Jun-13-22

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 13, 2022

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

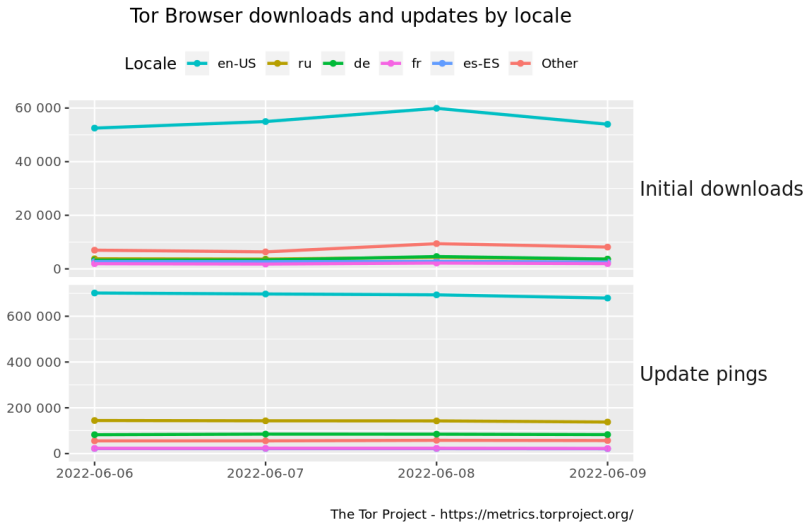
Internet Storm Center Infocon Status

The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

Index of Sections

Packet Storm Security

* U.S. Water Utilities Prime Cyberattack Target, Experts
* Since 2004, The Average American Has Had At Least 7 Data Breaches
* Apple M1 Chip Contains Hardware Vulnerability That Bypasses Memory Defense
* Potent Emotet Variant Spreads Via Stolen Email Credentials
* This Hacking Group Quietly Spied On Their Targets For 10 Years
* NASA To Figure Out How To Get Data On Unexplained Objects In The Sky
* Expect Downtime Next Week For Packet Storm
* Ministry Of Defence Acquires Government's First Quantum Computer
* Optimism Crypto Project Hopes Hacker Will Give Back $15 Million
* Russia Says West Risks Direct Military Clash Over Cyber Attacks
* New Tesla Hack Gives Thieves Their Own Personal Key
* Symantec: More Malware Operators Moving In To Exploit Follina
* 5 Key Questions The Jan. 6 Committee Will Tackle In Its Hearings
* This New Linux Malware Is Almost Impossible To Detect
* Black Basta Ransomware Teams Up With Malware Stalwart Qbot
* Maiar Exchange Taken Offline After Hacker Steals $113m
* Osmosis Blockchain Taken Offline After Hacker Steals $5m
* Data For 2 Million Patients Stolen In Largest Healthcare Breach So Far In 2022
* Feds Raid Dark Web Market Selling Data On 24 Million Americans
* NSA, FBI Warning: Hackers Are Using These Flaws To Target VPNs And Network Devices
* Spanish Court Calls CEO Of Israel's NSO Group To Testify In Spying Case
* Follina Exploited By State-Sponsored Hackers
* Attackers Use Public Exploits To Throttle Atlassian Confluence Flaw
* Microsoft Won't Say If It Will Patch Critical Windows Vuln Under Exploit
* Microsoft Seizes 41 Domains Tied To Iranian Phishing Ring

Krebs on Security

* Adconion Execs Plead Guilty in Federal Anti-Spam Case
* KrebsOnSecurity in New Netflix Series on Cybercrime
* What Counts as "Good Faith Security Research?"
* Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions
* Senators Urge FTC to Probe ID.me Over Selfie Data
* When Your Smart ID Card Reader Comes With Malware
* DEA Investigating Breach of Law Enforcement Data Portal
* Microsoft Patch Tuesday, May 2022 Edition
* Your Phone May Soon Replace Many of Your Passwords
* Russia to Rent Tech-Savvy Prisoners to Corporate IT?

Dark Reading

* CrowdStrike Introduces Humio for Falcon, Redefining Threat Hunting with Unparalleled Scale and Speed
* Symbiote Malware Poses Stealthy, Linux-Based Threat to Financial Industry
* CrowdStrike Introduces CrowdStrike Asset Graph to Help Organizations Proactively Identify and Elimina
* CrowdStrike Adds Strategic Partners to CrowdXDR Alliance and Expands Falcon XDR Capabilities
* EU Debates AI Act to Protect Human Rights, Define High-Risk Uses
* How to Blunt the Virulence of the New Ransomware
* How to Secure a High-Profile Event Like the Super Bowl
* Application Security Testing Is on the Mend With Automated Remediation
* New Linux Malware 'Nearly Impossible to Detect'
* Mitigating the Security Skills Shortage
* A Few Simple Ways to Transform Your Cybersecurity Hiring
* Artificial Intelligence and Security: What You Should Know
* How 4 Young Musicians Hacked Sheet Music to Help Fight the Cold War
* In a Quickly Evolving Landscape, CISOs Shift Their 2022 Priorities
* Design Weakness Discovered in Apple M1 Kernel Protections
* Sysdig Takes a Deeper Cut at Cloud Security
* Noname: Proactiveness Is the Name of the Game in App Security
* Lacework Blends Artificial Intelligence and Automation to Bolster Cloud Security
* Prevent Breaches and Malware With Proactive Defenses
* DigiCert Acquires DNS Made Easy

The Hacker News

* Researchers Disclose Rooting Backdoor in Mitel IP Phones for Businesses
* Quick and Simple: BPFDoor Explained
* Hello XD Ransomware Installing Backdoor on Targeted Windows and Linux Systems
* Iranian Hackers Spotted Using a new DNS Hijacking Malware in Recent Attacks
* MIT Researchers Discover New Flaw in Apple M1 CPUs That Can't Be Patched
* Researchers Find Bluetooth Signals Can be Fingerprinted to Track Smartphones
* Researchers Detail How Cyber Criminals Targeting Cryptocurrency Users
* Researchers Disclose Critical Flaws in Industrial Access Control System from Carrier
* New Privacy Framework for IoT Devices Gives Users Control Over Data Sharing
* Symbiote: A Stealthy Linux Malware Targeting Latin American Financial Sector
* Even the Most Advanced Threats Rely on Unpatched Systems
* A Decade-Long Chinese Espionage Campaign Targets Southeast Asia and Australia
* New Emotet Variant Stealing Users' Credit Card Information from Google Chrome
* Researchers Warn of Unpatched "DogWalk" Microsoft Windows Vulnerability
* U.S. Agencies Warn About Chinese Hackers Targeting Telecoms and Network Service Providers

Security Week

* Researcher Shows How Tesla Key Card Feature Can Be Abused to Steal Cars
* Cybersecurity Courses Ramp Up Amid Shortage of Professionals
* Billion-Dollar Valuations Can't Halt Layoffs at OneTrust, Cybereason
* 38 Tech Leaders Sign Cyber Resilience Pledge
* Vulnerabilities in HID Mercury Access Controllers Allow Hackers to Unlock Doors
* Chinese Cyberspy Group 'Aoqin Dragon' Targeting Southeast Asia, Australia Since 2013
* Chrome 102 Update Patches High-Severity Vulnerabilities
* InfiRay Thermal Camera Flaws Can Allow Hackers to Tamper With Industrial Processes
* Highly-Evasive Linux Malware 'Symbiote' Infects All Running Processes
* 'Follina' Vulnerability Exploited to Deliver Qbot, AsyncRAT, Other Malware
* US Details Chinese Attacks Against Telecoms Providers
* RSA Conference 2022 - Announcements Summary (Day 3)
* Threat Actors Start Exploiting Meeting Owl Pro Vulnerability Days After Disclosure
* Reports: Twitter to Provide Musk With Raw Daily Tweet Data
* DefenseStorm Raises $15 Million for Banking Security and Compliance Platform
* Snowflake Launches Cybersecurity Workload to Find Threats Across Massive Data Sets
* It Doesn't Pay to Pay: Study Finds Eighty Percent of Ransomware Victims Attacked Again
* Access Management Firm Opal Launches With $10 Million Series A Investment
* CISA Clarifies Criteria for Adding Vulnerabilities to 'Must Patch' List
* Data Breach at Shields Health Care Group Impacts 2 Million Patients
* OSINT Authentication Firm 443ID Emerges From Stealth with $8 Million Seed Funding
* Owl Labs Patches Severe Vulnerability in Video Conferencing Devices
* Cloud Data Access Firm Immuta Raises $100 Million
* RSA Conference 2022 - Announcements Summary (Day 2)
* SSNDOB Cybercrime Marketplace Taken Down by Law Enforcement
* Whistic Raises $35 Million in Series B Funding for Vendor Security Network

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Approaching Ransomware Victims Privately
* What About Password Manager Risks?
* Karakurt Adds Irritating Phone Calls to its Crimes
* 40% of CSOs say Their Organization is Not Prepared for Cyberattacks as Phishing is the Top Likely Cau
* Old Dog, New Trick: Hackers Use Logons in URLs to Bypass Email Scanners
* "Five Eyes" Nations Cybersecurity Authorities Issue Warning to MSPs of Stepped-Up Cyberattacks
* The Good, the Bad, and the Necessary State of Cyber Insurance
* Phishing Attacks Reach an All-Time High, More Than Tripling Attacks in Early 2022
* CyberheistNews Vol 12 #23 [Heads Up] Our Global Ransomware Damage Will Be More Than 265 Billion by 20
* FTC Warns that Scammers are Turning to Cryptocurrencies

ISC2.org Blog

* Just Released: 2022 (ISC)² Security Congress Agenda!
* Update on (ISC)² 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

HackRead

* Bluetooth Signals Can Be Abused To Detect and Track Smartphones
* How To Secure WordPress Website From Cyber Attacks?
* Hyperconverged Infrastructure (HCI) is Changing Data Centers
* Russian Radio Station Hacked to Broadcast Ukrainian National Anthem
* New MSDT 0-day Flaw 'DogWalk' Receives Free Unofficial Patches
* MyEasyDocs Exposed 30GB of Israeli and Indian Students PII Data
* SSNDOB Cybercrime Marketplace Seized in Intl. Coordinated Operation

Koddos

* Bluetooth Signals Can Be Abused To Detect and Track Smartphones
* How To Secure WordPress Website From Cyber Attacks?
* Hyperconverged Infrastructure (HCI) is Changing Data Centers
* Russian Radio Station Hacked to Broadcast Ukrainian National Anthem
* New MSDT 0-day Flaw 'DogWalk' Receives Free Unofficial Patches
* MyEasyDocs Exposed 30GB of Israeli and Indian Students PII Data
* SSNDOB Cybercrime Marketplace Seized in Intl. Coordinated Operation

Naked Security

* S3 Ep86: The crooks were in our network for HOW long?! [Podcast + Transcript]
* SSNDOB Market domains seized, identity theft "brokerage" shut down
* Know your enemy! Learn how cybercrime adversaries get in…
* Atlassian announces 0-day hole in Confluence Server - update now!
* Yet another zero-day (sort of) in Windows "search URL" handling
* S3 Ep85: Now THAT'S what I call a Microsoft Office exploit! [Podcast]
* 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…
* S3 Ep84: Government demand, Mozilla velocity, and Clearview fine [Podcast]

Threat Post

* U.S. Water Utilities Prime Cyberattack Target, Experts
* Potent Emotet Variant Spreads Via Stolen Email Credentials
* Feds Forced Travel Firms to Share Surveillance Data on Hacker
* Taming the Digital Asset Tsunami
* Paying Ransomware Paints Bigger Bullseye on Target's Back
* Black Basta Ransomware Teams Up with Malware Stalwart Qbot
* Cyber Risk Retainers: Not Another Insurance Policy
* Conducting Modern Insider Risk Investigations
* Follina Exploited by State-Sponsored Hackers
* Attackers Use Public Exploits to Throttle Atlassian Confluence Flaw

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

* What is behavioral analytics and when is it important?
* Where software development is headed in 2022
* JDK 19: The new features in Java 19
* Will Google's new bet on low code/no code pay off this time?
* Repatriating data and applications from the cloud
* Wasmer WebAssembly runtime adds native compilation
* What is Jamstack? The static website revolution upending web development
* "Do More with R" video tutorials
* How MongoDB's NoSQL database is encroaching on relational database turf
* Intro to JHipster: A full-stack framework for Java and JavaScript

C4ISRNET - Media for the Intelligence Age Military

* Using the 5Cs of fraud prevention in government programs
* AT&T demonstrates 5G capability for US Navy 'smart warehouse'
* Pentagon's Hicks expects real results from artificial intelligence office
* Pentagon chooses design for 'Project Pele' portable nuclear reactor prototype
* House cyber panel seeks review of delayed Air Force Link 16 upgrade
* Space Force urged to use single company for managing national security launch integration
* How Space Development Agency contractors are mitigating supply chain issues
* Lawmakers want Austin to report on progress, cost of JADC2
* House panel wants independent look at how Pentagon funds testing
* Why Martell left Lyft for Pentagon's top AI job

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.

* STANDCON CTF 2022
* TyphoonCon CTF 2022
* BSidesTLV 2022 CTF
* Google Capture The Flag 2022
* FAUST CTF 2022
* vsCTF 2022
* Crypto CTF 2022
* ImaginaryCTF 2022
* UACTF 2022
* 3kCTF-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

* 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
* COOPER Analysis Tool
* Aircrack-ng Wireless Network Tools 1.7
* Samhain File Integrity Checker 4.4.9

Kali Linux Tutorials

* Git-Dumper : A Tool To Dump A Git Repository From A Website
* Spring4Shell-Scan : A Fully Automated, Reliable, And Accurate Scanner For Finding Spring4Shell
* Spock SLAF : A Shared Library Application Firewall "SLAF"
* Sub3Suite : A Free, Open Source, Cross Platform Intelligence Gathering Tool
* Ecapture : Capture SSL/TLS Text Content Without CA Cert By eBPF
* Jfscan : A Super Fast And Customisable Port Scanner, Based On Masscan And NMap
* Ma2Tl : macOS Forensic Timeline Generator Using The Analysis Result DBs Of Mac_Apt
* DumpSMBShare : A Script To Dump Files And Folders Remotely From A Windows SMB Share
* Smap : A Drop-In Replacement For Nmap Powered By Shodan.Io
* ADReaper : A Fast Enumeration Tool For Windows Active Directory Pentesting Written In Go

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

* FluBot Android Banking Malware Shutdown - ThreatWire
* How Hackers Use DNS Spoofing to Phish Passwords (WiFi Pineapple Demo)
* Live Hacking Q&A with Kody Kinzie and Alex Lynd

The PC Security Channel [TPSC]

* SMS Scams
* Windows Defender Bypassed

Eli the Computer Guy

* What is the OSI Model
* eBeggar Wednesday - Elon Musk is a ME ME
* What is a Computer Network
* How to DESTROY a YOUTUBE CHANNEL

Security Now

* Passkeys, Take 2 - ServiceNSW Responds, Follina, Windows Search URL, UNISOC Chip Vulnerability
* DuckDuckGone? - Digital Driver's License, MS Office 0-day, GhostTouch, Vodafone TrustPiD

Troy Hunt

* Weekly Update 299

Intel Techniques: The Privacy, Security, & OSINT Show

* 265-HP Dev One with Pop!_OS
* 264-Back to Basics-Linux I

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Kik Messenger XMPP Stanza Smuggling
* WordPress Motopress Hotel Booking Lite 4.2.4 Cross Site Scripting
* Atlassian Confluence Namespace OGNL Injection
* WordPress Download Manager 3.2.42 Cross Site Scripting
* Microsoft Office Word MSDTJS Code Execution
* Backdoor.Win32.Cabrotor.10.d MVID-2022-0612 Remote Command Execution
* Ransom.Haron MVID-2022-0609 Code Execution
* Trojan-Proxy.Win32.Symbab.o MVID-2022-0610 Heap Corruption
* Trojan-Banker.Win32.Banbra.cyt MVID-2022-0611 Insecure Permissions
* Trojan-Banker.Win32.Banker.agzg MVID-2022-0608 Insecure Permissions
* Confluence OGNL Injection Proof Of Concept
* Through The Wire CVE-2022-26134 Confluence Proof Of Concept
* Confluence OGNL Injection Remote Code Execution
* Poly Studio X30 / Studio X50 / Studio X70 / G7500 Command Injection
* Poly EagleEye Director II 2.2.1.1 Command Injection / Authentication Bypass
* dbus-broker-29 Memory Corruption
* Korenix JetPort 5601V3 Backdoor Account
* Reolink E1 Zoom Camera 3.0.0.716 Configuration Disclosure
* Reolink E1 Zoom Camera 3.0.0.716 Private Key Disclosure
* Apache 2.4.50 Remote Code Execution
* 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

CXSecurity

* Atlassian Confluence Namespace OGNL Injection
* Microsoft Office Word MSDTJS Code Execution
* Confluence Data Center 7.18.0 Remote Code Execution (RCE)
* dotCMS Shell Upload
* NVIDIA Data Center GPU Manager Remote Memory Corruption
* Telesquare SDT-CW3B1 1.1.0 Command Injection
* IIPImage Remote Memory Corruption

Proof of Concept (PoC) & Exploits

Exploit Database

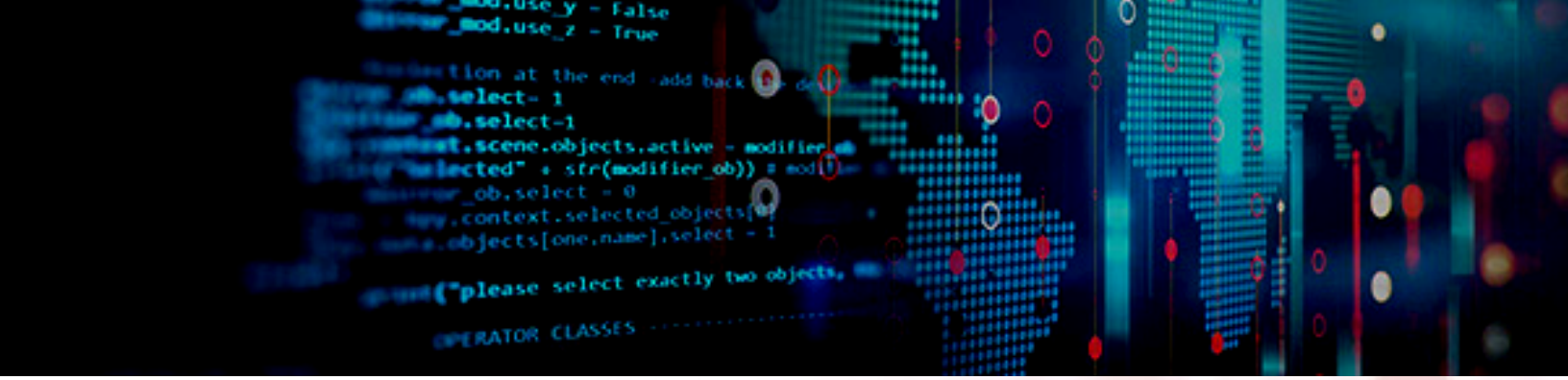
* [webapps] Confluence Data Center 7.18.0 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - 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)
* [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

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

user@yourlinux:~$ *searchsploit keyword1 keyword2*

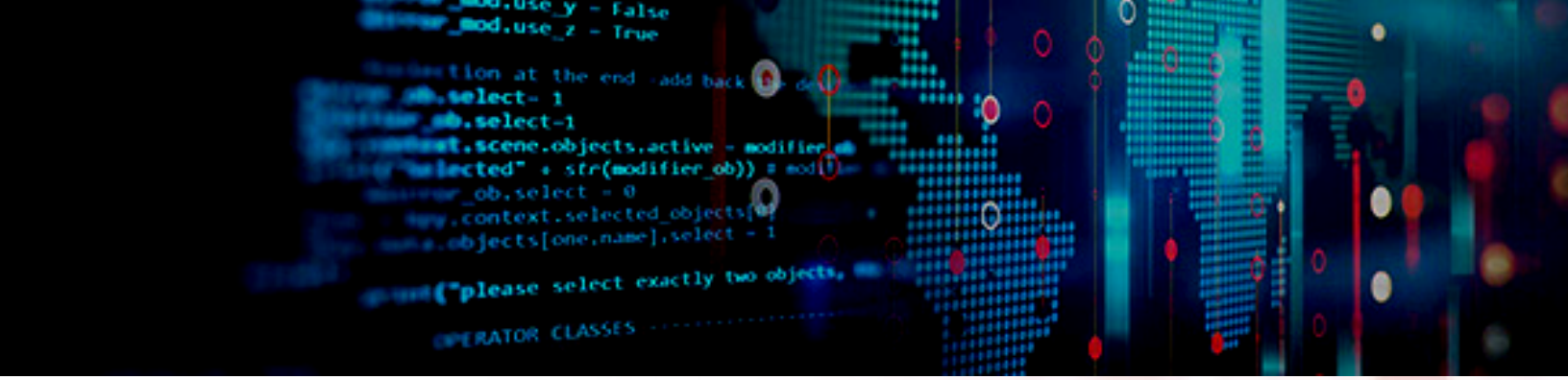
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.taxzonemymensingh.gov.bd
http://www.taxzonemymensingh.gov.bd notified by b0ogle
http://puskim.pu.go.id/itsme.html
http://puskim.pu.go.id/itsme.html notified by /Rayzky_
https://sante.gov.dz/vz.txt
https://sante.gov.dz/vz.txt notified by aDriv4
http://itaguai.rj.gov.br/kz.html
http://itaguai.rj.gov.br/kz.html notified by Mr.Kro0oz.305
http://bv.cultura.am.gov.br/license.txt
http://bv.cultura.am.gov.br/license.txt notified by aDriv4
https://taladlocal.go.th/kz.html
https://taladlocal.go.th/kz.html notified by Mr.Kro0oz.305
http://mediationbhc.gov.in
http://mediationbhc.gov.in notified by 1877
http://mja.gov.in
http://mja.gov.in notified by 1877
https://www.manage.gov.in
https://www.manage.gov.in notified by DragonForceMalaysia
https://indembassyisrael.gov.in
https://indembassyisrael.gov.in notified by DragonForceMalaysia
https://wangsomboonhospital.go.th/1975.html
https://wangsomboonhospital.go.th/1975.html notified by 1975 Team
https://scp.gob.gt/1.php
https://scp.gob.gt/1.php notified by -1
https://sikhiotown.go.th/kz.html
https://sikhiotown.go.th/kz.html notified by Mr.Kro0oz.305
https://khamthoa.go.th/kz.html
https://khamthoa.go.th/kz.html notified by Mr.Kro0oz.305
https://login-test.regione.puglia.it/mex/zct.html
https://login-test.regione.puglia.it/mex/zct.html notified by CyberTeam
https://login.regione.puglia.it/mex/zct.jsp
https://login.regione.puglia.it/mex/zct.jsp notified by CyberTeam
https://sipd.belitung.go.id/dz.php
https://sipd.belitung.go.id/dz.php notified by Gang Dz



Dark Web News

Darknet Live

Bavarian Dealer Allegedly Resold Drugs From the Darkweb

Narcotics investigators with the Memmingen Criminal Police Office arrested a 20-year-old for buying drugs on the darkweb and reselling them to local customers. Investigators with the Memmingen Criminal Police Office, assisted by the Bavarian State Criminal Police Office, raided the apartment of a 20-year-old for alleged drug crimes. During the search, police officers found several hundred LSD tabs, hundreds of ecstasy pills, marijuana, cocaine, and hundreds of grams of amphetamine and MDMA. According to an announcement from Bavarian Police, the 20-year-old has been purchasing drugs on the darkweb and reselling the drugs locally to "various buyers.” In addition to the ongoing narcotics trafficking investigation, police are investigating the suspect for counterfeiting-related crimes; during the search, police also found a fake 50-euro note.

There is a very serious bicycle patrol in Memmingen A judge at the Memmingen District Court issued a pre-trial detention order for the defendant. "The investigations, in particular regarding the delivery routes and the customers, are ongoing.” (via darknetlive.com at https://darknetlive.com/post/bavarian-man-arrested-for-reselling-darkweb-drugs/)

Feds Seized the SSNDOB Marketplace

Feds announced the seizure of the SSNDOB Marketplace. Federal law enforcement agencies seized a series of websites called the SSNDOB Marketplace, which "operated for years and were used to sell personal information, including the names, dates of birth, and Social Security numbers.” The SSNDOB Marketplace had listings for the personal information of approximately 24 million people living in the United States. The Marketplace generated more than $19 million in revenue.

Visitors of some of the seized sites are met with a seizure banner. "Identity theft can have a devastating impact on a victim's long-term emotional and financial health. Taking down the SSNDOB website disrupted I.D. theft criminals and helped millions of Americans whose personal information was compromised,” said Special Agent in Charge Darrell Waldon, IRS-CI Washington, D.C. Field Office. "Special agents with IRS-CI's D.C. Cyber Crimes Unit will continue to work with the U.S. and international law enforcement community to end these complex scams, regardless of where the money trail leads them.”

SSNDOB Marketplace | Source: notorious doxing gang "Brian Krebs” The administrators of the sites created advertisements on "darkweb criminal forums.” According to an announcement from the United States Attorney's Office for the Middle District of Florida, they provided support to customers. The administrators also took steps to conceal their identities and "thwart detection of their activities” by using servers in different countries and allowing customers to pay for services with cryptocurrency. On June 7, 2022, seizure orders were executed against the Marketplace's domain names, including ssndob.ws, ssndob.vip, ssndob.club, and blackjob.biz.

SSNDOB Marketplace | the "Brian Krebs” doxing gang "These seizures demonstrate the FBI's strong working relationship with our international partners in disrupting malicious cyber activity,” said FBI Tampa Special Agent in Charge David Walker. "Dismantling illicit marketplaces that threaten the privacy and security of the American public is a priority of the FBI.” SSNDOB Marketplace, A Series Of Websites That Listed More Than 20 Million Social Security

Numbers For Sale, Seized And Dismantled In International Operation | archive.is, archive.org, justice.gov (via darknetlive.com at https://darknetlive.com/post/feds-seized-ssndob-fraud-site/)

Alabama Man Sentenced for Buying Meth on the Darkweb

An Alabama man was sentenced to 15 months in prison for receiving methamphetamine packages through the mail. Investigators with the United States Postal Inspection Service established that 40-year-old Eric Michael Caylor, from Enterprise, Alabama, received packages of methamphetamine in 2019. During the investigation, Postal Inspectors learned that Caylor had been purchasing drugs on the darkweb using Bitcoin and having the packages mailed to his residence in Enterprise. During his plea hearing in February 2022, Caylor admitted that on May 2, 2019, he attempted to take possession of a methamphetamine package. He also admitted that he had been sharing or reselling the drugs he received. Hmmm On June 2, a federal judge sentenced Caylor to one year and three months in federal prison. After the custodial sentence, Caylor will remain on supervised release for three years. Enterprise Man Sentenced for Receiving Methamphetamine Through the Mail | archive.is, archive.org, justice.gov (via darknetlive.com at https://darknetlive.com/post/enterprise-man-sentenced-for-buying-meth/)

Where Did xChange.me Go?

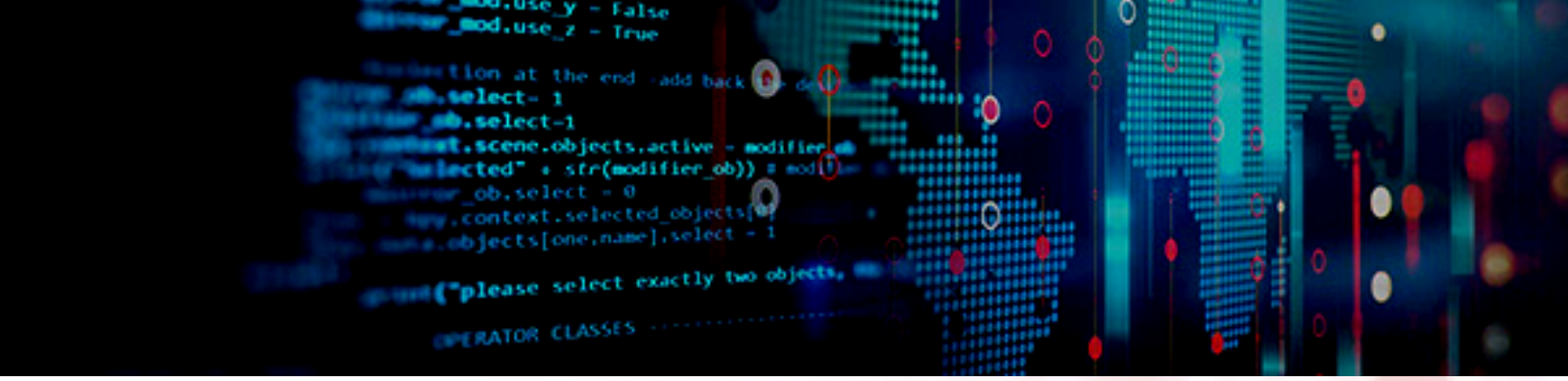
The Tor-friendly cryptocurrency exchange service xChange.me ended operations earlier this year to "rethink the direction” of the service. The xChange.me homepage before the shutdown. "Xchange.me is a modern cryptocurrency exchange software that offers fast, secure and cheap cryptocoins exchanges,” according to an archived description on the website. In April 2022, the service's official Twitter account, @xchange_me_, tweeted: "As of now, http://xchange.me's operations are suspended. The world rapidly changing around us makes us rethink the direction we want to go with our project. Please read the full message at our site, and remember to never trust any imposters you might encounter.” The xChange.me Twitter account has been inactive since this Tweet. Although the site still responded in May 2022, users could not exchange cryptocurrency. The site's homepage displayed a PGP-signed announcement about the shutdown. "These uncertain times cause Us to step back a little, and reconsider how to proceed with the xChange.me platform.” "Last few months have changed the world we live in so drastically that we cannot proceed the same way any longer. It doesn't mean that the xChange.me project is dead - we just need a little time to rethink some elements of the platform, and implement some improvements that we've been working on lately.”

"The community will remain active, as we'll share more details about our timeframe in the upcoming weeks. See you later!” "All xChange.me users! Please bear in mind, that this is the only iteration of xChange.me crypto exchanger. We've seen many imposters over the years, and can only assume that there'll be many to come. Please do not trust your funds with those fake services, as all of them are most certainly scam projects.” Signed Message support@xchange.me PGP key -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 These uncertain times cause Us to step back a little, and reconsider how to proceed with the xChange.me platform. Last few months have changed the world we live in so drastically, that we cannot proceed the same way any longer. It doesn't mean that the xChange.me project is dead - we just need a little time to rethink some elements of the platform, and implement some improvements that we've been working on lately. The community will remain active, as we'll share more details about our timeframe in the upcoming weeks. See you later! All xChange.me users! Please bear in mind, that this is the only iteration of xChange.me crypto exchanger. We've seen many imposters over the years, and can only assume that there'll be many to come. Please do not trust your funds with those fake services, as all of them are most certainly scam projects. -----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE+4P/aRCl5lJ/3ZkPFaCMnKV/PMAFAmJNSz4ACgkQFaCMnKV/
PMB5/w//RwjKJBfZnm6uao+Q8fvWBBp5147yAn1Se/kbZklKWcaHaj9ddrsU0XaB
8RxqqmLSoA2Nkaus4wobnm87HnoV2GkcQpieCM/+JRgujEUL/EgLDMjP5U3FpVHi
QSwrMIRLUSZvtpY2iBQ9OtvJxvMgQxNpfcsiPj3f+xJFR33wNuv2P60TsIlvYzxK
cRK/UN6ZYepdVQpvdsUx/E7Fan+3gQXLsfbsaIhdDx5ygBIwEhQ/LN5iaI+rdCMs
DPm9zeq1HFPNNXVWPOMPJUgLaHKdn8AwLS/yc84VkdGQdWGkAXatTCB8qeg+fZTr

+4U8h0Ak4CZT3QWbiVvSZSjIV2giKfK53IpewH9havvjEC2pjuJ0MjNXl9Y+uUmI
Kcsj+xijaOk5S9rQ05F0u4Arh89hT46kX86GYz8cT7mV0akcKamNx+JMZm/M+UbV
sFYI7uBo2V3wcSZo21ZHXjoxY3Yi/ZWaVhZMXCBjcj3r8P69uCNI19tZC/ceQcb8
aL+HFiKgHVPuud73DEnFKli87X24lBcAgwFbfojtQPc9F4TGCgjkl85leGZ0EId/
6JGx+qKZxfeQFxbPUR/8hDPUZEIXtOa/pO2gN1Z6EWLSksOnr8dSwOStOdLg7HNY
l8GzcSEIkHb5wK1kOB9+4Xcu5w+yAypimCxq+t4CXsADN1w1K/8= =hXfm -----END PGP SIGNATURE-----
(via darknetlive.com at https://darknetlive.com/post/where-did-xchangeme-go/)

Dark Web Link



Trend Micro Anti-Malware Blog

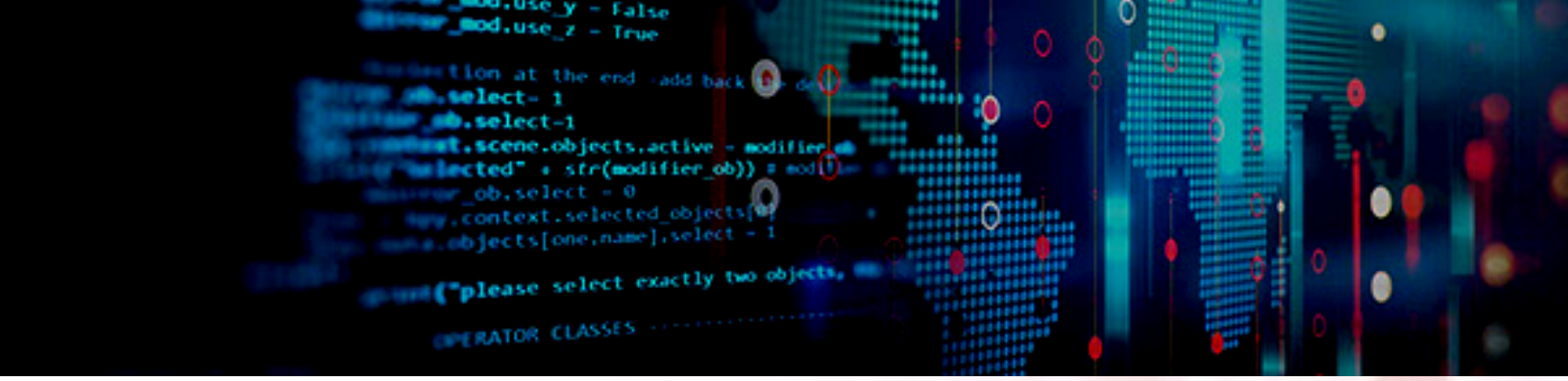
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap-Up
* [VIDEO] An Inside Look at the RSA 2022 Experience From the Rapid7 Team
* Announcing Metasploit 6.2
* [Security Nation] Phillip Maddux on HoneyDB, the Open-Source Honeypot Data Project
* Identifying Cloud Waste to Contain Unnecessary Costs
* The Hidden Harm of Silent Patches
* Evaluating the Security of an Enterprise IoT Deployment at Domino's Pizza
* Metasploit Weekly Wrap-Up
* Cybersecurity Is More Than a Checklist: Joel Yonts on Tech's Unfair Disadvantage
* Active Exploitation of Confluence CVE-2022-26134



Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* CISA Adds 36 Known Exploited Vulnerabilities to Catalog
* People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices
* Owl Labs Releases Security Updates for Meeting Owl Pro and Whiteboard Owl
* CISA Provides Criteria and Process for Updates to the KEV Catalog
* 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
* AA22-158A: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devi
* AA22-152A: Karakurt Data Extortion Group
* Vulnerability Summary for the Week of May 30, 2022
* Vulnerability Summary for the Week of May 23, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-4985-01

Red Hat Security Advisory 2022-4985-01 - New Cryostat 2.1.1 on RHEL 8 container images have been released, containing bug fixes and addressing security vulnerabilities. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2022-4956-01

Red Hat Security Advisory 2022-4956-01 - Red Hat Advanced Cluster Management for Kubernetes 2.5.0 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console—with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs and security issues. Issues addressed include privilege escalation and traversal vulnerabilities.

Ubuntu Security Notice USN-5472-1

Ubuntu Security Notice 5472-1 - It was discovered that FFmpeg would attempt to divide by zero when using Linear Predictive Coding or AAC codecs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10. It was discovered that FFmpeg incorrectly handled certain input. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 21.10.

Red Hat Security Advisory 2022-4940-01

Red Hat Security Advisory 2022-4940-01 - XZ Utils is an integrated collection of user-space file compression utilities based on the Lempel-Ziv-Markov chain algorithm, which performs lossless data compression. The algorithm provides a high compression ratio while keeping the decompression time short.

Red Hat Security Advisory 2022-4959-01

Red Hat Security Advisory 2022-4959-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR7-FP10.

Red Hat Security Advisory 2022-4941-01

Red Hat Security Advisory 2022-4941-01 - 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 2022-4957-01

Red Hat Security Advisory 2022-4957-01 - IBM Java SE version 7 Release 1 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 7 to version 7R1 SR5-FP10.

Red Hat Security Advisory 2022-4942-01

Red Hat Security Advisory 2022-4942-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-5474-1

Ubuntu Security Notice 5474-1 - It was dicovered that Varnish Cache did not clear a pointer between the handling of one client request and the next request within the same connection. A remote attacker could possibly use this issue to obtain sensitive information. It was discovered that Varnish Cache could have an assertion failure when a TLS termination proxy uses PROXY version 2. A remote attacker could possibly use this issue to restart the daemon and cause a performance loss.

Ubuntu Security Notice USN-5396-2

Ubuntu Security Notice 5396-2 - USN-5396-1 addressed a vulnerability in Ghostscript. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to access arbitrary files, execute arbitrary code, or cause a denial of

service.

Ubuntu Security Notice USN-5473-1

Ubuntu Security Notice 5473-1 - The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.50 version of the Mozilla certificate authority bundle.

Ubuntu Security Notice USN-5471-1

Ubuntu Security Notice 5471-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5469-1

Ubuntu Security Notice 5469-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5470-1

Ubuntu Security Notice 5470-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5468-1

Ubuntu Security Notice 5468-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5467-1

Ubuntu Security Notice 5467-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5466-1

Ubuntu Security Notice 5466-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5465-1

Ubuntu Security Notice 5465-1 - It was discovered that the Linux kernel did not properly restrict access to the kernel debugger when booted in secure boot environments. A privileged attacker could use this to bypass UEFI Secure Boot restrictions. Aaron Adams discovered that the netfilter subsystem in the Linux kernel did not properly handle the removal of stateful expressions in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-5464-1

Ubuntu Security Notice 5464-1 - Nils Bars discovered that e2fsprogs incorrectly handled certain file systems. A

local attacker could use this issue with a crafted file system image to possibly execute arbitrary code.

Red Hat Security Advisory 2022-4932-01

Red Hat Security Advisory 2022-4932-01 - This release of Red Hat Fuse 7.10.1 serves as a replacement for Red Hat Fuse 7.10 and includes bug fixes and enhancements, which are documented in the Release Notes document linked in the References.

Red Hat Security Advisory 2022-4929-01

Red Hat Security Advisory 2022-4929-01 - PostgreSQL is an advanced object-relational database management system.

Red Hat Security Advisory 2022-4930-01

Red Hat Security Advisory 2022-4930-01 - Twisted is an event-based framework for internet applications. Twisted Web is a complete web server, aimed at hosting web applications using Twisted and Python, but fully able to serve static pages too. Issues addressed include a HTTP request smuggling vulnerability.

Red Hat Security Advisory 2022-4924-01

Red Hat Security Advisory 2022-4924-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-5463-1

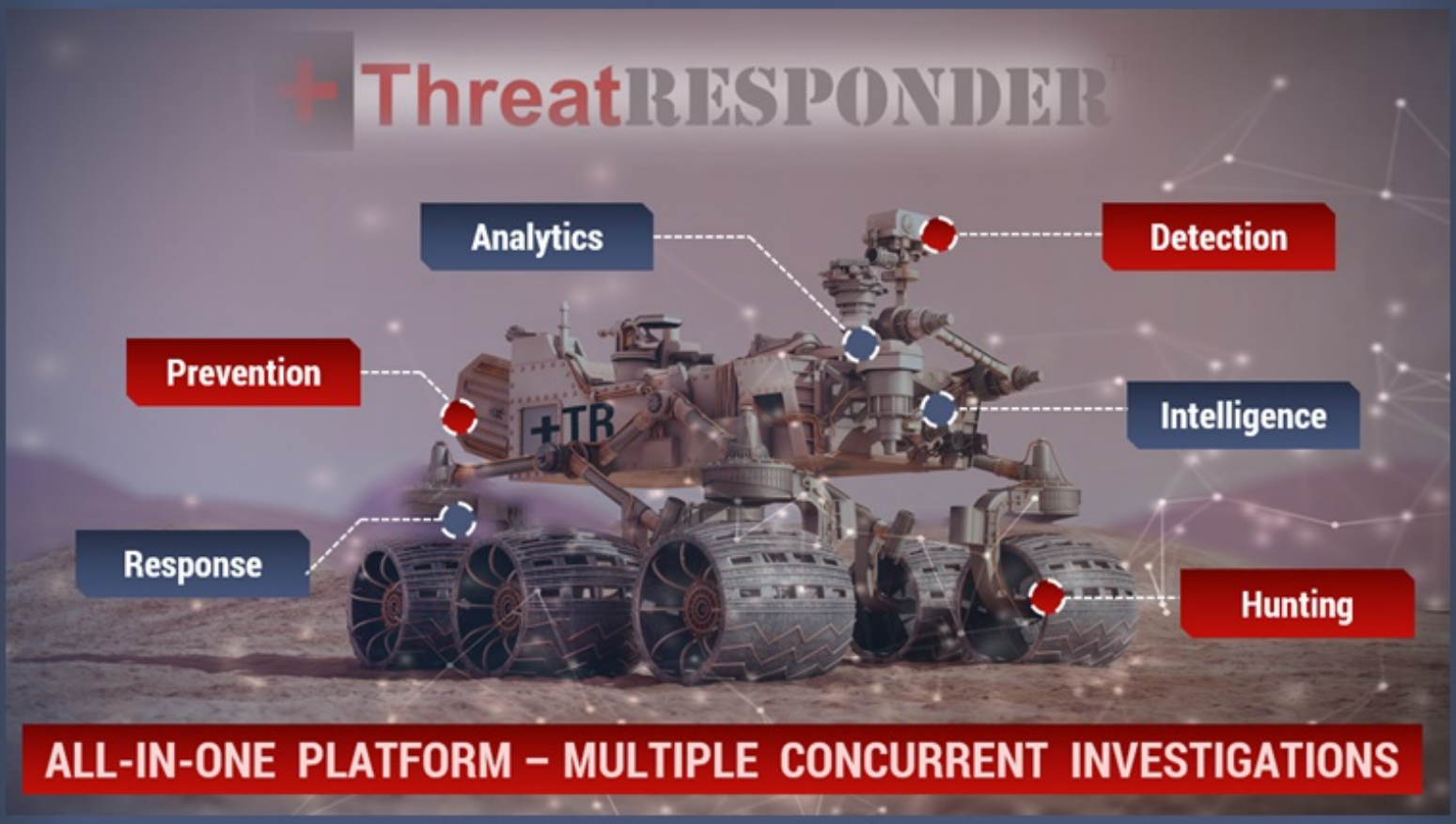
Ubuntu Security Notice 5463-1 - It was discovered that NTFS-3G incorrectly handled the ntfsck tool. If a user or automated system were tricked into using ntfsck on a specially crafted disk image, a remote attacker could possibly use this issue to execute arbitrary code. Roman Fiedler discovered that NTFS-3G incorrectly handled certain return codes. A local attacker could possibly use this issue to intercept protocol traffic between FUSE and the kernel.

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



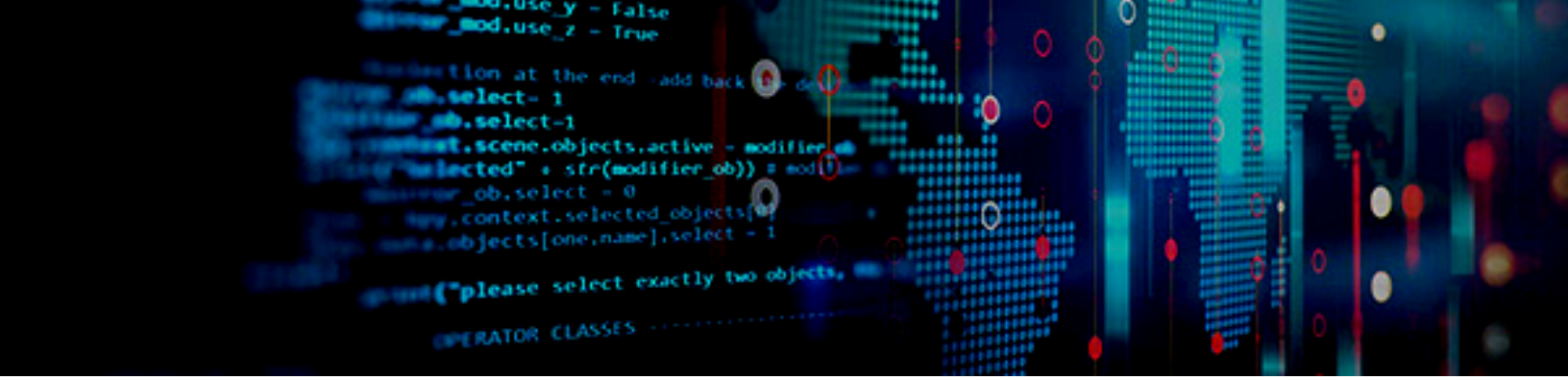
The Solution – ThreatResponder® Platform

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

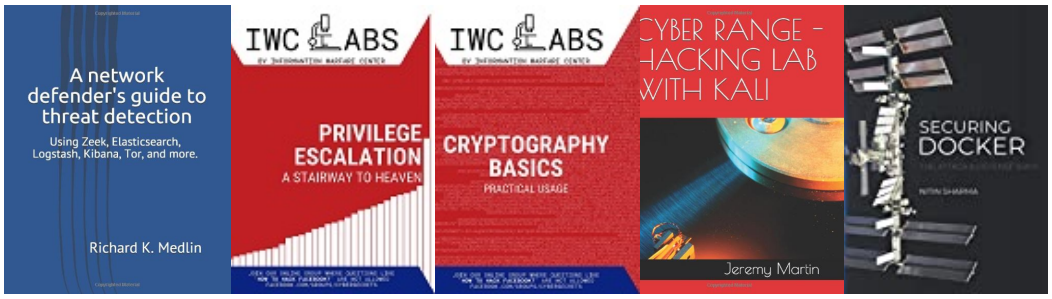


The Cyber Secrets publications on Amazon

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