Jul-26-21

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

netSecurity® INFORMATION WARFARE CENTER LINUX ARGOS APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

July 26, 2021

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

INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

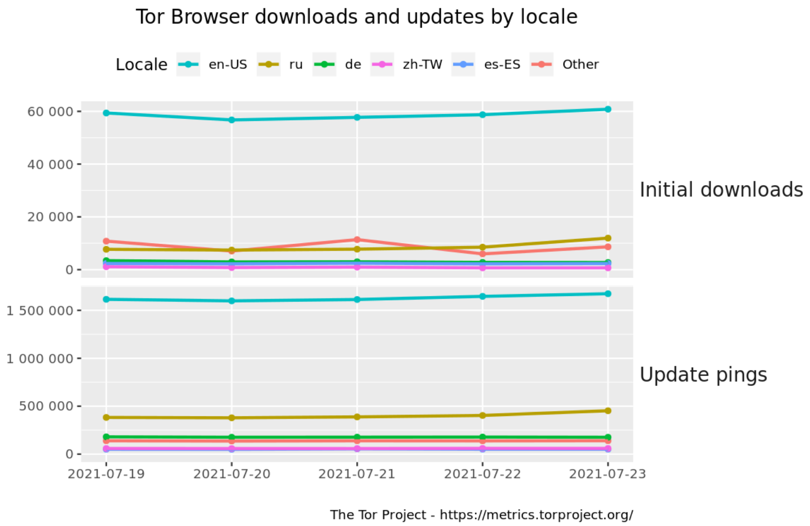
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

Just released!!! Web App Hacking: Carnage & Pwnage



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

Interesting News

* Subscribe to this OSINT resource to recieve it in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

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

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

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

- Researchers Find New Attack Vector Against Kubernetes Clusters
- Kaseya Has Acquired The REvil Ransomware Decryption Key
- Israel To Examine Whether Spyware Export Rules Should Be Tightened
- Critical Jira Flaw In Atlassian Could Lead To RCE
- NSO Will No Longer Talk To The Press About Damning Reports
- Long-Awaited Bill Would Force Breach Victims To Contact CISA
- 740 Ransomware Victims Named On Data Leak Sites In Q2 2021
- Saudi Aramco Denies Breach After Hackers Hawk Stolen Files
- NPM Package Steals Passwords Via Chrome's Account Recovery Tool
- Home And Office Routers Come Under Attack By China State Actors, France Warns
- Researchers Hid Malware Inside An AI's Neurons And It Worked Scarily Well
- Fortinet's Security Appliances Hit By Remote Code Exec Vuln
- EU Plans To Make Bitcoin Transfers More Traceable
- MacOS Being Picked Apart By $49 XLoader Data Stealer
- Why Apple's Walled Garden Is No Match For Pegasus Spyware
- TSA Announces New Pipeline Security Order
- Hundreds Of Touchscreen Ticket Machines Hit By Ransomware Attack
- China Denies Being Behind Major Microsoft Hack
- Apple Under Pressure Over iPhone Security After NSO Spyware Claims
- Chinese Hackers Hid Hacked Data In A Donald Trump Picture
- HP Patches Vulnerable Driver Lurking In Printers For 16 Years
- Hackers Got Past Windows Hello By Tricking A Webcam
- Swedish Man Sentenced For Gold-Backed Cryptocurrency Scam
- UK And White House Blame China For Microsoft Exchange Server Hack
- Facebook Catches Iranian Spies Catfishing US Military Targets

Krebs on Security

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

LATEST NEWS

Dark Reading

* Biden Administration Responds to Geopolitical Cyber Threats
* 7 Hot Cyber Threat Trends to Expect at Black Hat
* Law Firm for Ford, Pfizer, Exxon Discloses Ransomware Attack
* US Accuses China of Using Criminal Hackers in Cyber Espionage Operations
* How Gaming Attack Data Aids Defenders Across Industries
* NSO Group Spyware Used On Journalists & Activists Worldwide
* When Ransomware Comes to (Your) Town
* 7 Ways AI and ML Are Helping and Hurting Cybersecurity
* Breaking Down the Threat of Going All-In With Microsoft Security
* Researchers Create New Approach to Detect Brand Impersonation
* Recent Attacks Lead to Renewed Calls for Banning Ransom Payments
* 4 Future Integrated Circuit Threats to Watch
* How to Attract More Computer Science Grads to the Cybersecurity Field
* Attackers Exploited 4 Zero-Day Flaws in Chrome, Safari & IE
* State Dept. to Pay Up to $10M for Information on Foreign Cyberattacks
* CISA Launches New Website to Aid Ransomware Defenders
* Microsoft: Israeli Firm's Tools Used to Target Activists, Dissidents
* IoT-Specific Malware Infections Jumped 700% Amid Pandemic
* How to Bridge On-Premises and Cloud Identity
* What to Look for in an Effective Threat Hunter

The Hacker News

* BIMI: A Visual Take on Email Authentication and Security
* How to Mitigate Microsoft Windows 10, 11 SeriousSAM Vulnerability
* Microsoft Warns of LemonDuck Malware Targeting Windows and Linux Systems
* New PetitPotam NTLM Relay Attack Lets Hackers Take Over Windows Domains
* Nasty macOS Malware XCSSET Now Targets Google Chrome, Telegram Software
* Wake up! Identify API Vulnerabilities Proactively, From Production Back to Code
* Dutch Police Arrest Two Hackers Tied to "Fraud Family" Cybercrime Ring
* Kaseya Gets Universal Decryptor to Help REvil Ransomware Victims
* APT Hackers Distributed Android Trojan via Syrian e-Government Portal
* Reduce End-User Password Change Frustrations
* Oracle Warns of Critical Remotely Exploitable Weblogic Server Flaws
* Another Hacker Arrested for 2020 Twitter Hack and Massive Bitcoin Scam
* Malicious NPM Package Caught Stealing Users' Saved Passwords From Browsers
* XLoader Windows InfoStealer Malware Now Upgraded to Attack macOS Systems
* Several New Critical Flaws Affect CODESYS Industrial Automation Software

LATEST NEWS

Security Week

* 'Holy Moly!': Inside Texas' Fight Against a Ransomware Hack
* Leading Threat to Industrial Security is Not What You Think
* GitLab Releases Open Source Tool for Hunting Malicious Code in Dependencies
* Enterprises Warned of New PetitPotam Attack Exposing Windows Domains
* Threat Actors Target Kubernetes Clusters via Argo Workflows
* House Passes Several Critical Infrastructure Cybersecurity Bills
* TikTok fined â‚¬750,000 for Violating Children's Privacy
* Dutch Police Arrest Alleged Member of 'Fraud Family' Cybercrime Gang
* Cyber Risk Management Firm Safe Security Raises $33 Million
* Industrial Cybersecurity Firm SynSaber Launches With $2.5M in Seed Funding
* Estonian Botnet Operator Pleads Guilty in U.S. Court
* Kaseya Obtains Universal Decryptor for Ransomware Attack Victims
* Akamai Software Update Triggers Internet Outages
* Bug Bounty and VDP Platform YesWeHack Raises $18.8 Million
* Atlassian Patches Critical Vulnerability in Jira Data Center Products
* Google Cloud Unveils New SOC, IDS Solutions
* China-Linked APT31 Abuses Hacked Routers in Attacks, France Warns
* iOS Security Update Patches Recently Disclosed Wi-Fi Vulnerability
* CISA Details Malware Used in Attacks Targeting Pulse Secure Devices
* Is Your SecOps Solution Keeping Up?
* Dell Patches Critical Vulnerabilities in OpenManage Enterprise
* UK Man Arrested in Spain, Charged in US With Twitter Hack
* Biden to Meet Next Month With Private Sector on Cyber Issues
* Google Cloud Introduces New Zero Trust Offerings for Government

Infosecurity Magazine

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

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Mission Possible: Turning Compliance Into Tangible Security
* Remote Employees Adopt Bad Cybersecurity Habits While Working from Home
* U.S. State Department Issues a Reward for Information on Foreign Cybercriminals Targeting Critical In
* Updated Ransomware Simulator Now With 23 Latest Infection Scenarios
* Microsoft Takes Down Homoglyph Domains
* [HEADS UP] 2021 Tokyo Olympics Mean Olympic-Themed Phishing Attacks
* Mint Mobile, Porting Numbers, and Identity Theft
* Microsoft Continues to be the Top Impersonated Brand in Phishing Attacks
* The Cost and Impact of Cybercrime Can Now Be Measured in a Single Minute
* CyberheistNews Vol 11 #28 [HEADS UP] Live Phishing Attack Uses New Infection Technique to Deliver Mal

ISC2.org Blog

* The Role of Culture in Compliance
* Malware, Cybercrime and Cloud Security
* Cybersecurity Professionals to Newcomers: Focus on Vendor-Neutral Certifications
* Be The Strongest Link In Your Organization's Supply Chain
* Trending: 4,500+ Cyber Pros Enroll in Free (ISC)2 Ransomware Course in Less Than a Month in Order to

HackRead

* Defi protocol THORChain loses $8 million in "seemingly whitehat" attack
* Fake Windows 11 installers infecting devices with adware, malware
* Windows Defender update caught removing zip, exe, source code files
* WifiDemon - iPhone Wifi bug exposed devices to remote attacks
* Israeli spyware used in hacking phones of activists, journalists globally
* Misconfigured AWS bucket exposed 421GB of Artwork Archive data
* Google issues patches for Chrome flaw for Windows, Mac and Linux

Koddos

* Defi protocol THORChain loses $8 million in "seemingly whitehat" attack
* Fake Windows 11 installers infecting devices with adware, malware
* Windows Defender update caught removing zip, exe, source code files
* WifiDemon - iPhone Wifi bug exposed devices to remote attacks
* Israeli spyware used in hacking phones of activists, journalists globally
* Misconfigured AWS bucket exposed 421GB of Artwork Archive data
* Google issues patches for Chrome flaw for Windows, Mac and Linux

LATEST NEWS

Naked Security

* Windows "PetitPotam" network attack - how to protect against it
* US court gets UK Twitter hack suspect arrested in Spain
* S3 Ep42: Viruses, Nightmares, patches, rewards and scammers [Podcast]
* Windows "HiveNightmare" bug could leak passwords - here's what to do!
* Apple iPhone patches are out - no news if recent Wi-Fi bug is fixed
* S3 Ep41: Crashing iPhones, PrintNightmares, and Code Red memories [Podcast]
* More PrintNightmare: "We TOLD you not to turn the Print Spooler back on!"
* Want to earn $10 million? Snitch on a cybercrook!
* The Code Red worm 20 years on - what have we learned?
* Home delivery scams get smarter - don't get caught out

Threat Post

* The True Impact of Ransomware Attacks
* Discord CDN and API Abuses Drive Wave of Malware Detections
* 5 Steps to Improving Ransomware Resiliency
* FIN7's Liquor Lure Compromises Law Firm with Backdoor
* Kaseya Obtains Universal Decryptor for REvil Ransomware
* FBI: Cybercriminals Eyeing Broadcast Disruption at Tokyo Olympics
* Phish Swims Past Email Security With Milanote Pages
* Critical Jira Flaw in Atlassian Could Lead to RCE
* Industrial Networks Exposed Through Cloud-Based Operational Tech
* Apple Issues Urgent iPhone Updates; None for Pegasus Zero-Day

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

* How AI Will Transform Data Security
* API Abuse Is a Data Security Issue Here to Stay
* Thriving in Chaos: How Cyber Resilience Works
* This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered
* Beyond Ransomware: Four Threats Facing Companies Today
* How to Fix the Big Problems With Two-Factor and Multifactor Authentication
* Avoid Blind Spots: Is Your Incident Response Team Cloud Ready?
* How Data Discovery and Zero Trust Can Help Defend Against a Data Breach
* Two (or More) Is Better Than One: Digital Twin Tech for Cybersecurity
* FragAttacks: Everything You Need to Know

InfoWorld

* The uber-importance of docs
* 5 takeaways from recent agile and devops reports
* TypeScript 4.4 brings performance boosts
* SolidJS creator: JavaScript innovation isn't slowing down
* The importance of classifying analytics
* 3 creative ways to obtain cloud talent
* Microsoft sunsets Xamarin toolkit
* "Do More with R" video tutorials
* How to run R in Visual Studio Code
* An introduction to time series forecasting

C4ISRNET - Media for the Intelligence Age Military

* Israel pushes military digital transformation in the age of 'artificial intelligence war'
* Lawmakers want Pentagon to map supply chain risks, cut China products
* Space Force delivers software upgrades to satellite communications system
* Submarine leaders want to tap into JADC2 network without giving away their position
* To afford next-gen combat aircraft, the US Air Force will make cuts to ISR inventory
* National Reconnaissance Office wants a more distributed architecture
* Marines adopt DARPA force design software to build the Corps for future fight
* Path for DARPA tech to become part of military's JADC2 enterprise still unclear
* Planning for a rainy day in space: How America can build a resilient space future
* US Army matures tactical tools for trustworthy data, cyber op action plans

The Hacker Corner

Conferences

* Marketing For Cybersecurity
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* An EPYC escape: Case-study of a KVM breakout
* Fuzzing iOS code on macOS at native speed

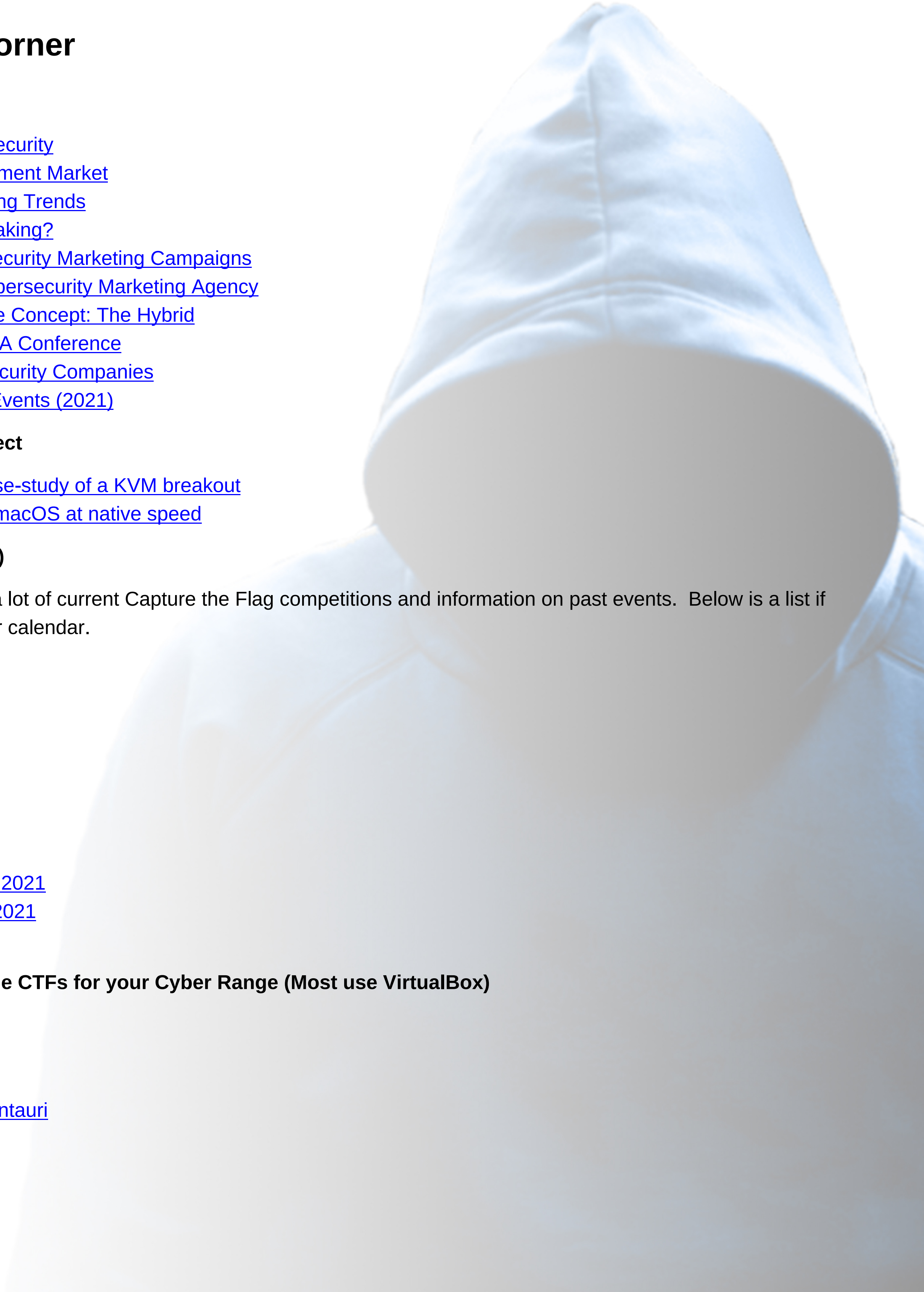
Capture the Flag (CTF)

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.

* Crypto CTF 2021
* UIUCTF 2021
* RTLxHA CTF 21
* RaRCTF 2021
* TSG CTF 2021
* BSides Noida CTF
* InCTF 2021
* Really Awesome CTF 2021
* Hacker's Playground 2021
* corCTF 2021

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

* HackathonCTF: 2
* Hackable: II
* VulnCMS: 1
* hacksudo: ProximaCentauri
* Tech_Supp0rt: 1



Tools & Techniques

Packet Storm Security Tools Links

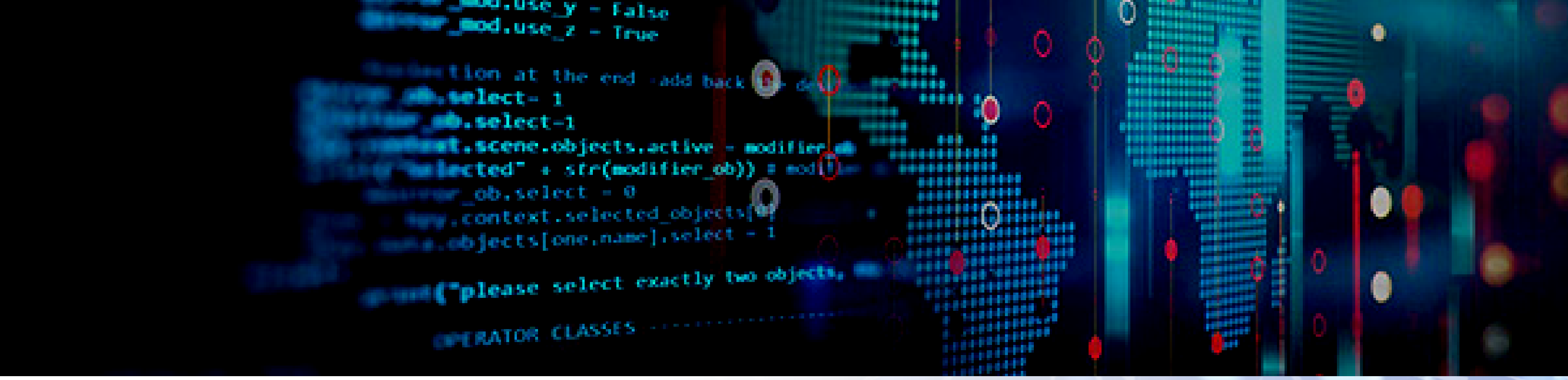
* Logwatch 7.5.6
* Lynis Auditing Tool 3.0.6
* American Fuzzy Lop plus plus 3.14c
* Hashcat Advanced Password Recovery 6.2.3 Source Code
* Hashcat Advanced Password Recovery 6.2.3 Binary Release
* Wireshark Analyzer 3.4.7
* UFONet 1.7
* Global Socket 1.4.33
* Zeek 4.0.3
* Stegano 0.9.9

Kali Linux Tutorials

* Regexploit : Find Regular Expressions Which Are Vulnerable To ReDoS (Regular Expression Denial Of Ser
* Cyberstalkers: How to Protect Yourself
* Data Breaches Aren't Going Away: Everything You Need to Know to Protect Your Business
* Orbitaldump : A Simple Multi-Threaded Distributed SSH Brute-Forcing Tool Written In Python
* ARTIF : An Advanced Real Time Threat Intelligence Framework To Identify Threats And Malicious Web Tra
* JWTweak : Detects The Algorithm Of Input JWT Token And Provide Options To Generate The New JWT Token
* DNSrr : A Tool Written In Bash, Used To Enumerate All The Juicy Stuff From DNS
* Whisker : A C# Tool For Taking Over Active Directory User And Computer Accounts By Manipulating Their
* The-Bastion : Authentication, Authorization, Traceability And Auditability For SSH Accesses
* DNSStager : Hide Your Payload In DNS

GBHackers Analysis

* Critical Oracle Weblogic Flaw Let Remote Attacker Take Control of The System
* Millions of Printers Worldwide Vulnerable To The 16-Year-Old Bug
* Russian APT Hackers Launched A Mass Global Brute Force Attack to Hack Enterprise & Cloud Networks
* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices
* 5 Key Phases of Ethical Hacking



Weekly Cyber Security Video and Podcasts

SANS DFIR

* Getting started in DFIR: Testing 1,2,3
* DFIR Summit 2021
* STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign
* FOR585: Smartphone Forensic Analysis In-Depth

Defcon Conference

* DEF CON China Party 2021 - Keynote Interview Excerpt - Steve Wozniak, The Dark Tangent
* DEF CON China Party 2021 - Whispers Among the Stars - James Pavur
* DEF CON China Party 2021- Wall of Sheep: Hilarious Fails and the Sheep Behind Them - Riverside
* DEF CON China Party - Cooper Quintin- Detecting Fake 4G Base Stations in Real Time

Hak5

* HakByte: Use Android Studio to Learn Android App Security Part 3
* A Look at Glytch's Pocket Hardware Hacking Kit
* HakByte: Use Android Studio to Learn Android App Security Part 2

The PC Security Channel [TPSC]

* Discord Ransomware
* Windows 11: Better Security?

Eli the Computer Guy

* Hacking Introduction
* eBeggar Wednesday - ALPHA MALE Edition
* "Easy" Computer Speech Recognition with Azure Cognitive Services and Python
* How to Become a YouTuber

Security Now

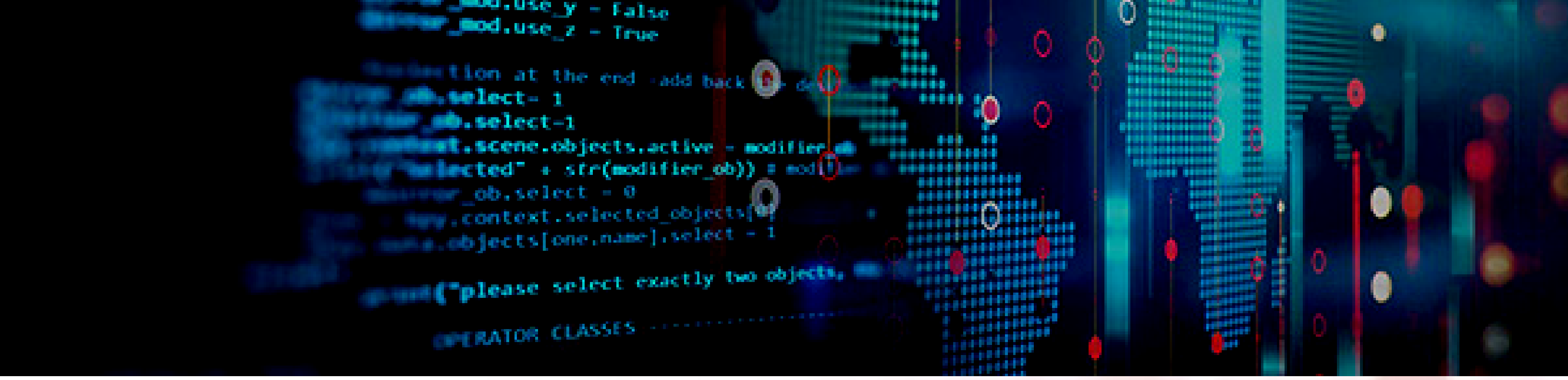
* REvil Vanishes! - Chrome Zero-Day Vulnerability, iOS WiFi SSID Bug, Patch Tuesday Review
* REvil's Clever Crypto - Microsoft Fails to Patch PrintNightmare & Sodinokibi Malware's Crypto Design

Troy Hunt

* Weekly Update 253

Intel Techniques: The Privacy, Security, & OSINT Show

* 226-Personal Ransomware Exposure
* 225-Lessons Learned This Week


_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
"elected" + str(modifier_ob)) # modi
_ob.select = 0
context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Trend Micro Anti-Malware Blog

* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

RiskIQ

* Taking a Closer Look at a Malicious Infrastructure Mogul
* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think
* MobileInter: A Popular Magecart Skimmer Redesigned For Your Phone
* DarkSide is Standing Down, But Its Affiliates Live On

FireEye

* Metasploit Wrap-Up
* What's New in InsightAppSec and tCell: Q2 2021 in Review
* [Security Nation] Brian Honan on creating Ireland's first CERT
* Microsoft SAM File Readability CVE-2021-36934: What You Need to Know
* Grow Your Career at Rapid7: North America Sales
* [The Lost Bots] Episode 1: External Threat Intelligence
* Rapid7 + XDR: Security that Moves as Fast as Your Business
* Rapid7 Acquires IntSights to Tackle the Expanding Threat Landscape
* Accelerating SecOps and Emergent Threat Response with the Insight Platform
* What's New in InsightVM: Q2 2021 in Review

Proof of Concept (PoC) & Exploits

Packet Storm Security

* ElasticSearch 7.13.3 Memory Disclosure
* Microsoft SharePoint Server 2019 Remote Code Execution
* WordPress Simple Post 1.1 Cross Site Scripting
* Sage X3 Administration Service Authentication Bypass / Command Execution
* WordPress Backup Guard Authenticated Remote Code Execution
* Sequoia: A Deep Root In Linux's Filesystem Layer
* Ampache 4.4.2 Cross Site Scripting
* CSZ CMS 1.2.9 Arbitrary File Deletion
* News Portal Project 3.1 SQL Injection
* Online Shopping Portal 3.1 SQL Injection
* Vehicle Parking Management System 1.0 SQL Injection
* Vehicle Parking Management System 1.0 Cross Site Scripting
* KevinLAB BEMS 1.0 Authenticated File Path Traversal / Information Disclosure
* KevinLAB BEMS 1.0 Unauthenticated SQL Injection / Authentication Bypass
* KevinLAB BEMS 1.0 Undocumented Backdoor Account
* Dell OpenManage Enterprise Hardcoded Credentails / Privilege Escalation / Deserialization
* Microsoft Windows WFP Default Rules AppContainer Capability Bypass Privilege Escalation
* Webmin 1.973 Cross Site Request Forgery
* WordPress KN Fix Your Title 1.0.1 Cross Site Scripting
* Backdoor.Win32.IRCBot.gen Remote Command Execution
* WordPress Mimetic Books 0.2.13 Cross Site Scripting
* Trojan-Spy.Win32.SpyEyes.hqd Insecure Permissions
* Trojan-Spy.Win32.SpyEyes.abdb Insecure Permissions
* Dolibarr ERP/CRM 10.0.6 Login Brute Forcer
* Backdoor.Win32.Agent.bjev Insecure Permissions

CXSecurity

* Linux Kernel 2.6.19
* Microsoft SharePoint Server 2019 Remote Code Execution (2)
* ElasticSearch 7.13.3 Memory Disclosure
* Sage X3 Administration Service Authentication Bypass / Command Execution
* Dell OpenManage Enterprise Hardcoded Credentails / Privilege Escalation / Deserialization
* Linux Kernel Netfilter Heap Out-Of-Bounds Write
* ForgeRock Access Manager/OpenAM 14.6.3 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

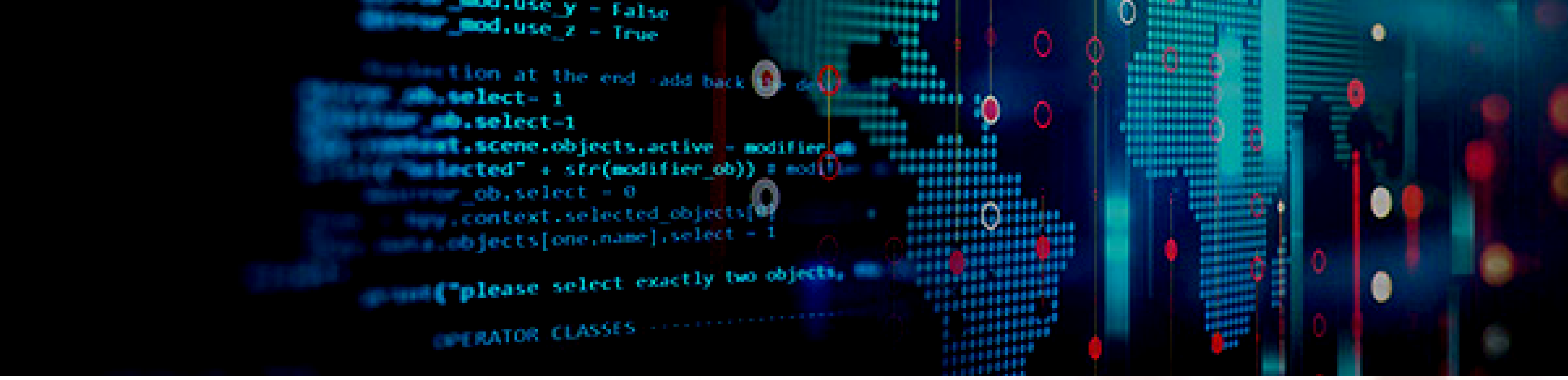
* [webapps] XOS Shop 1.0.9 - 'Multiple' Arbitrary File Deletion (Authenticated)
* [webapps] NoteBurner 2.35 - Denial Of Service (DoS) (PoC)
* [dos] Leawo Prof. Media 11.0.0.1 - Denial of Service (DoS) (PoC)
* [webapps] Elasticsearch ECE 7.13.3 - Anonymous Database Dump
* [webapps] Microsoft SharePoint Server 2019 - Remote Code Execution (2)
* [webapps] WordPress Plugin Simple Post 1.1 - 'Text field' Stored Cross-Site Scripting (XSS)
* [webapps] ElasticSearch 7.13.3 - Memory disclosure
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Arbitrary File Deletion
* [webapps] KevinLAB BEMS 1.0 - File Path Traversal Information Disclosure (Authenticated)
* [webapps] KevinLAB BEMS 1.0 - Unauthenticated SQL Injection / Authentication Bypass
* [remote] KevinLAB BEMS 1.0 - Undocumented Backdoor Account
* [webapps] Webmin 1.973 - 'run.cgi' Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin KN Fix Your Title 1.0.1 - 'Separator' Stored Cross-Site Scripting (XSS)
* [webapps] PEEL Shopping 9.3.0 - 'id' Time-based SQL Injection
* [webapps] Dolibarr ERP/CRM 10.0.6 - Login Brute Force
* [webapps] WordPress Plugin Mimetic Books 0.2.13 - 'Default Publisher ID field' Stored Cross-Site Scri
* [webapps] WordPress Plugin LearnPress 3.2.6.8 - Privilege Escalation
* [webapps] WordPress Plugin LearnPress 3.2.6.7 - 'current_items' SQL Injection (Authenticated)
* [remote] Aruba Instant (IAP) - Remote Code Execution
* [local] Linux Kernel 2.6.19
* [remote] Aruba Instant 8.7.1.0 - Arbitrary File Modification
* [webapps] Seagate BlackArmor NAS sg2000-2000.1331 - Command Injection
* [webapps] ForgeRock Access Manager/OpenAM 14.6.3 - Remote Code Execution (RCE) (Unauthenticated)
* [local] Argus Surveillance DVR 4.0 - Weak Password Encryption

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
```

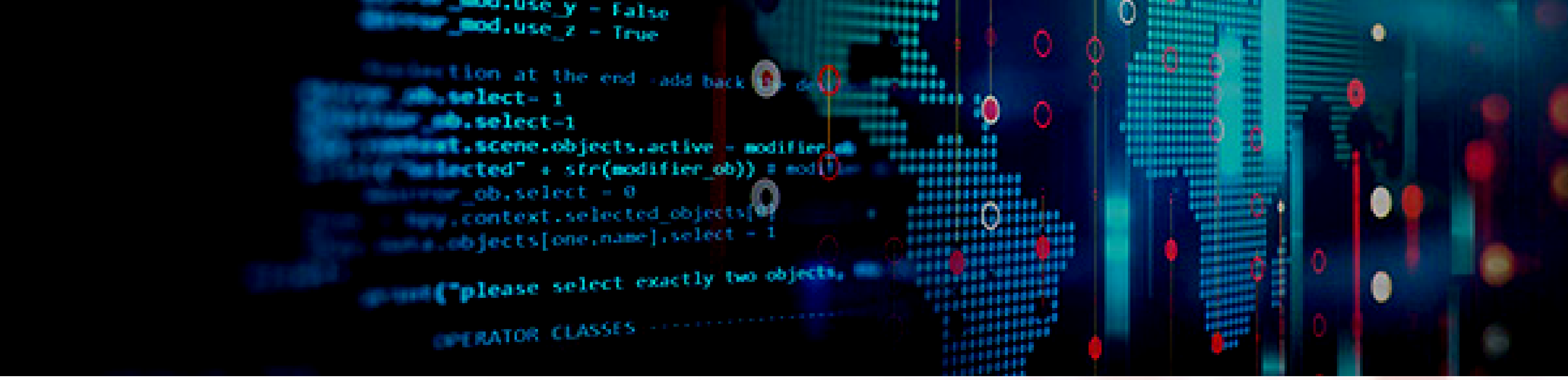
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

Unfortunately, at the time of this report, the Zone-H.org last hacked feed was not availible.



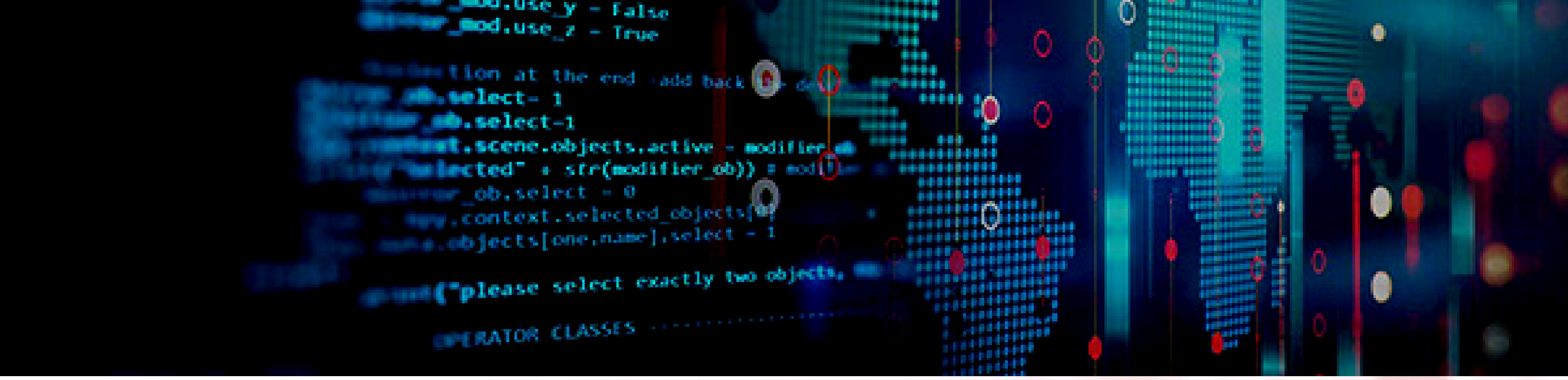
Dark Web News

Darknet Live

Ethereum Dev Violated Bail Conditions by Signing into Coinbase
Former Ethereum Foundation member Virgil Griffith has been taken into custody after violating the terms of his bail by signing into his Coinbase account. (via darknetlive.com)
Jury Convicts "XanaxKing2" of Selling Fentanyl Analogues
A jury convicted a California man of conspiring and manufacturing and distributing fentanyl pills through the darkweb. (via darknetlive.com)
Student Sentenced for Reselling Drugs Sourced on the Darkweb
A student at the University of Chester was sentenced to prison for buying drugs on the darkweb and selling them locally. (via darknetlive.com)
Dream Vendor "FatSam" Avoids Prison in Drug Case
A judge in the U.K. sentenced a Dream Market vendor to time served and community service instead of time behind bars. (via darknetlive.com)

Dark Web Link

Crypto Short & Long: Crypto Needs Extra Than Vc Interest
Correcting misconceptions about institutional interest in crypto and why Circle's IPO could bring more regulatory clarity to stable coins in the United States. So the consumer price index finally showed signs of inflation this week. And it came in hot, with year-over-year inflation in the United States hitting 5.4 percent, well above the Federal Reserve's [...] The post Crypto Short & Long: Crypto Needs Extra Than Vc Interest appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Does Bitcoin Have The Scope To Exchange Traditional Currencies?
Let's take a look at why Bitcoin will prosper as a real currency. The first is that it is independent of any central entity in terms of maintaining its value, being regulated, or being accepted by others. Bitcoin's security is based solely on math and cryptography, allowing users to maintain complete control over their funds [...] The post Does Bitcoin Have The Scope To Exchange Traditional Currencies? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Profiteering, Fraud, Discrimination - Jackson Palmer, Dogecoin Co-Founder Discloses Dark Side Of Cryptocurrency
Jackson Palmer, co-founder of Dogecoin,knocked the cryptocurrency industry and stated that he would no longer participate in it. In a series of tweets, he explained his decision, calling cryptocurrency &#8220;an integrallyhyper-capitalistic, right-wing, technology.&#8221; It's &#8220;built primarily to intensify the wealth of its supporters through a mixture of tax avoidance, reduced controlling oversight, and enforced scarcity [...] The post Profiteering, Fraud, Discrimination &mdash; Jackson Palmer, Dogecoin Co-Founder Discloses Dark Side Of Cryptocurrency appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* &#8239;Cisco Releases Security Updates
* Drupal Releases Security Updates
* 2021 CWE Top 25 Most Dangerous Software Weaknesses
* Malware Targeting Pulse Secure Devices
* Adobe Releases Security Updates for Multiple&#8239;Products&#8239;
* Apple Releases Security Updates
* Google Releases Security Updates for Chrome
* Significant Historical Cyber-Intrusion Campaigns Targeting ICS
* AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013
* AA21-200B: Chinese State-Sponsored Cyber Operations: Observed TTPs
* Vulnerability Summary for the Week of July 12, 2021
* Vulnerability Summary for the Week of July 5, 2021

Zero Day Initiative Advisories

ZDI-CAN-14486: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14396: Foxit
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'ZhangJiaxing(@r0fm1a) from Codesafe Team of Legendsec at Qi'anxin Group' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14206: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14458: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14222: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14272: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'ZhangJiaxing(@r0fm1a) from Codesafe Team of Legendsec at Qi'anxin Group' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14496: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14497: Oracle

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14491: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14521: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14502: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14506: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14494: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14487: Oracle

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14509: Oracle

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14523: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14493: Oracle
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14490: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14524: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14492: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14501: Oracle
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14507: Oracle
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14489: Oracle
A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-14505: Oracle
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-23, 3 days ago. The vendor is given until 2021-11-20 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Apple Security Advisory 2021-07-21-6

Apple Security Advisory 2021-07-21-6 - tvOS 14.7 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-07-21-5

Apple Security Advisory 2021-07-21-5 - watchOS 7.6 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-07-21-4

Apple Security Advisory 2021-07-21-4 - Security Update 2021-005 Mojave addresses code execution, double free, information leakage, integer overflow, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2021-07-21-3

Apple Security Advisory 2021-07-21-3 - Security Update 2021-004 Catalina addresses buffer overflow, code execution, double free, information leakage, integer overflow, out of bounds read, and out of bounds write vulnerabilities.

Apple Security Advisory 2021-07-21-2

Apple Security Advisory 2021-07-21-2 - macOS Big Sur 11.5 addresses buffer overflow, bypass, code execution, information leakage, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Apple Security Advisory 2021-07-21-1

Apple Security Advisory 2021-07-21-1 - iOS 14.7 and iPadOS 14.7 addresses buffer overflow, bypass, code execution, integer overflow, out of bounds read, out of bounds write, and use-after-free vulnerabilities.

Gentoo Linux Security Advisory 202107-52

Gentoo Linux Security Advisory 202107-52 - Multiple vulnerabilities have been found in Apache Velocity, the worst of which could result in the arbitrary execution of code. Versions less than 2.3 are affected.

Gentoo Linux Security Advisory 202107-51

Gentoo Linux Security Advisory 202107-51 - Multiple vulnerabilities have been found in IcedTeaWeb, the worst of which could result in the arbitrary execution of code. Versions less than 1.8.4-r1 are affected.

Asterisk Project Security Advisory - AST-2021-009

Depending on the timing, it is possible for Asterisk to crash when using a TLS connection if the underlying socket parent/listener gets destroyed during the handshake.

Asterisk Project Security Advisory - AST-2021-008

If the IAX2 channel driver receives a packet that contains an unsupported media format it can cause a crash to occur in Asterisk.

Asterisk Project Security Advisory - AST-2021-007

When Asterisk receives a re-INVITE without SDP after having sent a BYE request a crash will occur. This occurs due to the Asterisk channel no longer being present while code assumes it is.

Ubuntu Security Notice USN-5021-1

Ubuntu Security Notice 5021-1 - Harry Sintonen and Tomas Hoger discovered that curl incorrectly handled TELNET connections when the -t option was used on the command line. Uninitialized data possibly containing sensitive information could be sent to the remote server, contrary to expectations. Harry Sintonen discovered that curl incorrectly reused connections in the connection pool. This could result in curl reusing the wrong connections. Various other issues were also addressed.

Red Hat Security Advisory 2021-2866-01

Red Hat Security Advisory 2021-2866-01 - The ovirt-engine package provides the Red Hat Virtualization Manager, a centralized management platform that allows system administrators to view and manage virtual machines. The Manager provides a comprehensive range of features including search capabilities, resource management, live migrations, and virtual infrastructure provisioning. The ovirt-ansible-hosted-engine-setup package provides an Ansible role for deploying Red Hat Virtualization Hosted-Engine.

Red Hat Security Advisory 2021-2865-01

Red Hat Security Advisory 2021-2865-01 - The ovirt-engine package provides the manager for virtualization environments. This manager enables admins to define hosts and networks, as well as to add storage, create VMs and manage user permissions. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-2736-01

Red Hat Security Advisory 2021-2736-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-2779-01

Red Hat Security Advisory 2021-2779-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for Windows serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2780-01

Red Hat Security Advisory 2021-2780-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2777-01

Red Hat Security Advisory 2021-2777-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Red Hat Security Advisory 2021-2778-01

Red Hat Security Advisory 2021-2778-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section.

Gentoo Linux Security Advisory 202107-50

Gentoo Linux Security Advisory 202107-50 - A vulnerability in Singularity could result in remote code execution. Versions less than 3.7.4 are affected.

Gentoo Linux Security Advisory 202107-49

Gentoo Linux Security Advisory 202107-49 - Multiple vulnerabilities have been found in Chromium and Google Chrome, the worst of which could result in the arbitrary execution of code. Versions less than 91.0.4472.164 are affected.

Ubuntu Security Notice USN-5020-1

Ubuntu Security Notice 5020-1 - It was discovered that Ruby incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. It was discovered that Ruby incorrectly handled certain inputs. An attacker could possibly use this issue to conduct port scans and service banner extractions. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. Various other issues were also addressed.

Red Hat Security Advisory 2021-2737-01

Red Hat Security Advisory 2021-2737-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4336-2

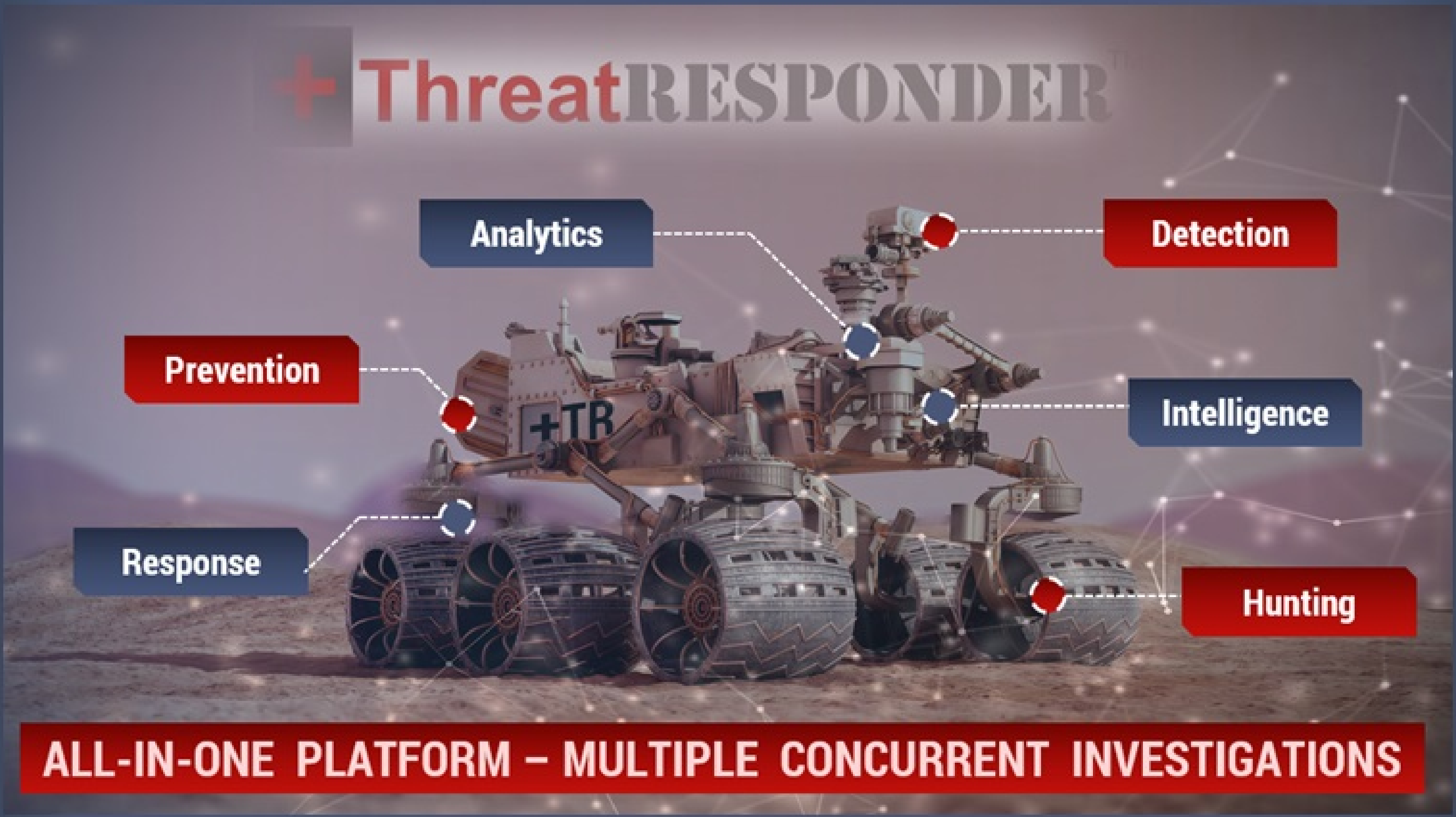
Ubuntu Security Notice 4336-2 - USN-4336-1 fixed several vulnerabilities in GNU binutils. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that GNU binutils contained a large number of security issues. If a user or automated system were tricked into processing a specially-crafted file, a remote attacker could cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

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



ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

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

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

CSI Linux is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux has been rebuilt from the ground up on Ubuntu 20.04 LTS to provide long term support for the backend OS and has become a powerful Investigation environment that comes in both the traditional Virtual Machine option and a bootable image that you can install onto an external drive or USB to use as your daily driver or DFIR triage drive. The SIEM has been given an evolution boost with capability while being encapsulated into a Docker container

CSI Linux Tutorials:

PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

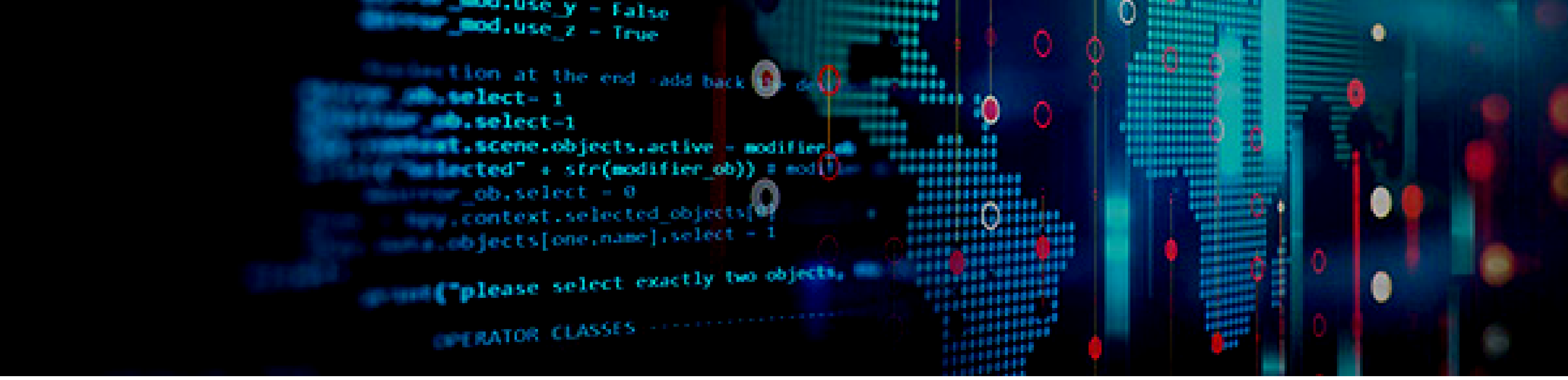
Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

* Amazon FireTV App - amzn.to/30oiUpE
* YouTube - youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg

Printed / Kindle Publications:

* Cyber Secrets on Amazon - amzn.to/2UuIG9B



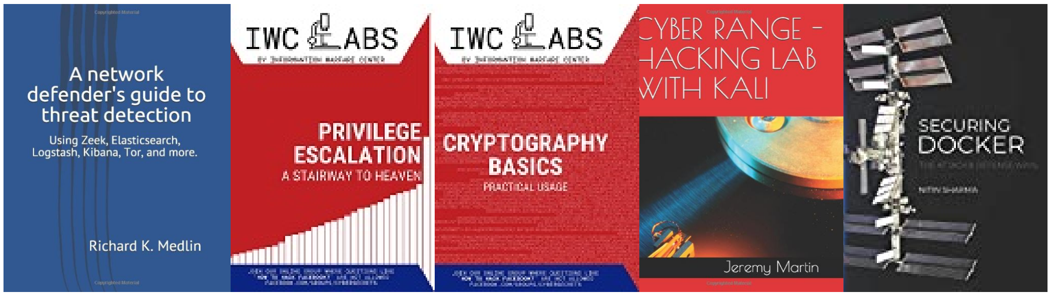
The Cyber Secrets publications on Amazon

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
What's Inside?
Threat Intelligence & Training
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE EVIDENCE PRESERVATION AND COLLECTION

Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin
IWC LABS
PRIVILEGE ESCALATION A STAIRWAY TO HEAVEN
IWC LABS
CRYPTOGRAPHY BASICS PRACTICAL USAGE
CYBER RANGE - HACKING LAB WITH KALI
Jeremy Martin
SECURING DOCKER
NITIN SHARMA

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