executed search warrants in connection with this case in March 2020. The Rhules made over $13 million in sales from marijuana distribution but netted only $2.5 million. The federal government is very concerned that Washington state could not tax the defendants' marijuana distribution operation. "&hellip;[T]he state has set up a regulatory framework to serve many important purposes, including ensuring the safety of those who produce and consume marijuana products. The state is also, of course, entitled to tax the marijuana industry. Yet the defendants ignored all this. Perhaps, as is so often true in fraud cases, they were motivated by simple greed. But in running their business in this way, they put a lot of people at risk, and disadvantaged others in the industry who chose to play by the rules.&rdquo; Judge Coughenour justified the sentence by noting the size of the enterprise and the presence of firearms. Father and son sentenced to prison for money laundering and illegal marijuana business | archive.is, archive.org, justice.gov Complaint: pdf
plea: pdf
indictment: pdf (via darknetlive.com at https://darknetlive.com/post/father-and-son-sentenced-to-five-years-for-money-laundering/)

Dark Web Link



Trend Micro Anti-Malware Blog

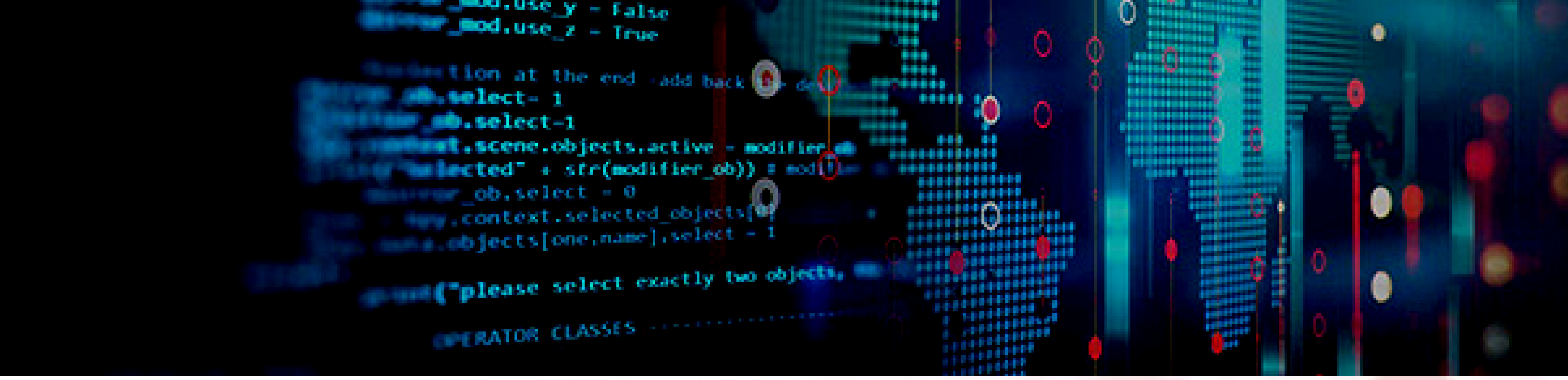
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap-Up
* Cybersecurity Is More Than a Checklist: Joel Yonts on Tech's Unfair Disadvantage
* Active Exploitation of Confluence CVE-2022-26134
* The Average SIEM Deployment Takes 6 Months. Don't Be Average.
* CVE-2022-30190: "Follina" Microsoft Support Diagnostic Tool Vulnerability
* 3 Takeaways From the 2022 Verizon Data Breach Investigations Report
* Metasploit Weekly Wrap-Up
* The Forecast Is Flipped: Flipping L&D Enables Managers to Be Impact Multipliers
* The Rapid7 Sales Culture and Experience: An Inside Look From 2 VPs
* [Security Nation] Omer Akgul and Richard Roberts on YouTube VPN Ads



Advisories

US-Cert Alerts & bulletins

* CISA Releases Security Advisory on Dominion Voting Systems Democracy Suite ImageCast X
* Atlassian Releases New Versions of Confluence Server and Data Center to Address CVE-2022-26134
* Atlassian Releases Security Advisory for Confluence Server and Data Center, CVE-2022-26134
* CISA Adds One Known Exploited Vulnerability (CVE-2022-26134) to Catalog&#8239;&#8239;
* CISA Releases Security Advisory on Illumina Local Run Manager
* CISA Updates Advisory on Threat Actors Chaining Unpatched VMware Vulnerabilities
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* Karakurt Data Extortion Group
* AA22-152A: Karakurt Data Extortion Group
* AA22-138B: Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control
* Vulnerability Summary for the Week of May 23, 2022
* Vulnerability Summary for the Week of May 16, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5459-1

Ubuntu Security Notice 5459-1 - Aur&eacute;lien Aptel discovered that cifs-utils invoked a shell when requesting a password. In certain environments, a local attacker could possibly use this issue to escalate privileges. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. It was discovered that cifs-utils incorrectly used host credentials when mounting a krb5 CIFS file system from within a container. An attacker inside a container could possibly use this issue to obtain access to sensitive information. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Red Hat Security Advisory 2022-4582-01

Red Hat Security Advisory 2022-4582-01 - The gzip packages contain the gzip data compression utility. gzip is used to compress regular files. It replaces them with files containing the .gz extension, while retaining ownership modes, access, and modification times.

Red Hat Security Advisory 2022-4592-01

Red Hat Security Advisory 2022-4592-01 - The rsync utility enables the users to copy and synchronize files locally or across a network. Synchronization with rsync is fast because rsync only sends the differences in files over the network instead of sending whole files. The rsync utility is also used as a mirroring tool.

Red Hat Security Advisory 2022-4584-01

Red Hat Security Advisory 2022-4584-01 - The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.

Red Hat Security Advisory 2022-1728-01

Red Hat Security Advisory 2022-1728-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Kernel Live Patch Security Notice LSN-0086-1

It was discovered that a race condition existed in the network scheduling subsystem of the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. Various other issues were also addressed.

Red Hat Security Advisory 2022-1729-01

Red Hat Security Advisory 2022-1729-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit.

Red Hat Security Advisory 2022-4590-1

Red Hat Security Advisory 2022-4590-1 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.9.0 ESR. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-4588-01

Red Hat Security Advisory 2022-4588-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 6.0.105 and .NET Core Runtime 6.0.5. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-4671-01

Red Hat Security Advisory 2022-4671-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-1357-01

Red Hat Security Advisory 2022-1357-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.10.

Red Hat Security Advisory 2022-2137-01

Red Hat Security Advisory 2022-2137-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java

Runtime Environment and the OpenJDK 8 Java Software Development Kit.

Red Hat Security Advisory 2022-4589-01

Red Hat Security Advisory 2022-4589-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.9.0. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-0737-01

Red Hat Security Advisory 2022-0737-01 - This release of Red Hat build of Eclipse Vert.x 4.2.5 GA includes security updates. For more information, see the release notes listed in the References section.

Red Hat Security Advisory 2022-4591-01

Red Hat Security Advisory 2022-4591-01 - Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes.

Red Hat Security Advisory 2022-4587-01

Red Hat Security Advisory 2022-4587-01 - The pcs packages provide a command-line configuration system for the Pacemaker and Corosync utilities. Issues addressed include a traversal vulnerability.

Red Hat Security Advisory 2022-1370-01

Red Hat Security Advisory 2022-1370-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.8.37.

Red Hat Security Advisory 2022-4889-01

Red Hat Security Advisory 2022-4889-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.10.0. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2022-4891-01

Red Hat Security Advisory 2022-4891-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.10.0. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-5458-1

Ubuntu Security Notice 5458-1 - It was discovered that Vim was incorrectly handling virtual column position operations, which could result in an out-of-bounds read. An attacker could possibly use this issue to expose sensitive information. It was discovered that Vim was not properly performing bounds checks when updating windows present on a screen, which could result in a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Red Hat Security Advisory 2022-4880-01

Red Hat Security Advisory 2022-4880-01 - Updated images are now available for Red Hat Advanced Cluster Security for Kubernetes (RHACS). The updated image includes bug fixes and feature improvements. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-4866-01

Red Hat Security Advisory 2022-4866-01 - Updated Satellite 6.10 Tools packages that fix several bugs are now available.

Red Hat Security Advisory 2022-4855-01

Red Hat Security Advisory 2022-4855-01 - PostgreSQL is an advanced object-relational database management system.

Red Hat Security Advisory 2022-4872-01

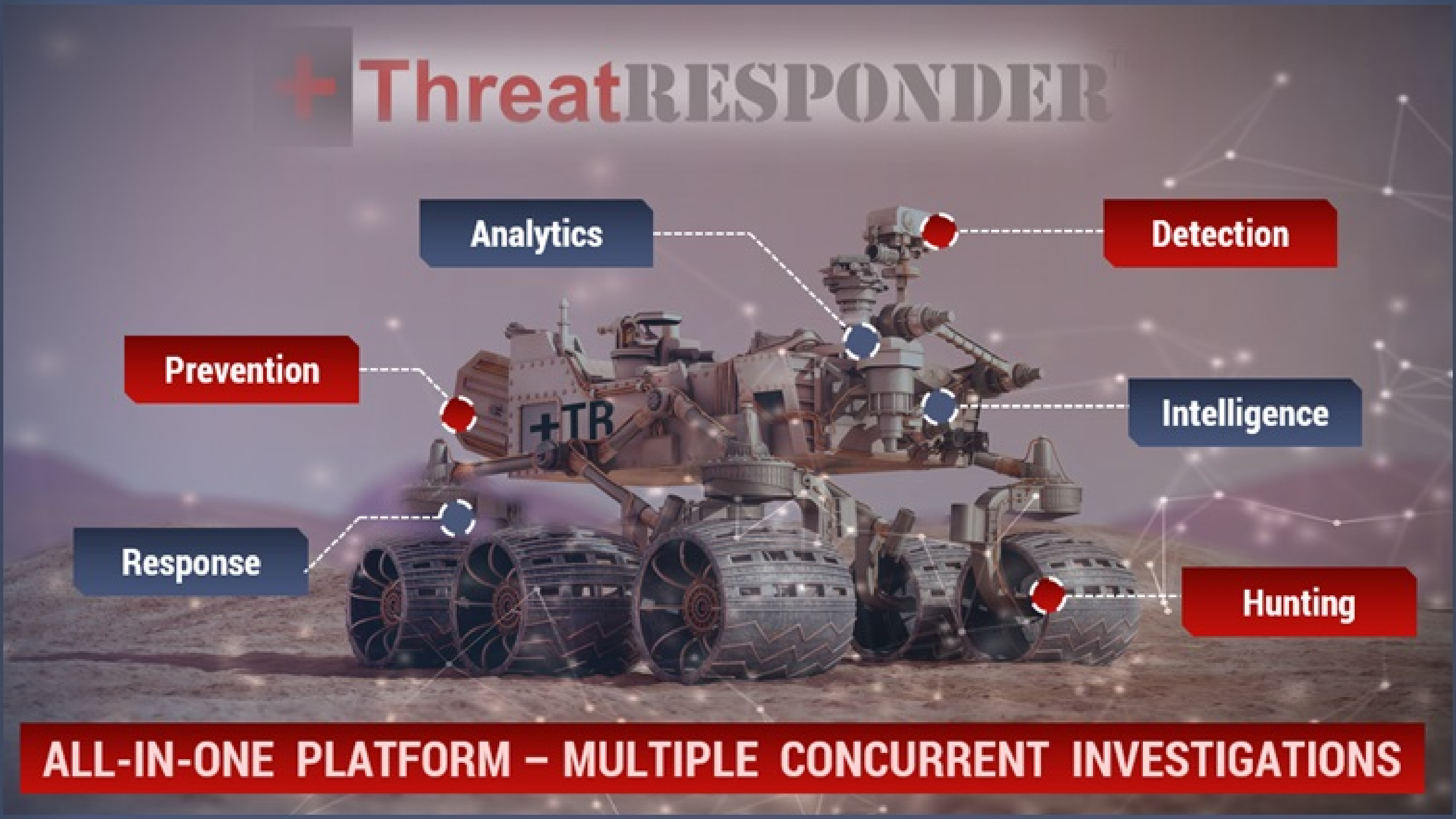
Red Hat Security Advisory 2022-4872-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.10.0 ESR. Issues addressed include a buffer overflow vulnerability.

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



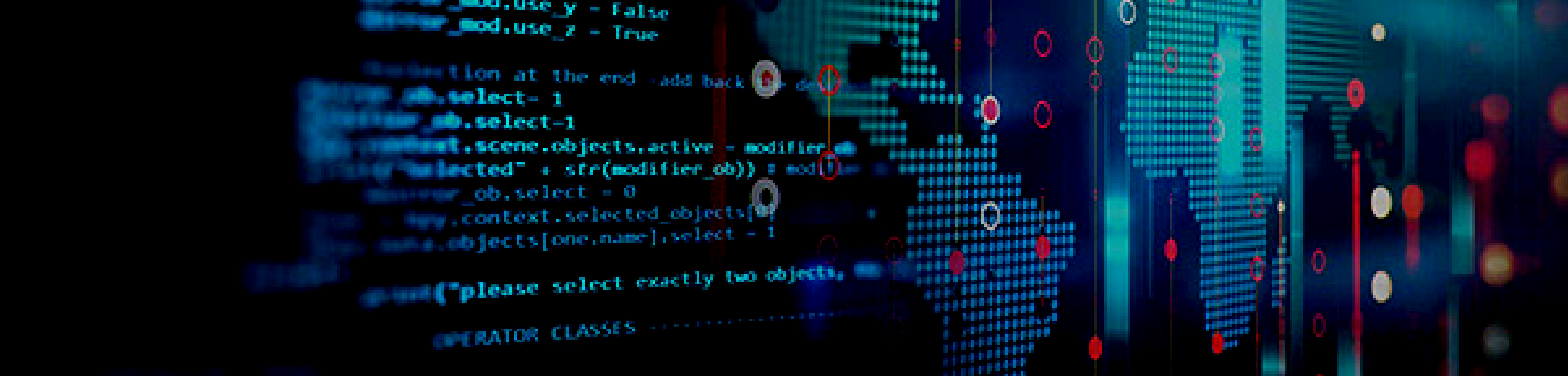
The Solution – ThreatResponder® Platform

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

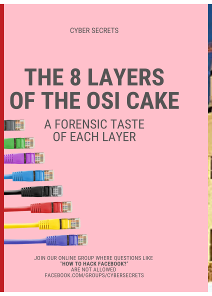


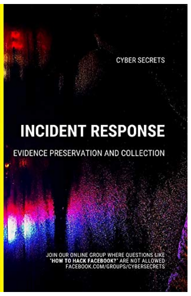
The Cyber Secrets publications on Amazon

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.

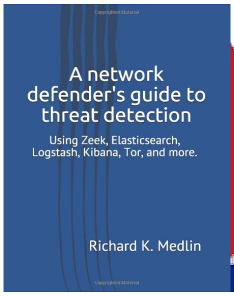
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

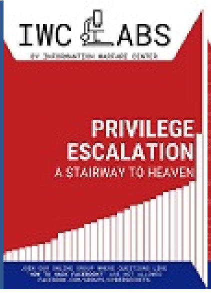
CYBER Secrets
Information Warfare Center
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training

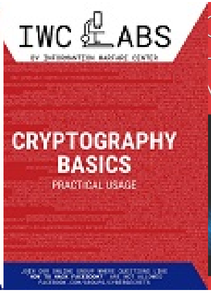


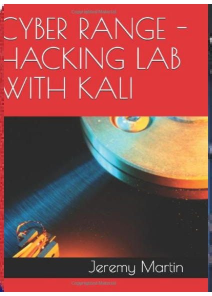


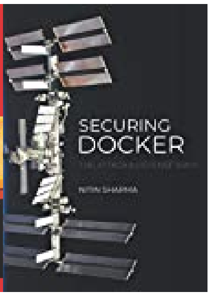
Other Publications from Information Warfare Center











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