Jun-28-21

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

June 28, 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

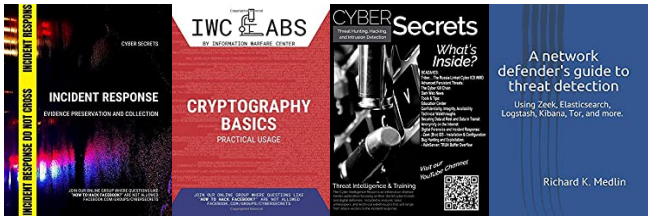
Internet Storm Center Infocon Status

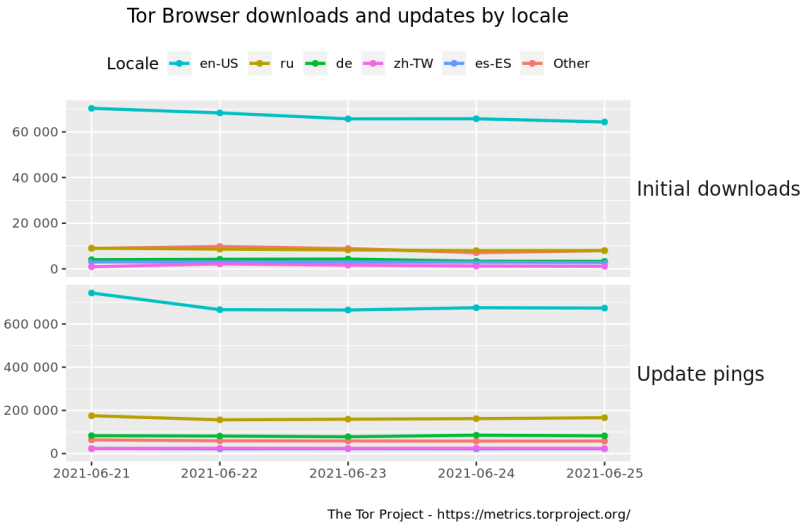
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* 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

Packet Storm Security

* Google Tracking Cookies Ban Delayed Until 2023
* Disconnect Your WD My Book Live NAS Off The Internet Now
* How Hackers Are Using Gamers To Become Crypto-Rich
* FIN7 Hacking Group Member Lands Seven Year Prison Term
* Hackers Use Fake Call Center To Trick Victims Into Installing Ransomware
* US Seizes 33 Iranian State-Run Media Sites Accused Of Election Disinformation
* The Final Years Of John McAfee's Controversial Life
* BIOSConnect Code Execution Bugs Impact Millions Of Dell Devices
* John McAfee Reportedly Dead From Suspected Suicide In Spanish Jail
* ChaChi: A New GoLang Trojan Used In Attacks Against US Schools
* Zephyr OS Bluetooth Vulns Left Smart Devices Open To Attack
* SonicWall Botches October Patch For Critical VPN Bug
* Unpatched Linux Marketplace Bugs Allow RCE
* EU Wants Emergency Team For Nightmare Cyber-Attacks
* Six Flags To Pay $36 Million Over Collection Of Fingerprints
* Biden Is Worried About Cybersecurity. Japan Says Watch Cartoons.
* Ransomware Gang Cl0p Announces New Victim After Police Bust
* SEC Probing SolarWinds Clients Over Cyber Breach Disclosures
* Lexmark Printers Open To Arbitrary Code Execution Zero Day
* Ten-Year Hacktivisit Fugitive Commander X Arrested In Mexico
* Sideloading Apps Would Destroy iOS Security And Privacy
* Why Cyber Gangs Won't Worry About US-Russia Talks
* Millions Of Connected Cameras Open To Eavesdropping
* Digital Ad Industry Accused Of Huge Data Breach
* Peloton Bike+ Was Vulnerable To Remote Hacking, Researchers Find

Krebs on Security

* MyBook Users Urged to Unplug Devices from Internet
* How Cyber Sleuths Cracked an ATM Shimmer Gang
* How Cyber Safe is Your Drinking Water Supply?
* First American Financial Pays Farcical $500K Fine
* Ukrainian Police Nab Six Tied to CLOP Ransomware
* How Does One Get Hired by a Top Cybercrime Gang?
* Microsoft Patches Six Zero-Day Security Holes
* Justice Dept. Claws Back $2.3M Paid by Colonial Pipeline to Ransomware Gang
* Adventures in Contacting the Russian FSB
* Using Fake Reviews to Find Dangerous Extensions

Dark Reading

* The Role of Encryption in Protecting LGBTQ+ Community Members
* New CPU Baseline for Windows 11 Will Ensure Better Security, Microsoft Says
* Amazon Acquires Secure Messaging Platform Wickr
* Data Privacy Is in 23andMe CSO's DNA
* School's Out for Summer, but Don't Close the Book on Cybersecurity Training
* High-Level FIN7 Member Sentenced to 7 Years in Prison
* 7 Unconventional Pieces of Password Wisdom
* 74% of Q1 Malware Was Undetectable Via Signature-Based Tools
* D3FEND Framework Seeks to Lay Foundation for Cyber Defense
* Tulsa Officials Warn Ransomware Attackers Leaked City Files
* Preinstalled Firmware Updater Puts 128 Dell Models at Risk
* Boardroom Perspectives on Cybersecurity: What It Means for You
* Storms & Silver Linings: Avoiding the Dangers of Cloud Migration
* John McAfee, Creator of McAfee Antivirus Software, Dead at 75
* rMTD: A Deception Method That Throws Attackers Off Their Game
* 79% of Third-Party Libraries in Apps Are Never Updated
* VMs Help Ransomware Attackers Evade Detection, but It's Uncommon
* Microsoft Tracks New BazaCall Malware Campaign
* New DNS Name Server Hijack Attack Exposes Businesses, Government Agencies
* Survey Seeks to Learn How 2020 Changed Security

The Hacker News

* Microsoft Edge Bug Could've Let Hackers Steal Your Secrets for Any Site
* Hackers Trick Microsoft Into Signing Netfilter Driver Loaded With Rootkit Malware
* DMARC: The First Line of Defense Against Ransomware
* Cisco ASA Flaw Under Active Attack After PoC Exploit Posted Online
* SolarWinds Hackers Breach Microsoft Customer Support to Target its Customers
* Google Extends Support for Tracking Party Cookies Until 2023
* Watch Out! Zyxel Firewalls and VPNs Under Active Cyberattack
* Crackonosh virus mined $2 million of Monero from 222,000 hacked computers
* FIN7 Supervisor Gets 7-Year Jail Term for Stealing Millions of Credit Cards
* Clop Gang Partners Laundered $500 Million in Ransomware Payments
* BIOS Disconnect: New High-Severity Bugs Affect 128 Dell PC and Tablet Models
* Reduce Business Risk By Fixing 3 Critical Endpoint-to-Cloud Security Requirements
* One-Click Exploit Could Have Let Attackers Hijack Any Atlassian Account
* Critical Auth Bypass Bug Affects VMware Carbon Black App Control
* Antivirus Pioneer John McAfee Found Dead in Spanish Jail

Security Week

* Mercedes-Benz USA Says Vendor Exposed Customer Information
* GitHub Paid Out Over $1.5 Million via Bug Bounty Program Since 2016
* Microsoft: SolarWinds Hackers Continue to Target IT Companies
* XSS Vulnerability in Cisco Security Products Exploited in the Wild
* Cybersecurity Leaders Scramble to Decipher SBOM Mandate
* NewsBlur Restores Service After Hacker Wipes Database
* Bit Discovery Banks $4 Million for Attack Surface Management Tech
* AWS Acquires Encrypted Communications Service Wickr
* Old Vulnerability Exploited to Hack, Wipe WD Storage Devices
* Google Rolling Out Security Update for Google Drive
* Member of FIN7 Cybercrime Gang Sentenced to Prison in U.S.
* Vulnerabilities Expose Fortinet Firewalls to Remote Attacks
* Dutch Group Launches Data Harvesting Claim Against TikTok
* Researchers Detail Exploit Chain for Hijacking Atlassian Accounts
* Eclypsium: BIOSConnect Flaws Haunt Millions of Dell Computers
* Zyxel Warns Customers of Attacks on Security Appliances
* Google Delays Phase Out of Tracking Tech by Nearly 2 Years
* EU Announces New Joint Cyber Unit to Protect Against Critical Attacks
* Cybersecurity Companies Join Forces Against Controversial DMCA Section
* Google Expands Open Source Vulnerabilities Database
* XDR is a Destination, Not a Solution
* Cybersecurity is Never Out-of-Office
* Threat Monitoring Firm FYEO Announces Acquisition as It Emerges From Stealth
* Weidmueller Patches Dozen Vulnerabilities in Industrial WLAN Devices

Infosecurity Magazine

* Seamless EU-UK Data Flows to Continue Following Adequacy Decisions
* Reported HMRC-Branded Phishing Scams Grew by 87% During COVID-19
* Mercedes Benz Data Leak Includes Card and Social Security Details
* Sensitive Defense Documents Found at Bus Stop
* Former Health Secretary Faces Probe Over Use of Personal Emails
* Young Americans Twice as Likely to Cyber-stalk
* FIN7 Pen Tester to Serve Seven Years
* World's Largest E-tailers to be Investigated Over Fake Reviews
* AWS BugBust Aims to Fix One Million Vulnerabilities Globally
* Newly Discovered Dell Bugs Impact 30 Million PCs
* Cloud Database Exposes 800M+ WordPress Users' Records
* Cyber-stalker Blackmailed Nebraska Legislature Candidate's Wife

KnowBe4 Security Awareness Training Blog RSS Feed

* Misconfigured Cloud Database Increases Risk of Social Engineering
* [HEADS UP] Over 400% Increase in Ransomware Victims
* Threat Actors use Google Ads to Target People Migrating to Encrypted Messaging Services like Signal a
* Attackers Abuse Google Docs for Phishing Attacks
* ADATA Ransomware Attack Results in the Publishing of 700GB of Data Stolen
* 60% of Orgs Needed New Security Policies to Secure Their Remote Workforce
* Turning Compliance Into Tangible Security
* 80% of Ransomware Victim Organizations Experience a Second Attack
* Leaked Copies of Windows 11 Could Be Tempting Phishbait for Techies
* Why Phishing Attacks Are So Easy, Successful and Profitable - and What to do About It

ISC2.org Blog

* NIST Has Come Out With Its Own Ransomware Guidance | #RansomwareWeek
* Six Steps to Protect Your Organization from Ransomware | #RansomwareWeek
* (ISC)² Offers Free Access to Ransomware Education | #RANSOMWAREWEEK
* Prepare your defense against cybercriminals with ransomware best practice resources | #RansomwareWeek
* U.S. Government Equates Threat of Ransomware with Terrorism | #RansomwareWeek

HackRead

* Microsoft signed a driver called Netfilter, turns out it contained malware
* Western Digital My Book Live hard drives remotely wiped by hackers
* New malware in pirated games disables Windows Updates, Defender
* US supermarket giant Wegmans exposed sensitive data
* 6 official Python repositories plagued with cryptomining malware
* DreamHost hosting firm exposed almost a billion sensitive records
* 30 million Dell devices affected by BIOSConnect code execution bugs

Koddos

* Microsoft signed a driver called Netfilter, turns out it contained malware
* Western Digital My Book Live hard drives remotely wiped by hackers
* New malware in pirated games disables Windows Updates, Defender
* US supermarket giant Wegmans exposed sensitive data
* 6 official Python repositories plagued with cryptomining malware
* DreamHost hosting firm exposed almost a billion sensitive records
* 30 million Dell devices affected by BIOSConnect code execution bugs

Naked Security

* British tourists charged Â£1000s for pier visits in billing blunder
* S3 Ep38: Clop busts, destructive Linux hacking, and rooted bicycles [Podcast]
* Ransomware: What REALLY happens if you pay the crooks?
* Can *YOU* blow a PC speaker using only a Linux kernel driver?
* S3 Ep37: Quantum crypto, refunding Bitcoins, and Alpaca problems [Podcast]
* How to hack a bicycle - Peloton Bike+ rooting bug patched
* Clop ransomware suspects busted in Ukraine, money and motors seized
* "Face of Anonymous" suspect deported from Mexico to face US hacking charges
* ALPACA - the wacky TLS security vulnerability with a funky name
* S3 Ep36: Trickbot coder busted, passwords cracked, and breaches judged [Podcast]

Threat Post

* Mercedes-Benz Customer Data Flies Out the Window
* PS3 Players Ban: Latest Victims of Surging Attacks on Gaming Industry
* FIN7 'Pen Tester' Headed to Jail Amid $1B in Payment-Card Losses
* Cisco ASA Bug Now Actively Exploited as PoC Drops
* My Book Live Users Wake Up to Wiped Devices, Active RCE Attacks
* Hackers Crack Pirated Games with Cryptojacking Malware
* Spam Downpour Drips New IcedID Banking Trojan Variant
* Oh FCUK! Fashion Label, Medical Diagnostics Firm Latest REvil Victims
* Musk-Themed '$SpaceX' Cryptoscam Invades YouTube Advertising
* Critical VMware Carbon Black Bug Allows Authentication Bypass

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

* The OSI Model and You Part 6: Stopping Threats at the OSI Presentation Layer
* Cloud Security: Navigating the Cloud Migration Journey Successfully
* Data Security Along Every Stage of the Journey
* Shifting Left With Analytics to Identify Software Supply Chain Anomalies
* Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy
* "Our IT teams have an Incident Response Plan. We're prepared for a cyberattack." Maybe not.
* How One Application Test Uncovered an Unexpected Opening in an Enterprise Call Tool
* XDR: The Central Nervous System of Zero Trust
* The OSI Model and You Part 5: Stopping Threats at the OSI Session Layer
* Data is Wealth: Data Security is Wealth Protection

InfoWorld

* 5 enabling technologies for hybrid and multicloud architectures
* How enterprises are bringing pandemic-driven cloud costs under control
* Review: 6 top videoconferencing services put to the test
* What's new in Angular 12
* State of AI report finds AI is now core to business success
* Cloud security is still a work in progress
* 11 hot language projects riding WebAssembly
* Deno Company unveils server-side JavaScript hosting service
* How to visualize time series data
* Tailwind CSS: Learn the joys of functional, responsive CSS

C4ISRNET - Media for the Intelligence Age Military

* The Air Force's new ABMS strategy: Buy new capability, now
* Inhofe revives bill to target Ligado
* 'Just like your iPhone': Marines need to connect battlefield to larger network for future conflicts
* Northrop CEO: To beat China, US must step up investments in advanced computing
* Air Force's experimental football field-sized satellite ends operations
* US Cyber Command exercise will help shape new tactics for changing threats
* It's more than chips: Other risks exist in defense electronics supply chain
* Guardsmen train for real-world cyber disruptions
* Pentagon launches artificial intelligence effort to prep combatant commands for JADC2
* NATO hopes to launch new defense tech accelerator by 2023

The Hacker Corner

Conferences

* 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)
* How To Sponsor Cybersecurity Conferences

Google Zero Day Project

* Fuzzing iOS code on macOS at native speed
* Designing sockfuzzer, a network syscall fuzzer for XNU

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.

* Hacky Holidays - Space Race
* CyberThreatForce CTF | 2021
* 0CTF/TCTF 2021 Quals
* Capture the Signal CTF 2021
* redpwnCTF 2021
* ENOWARS 5
* TyphoonCon CTF 2021
* Google Capture The Flag 2021
* RuCTF 2021
* HTB Business CTF 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

* Flawfinder 2.0.18
* Falco 0.29.0
* Clam AntiVirus Toolkit 0.103.3
* GRAudit Grep Auditing Tool 3.1
* Hashcat Advanced Password Recovery 6.2.2 Source Code
* Hashcat Advanced Password Recovery 6.2.2 Binary Release
* TOR Virtual Network Tunneling Tool 0.4.6.5
* tcpdump 4.99.1
* nfstream 6.3.2
* GNU Privacy Guard 2.2.28

Kali Linux Tutorials

* RdpCacheStitcher : RdpCacheStitcher Is A Tool That Supports Forensic Analysts
* FalconEye : Real-time detection software for Windows process injections
* Rustcat : Netcat Alternative
* Joern : Open-source Code Analysis Platform For C/C++/Java Based On Code Property Graphs
* PPLdump : Dump The Memory Of A PPL With A Userland Exploit
* Aggrokatz : An Aggressor Plugin Extension For Cobalt Strike Which Enables Pypykatz To Interface With
* Volatility GUI : GUI For Volatility Forensics Tool
* Gundog : Guided Hunting In Microsoft 365 Defender
* Redpill : Assist Reverse Tcp Shells In Post-Exploration Tasks
* iOS Malicious Bit Hunter : A Malicious Plug-In Detection Engine For iOS Applications

GBHackers Analysis

* Researcher Managed to Hack ATMs Using His Phone's NFC & Android App
* 10 Best WiFi Hacking Apps for Android - 2021 Edition
* How to Protect Your Email From Hacking?
* EA Sports Hacked - Hackers Stolen Source Code With 780 GB of Data
* Russian Hacker Jailed for Running a Darkweb Market Place that Sells Stolen Credit card Details

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Mobile Validation - Working together for the Common Good
* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course

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 About Android Exploits
* Update Your Pelaton Bikes ASAP; Nuclear Research Institute Had a VPN Vulnerability - ThreatWire
* OMG: This Malicious Crypto Wallet Steals Bitcoin

The PC Security Channel [TPSC]

* Windows Defender vs Malware in 2021
* Darkside Ransomware: The threat behind the state of emergency in the US

Eli the Computer Guy

* How to Become a Tech Professional
* "Easy" SMS with Twilio (Add SMS to Your Coding Projects)
* "Easy" Computer Vision with Azure and AWS
* DNS for Cybersecurity

Security Now

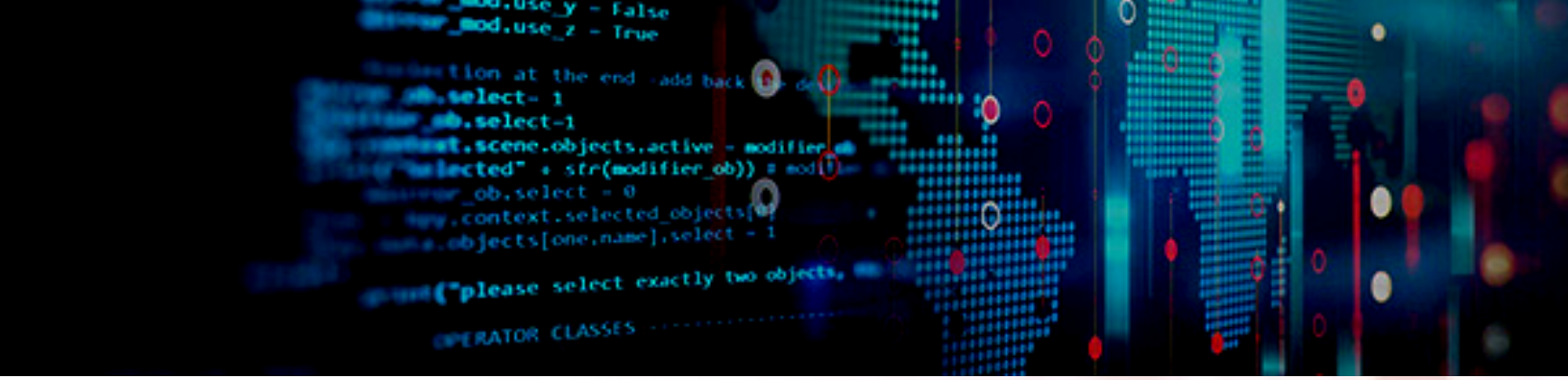
* Avaddon Ransonomics - Chrome 0-Day, Big Spinrite Update, iOS Wi-Fi Bug, Economics of Ransomware
* TLS Confusion Attacks - TikTok Privacy, iOS 14.5 Tracking Permission, Industry-Wide Patch Tuesday

Troy Hunt

* Weekly Update 249

Intel Techniques: The Privacy, Security, & OSINT Show

* 222-Spoiler: We all die
* 221-Anonymous Mobile Devices



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

* 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
* Next-Gen Threat Intelligence: Adding Profound Value to Security and Risk Functions
* TrickBot: Get to Know the Malware That Refuses to Be Killed
* SolarWinds: Illuminating the Hidden Patterns That Advance the Story
* For Threat Actors, Shadow Z118 is the Kit That Keeps on Giving

FireEye

* Automated remediation level 3: Governance and hygiene
* 3 Takeaways From The 2021 VDBIR: It's An Appandemic
* Metasploit Wrap-Up
* Kill Chains: Part 3→What's Next
* CVE-2021-20025: SonicWall Email Security Appliance Backdoor Credential
* Don Spies and Kim Grauer on tracking illicit Bitcoin transactions
* Rapid7 Joins Statement On DMCA Lawsuits Against Security Tools
* InsightVM Release Announcement: Global Dashboard Filters
* Attack Surface Analysis Part 3: Red and Purple Teaming
* Automated remediation level 2: Best practices

Proof of Concept (PoC) & Exploits

Packet Storm Security

* SAPSprint 7.60 Unquoted Service Path
* Lightweight Facebook-Styled Blog Remote Code Execution
* Seeddms 5.1.10 Remote Command Execution
* Online Pet Shop We App 1.0 SQL Injection / Shell Upload
* Simple Client Management System 1.0 SQL Injection
* rConfig Shell Upload
* Trojan-Dropper.Win32.Krepper.a Remote Command Execution
* Trojan-Dropper.Win32.Juntador.a Weak Hardcoded Password
* TP-Link TL-WR841N Command Injection
* Huawei DG8045 Authentication Bypass
* Trojan.Win32.Banpak.kh Insecure Permissions
* Adobe ColdFusion 8 Remote Command Execution
* Trojan.Win32.SecondThought.ak Insecure Permissions
* Backdoor.Win32.ReverseTrojan.200 Authentication Bypass
* VMware vCenter 6.5 / 6.7 / 7.0 Remote Code Execution
* HPE RDA-CAS 1.23.826 Denial Of Service
* Cisco Modeling Labs 2.1.1-b19 Remote Command Execution
* F5 BIG-IQ VE 8.0.0-2923215 Remote Root
* Monitorr 1.7.6m Bypass / Information Disclosure / Shell Upload
* WordPress WP Google Maps 8.1.11 Cross Site Scripting
* WordPress Poll, Survey, Questionnaire And Voting System 1.5.2 SQL Injection
* Microsoft Windows Filtering Platform Token Access Check Privilege Escalation
* Simple CRM 3.0 SQL Injection
* Online Library Management System 1.0 Shell Upload
* Online Library Management System 1.0 SQL Injection

CXSecurity

* rConfig Shell Upload
* Adobe ColdFusion 8 Remote Command Execution
* VMware vCenter 6.5 / 6.7 / 7.0 Remote Code Execution
* Lightweight Facebook-Styled Blog Remote Code Execution
* HPE RDA-CAS 1.23.826 Denial Of Service
* Monitorr 1.7.6m Bypass / Information Disclosure / Shell Upload
* Post-it 5.0.1 Denial of Service (PoC)

Proof of Concept (PoC) & Exploits

Exploit Database

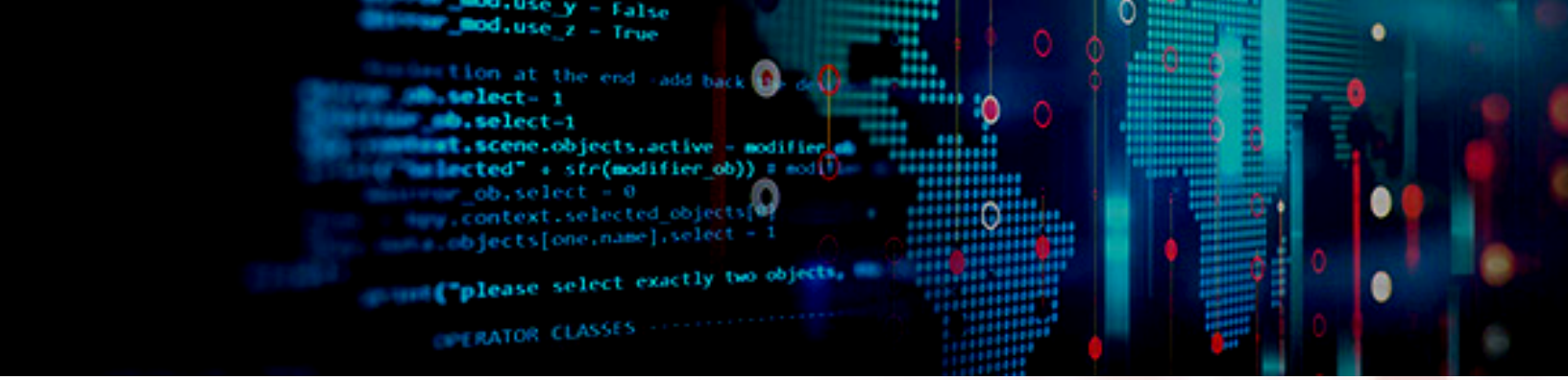
* [webapps] Netgear WNAP320 2.0.3 - 'macAddress' Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Atlassian Jira Server/Data Center 8.16.0 - Reflected Cross-Site Scripting (XSS)
* [webapps] SAS Environment Manager 2.5 - 'name' Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin YOP Polls 6.2.7 - Stored Cross Site Scripting (XSS)
* [webapps] Lightweight facebook-styled blog 1.3 - Remote Code Execution (RCE) (Authenticated) (Metaspl
* [webapps] Simple Client Management System 1.0 - 'uemail' SQL Injection (Unauthenticated)
* [webapps] Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated)
* [local] SAPSprint 7.60 - 'SAPSprint' Unquoted Service Path
* [webapps] Huawei dg8045 - Authentication Bypass
* [webapps] TP-Link TL-WR841N - Command Injection
* [webapps] Adobe ColdFusion 8 - Remote Command Execution (RCE)
* [webapps] VMware vCenter Server RCE 6.5 / 6.7 / 7.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Simple CRM 3.0 - 'email' SQL injection (Authentication Bypass)
* [webapps] Online Library Management System 1.0 - Arbitrary File Upload Remote Code Execution (Unauthe
* [webapps] Online Library Management System 1.0 - 'Search' SQL Injection
* [webapps] WordPress Plugin Poll, Survey, Questionnaire and Voting system 1.5.2 - 'date_answers' Blind
* [webapps] WordPress Plugin WP Google Maps 8.1.11 - Stored Cross-Site Scripting (XSS)
* [webapps] Phone Shop Sales Managements System 1.0 - Insecure Direct Object Reference (IDOR)
* [webapps] Responsive Tourism Website 3.1 - Remote Code Execution (RCE) (Unauthenticated)
* [local] ASUS DisplayWidget Software 3.4.0.036 - 'ASUSDisplayWidgetService' Unquoted Service Path
* [local] Remote Mouse GUI 3.008 - Local Privilege Escalation
* [webapps] Customer Relationship Management System (CRM) 1.0 - Remote Code Execution
* [local] Lexmark Printer Software G2 Installation Package 1.8.0.0 - 'LM__bdsvc' Unquoted Service Path
* [webapps] Simple CRM 3.0 - 'name' Stored Cross site scripting (XSS)

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

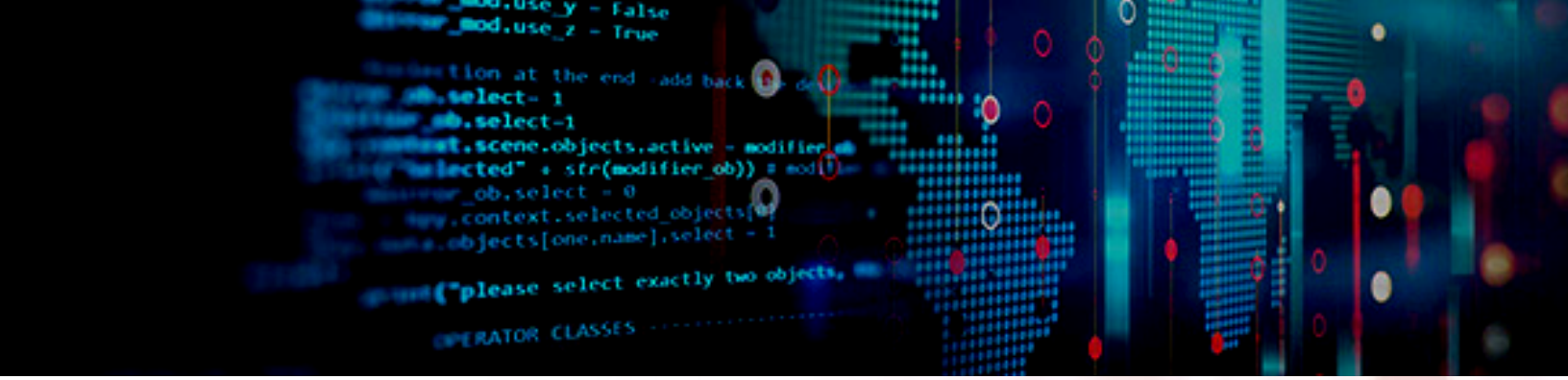
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://bappeda.bondowosokab.go.id/AnonSec.html
https://bappeda.bondowosokab.go.id/AnonSec.html notified by AnonSec Team
http://pdmakp.gov.pk/index.html
http://pdmakp.gov.pk/index.html notified by B3g0k[Kurdish Hacker]
https://pa-banggai.go.id/hyme.html
https://pa-banggai.go.id/hyme.html notified by Family Attack Cyber
https://sipp.pa-banggai.go.id/hyme.html
https://sipp.pa-banggai.go.id/hyme.html notified by Family Attack Cyber
https://panjar.pa-banggai.go.id/hyme.html
https://panjar.pa-banggai.go.id/hyme.html notified by Family Attack Cyber
https://pa-padangsidempuankota.go.id/hyme.html
https://pa-padangsidempuankota.go.id/hyme.html notified by Family Attack Cyber
http://kejari-empatlawang.go.id
http://kejari-empatlawang.go.id notified by ./s3nt1n3L
http://pa-padangsidempuan.go.id/hyme.html
http://pa-padangsidempuan.go.id/hyme.html notified by Family Attack Cyber
http://pn-waikabubak.go.id/hyme.html
http://pn-waikabubak.go.id/hyme.html notified by Family Attack Cyber
http://tilang.pn-waikabubak.go.id/hyme.html
http://tilang.pn-waikabubak.go.id/hyme.html notified by Family Attack Cyber
https://sipp.pn-waikabubak.go.id/hyme.html
https://sipp.pn-waikabubak.go.id/hyme.html notified by Family Attack Cyber
http://comune.dolo.ve.it/ok.html
http://comune.dolo.ve.it/ok.html notified by Moroccan Revolution
http://henrycounty.in.gov/rn.html
http://henrycounty.in.gov/rn.html notified by Ren4Sploit
https://www.afrims.go.th/o.txt
https://www.afrims.go.th/o.txt notified by Mr.ToKeiChun69
https://bkpd.bonebolangokab.go.id/pensiun.txt
https://bkpd.bonebolangokab.go.id/pensiun.txt notified by Mr.Rm19
https://pn-kualakapuas.go.id/pensiun.txt
https://pn-kualakapuas.go.id/pensiun.txt notified by Mr.Rm19
https://upcrndp.gov.in/by_Panataran.html
https://upcrndp.gov.in/by_Panataran.html notified by Panataran



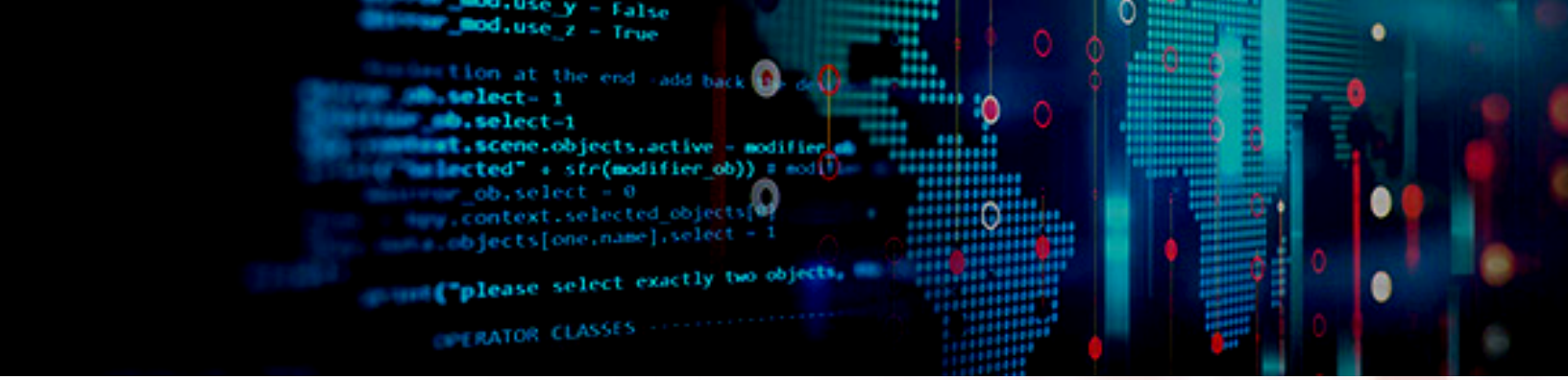
Dark Web News

Darknet Live

White House and Dark0de Launch Harm Reduction Programs
White House Market and Dark0de Reborn both announced the launch of harm reduction programs focused primarily on product quality. (via darknetlive.com)
Two Sentenced for Reselling Amphetamine from the Darkweb
Two Austrian men were sentenced to prison for their roles in the importation and resale of large quantities of drugs purchased through the darkweb. (via darknetlive.com)
Austrian Brothers Allegedly Resold Drugs from the Darkweb
Police in Austria identified two brothers suspected of importing and reselling drugs purchased through the darkweb. (via darknetlive.com)
Connecticut Man Admits Selling Counterfeit Oxycodone
A Connecticut man admitted participating in the production and distribution of counterfeit oxycodone pills through the darkweb. (via darknetlive.com)

Dark Web Link

Brit Paedophile Arrested After 70 Home Security Camera Hack
A Brit paedophile has been arrested in Benidorm. The man had been under suspicion of hacking over 70 families' home security cameras around the world. Spanish Police stated that the unnamed pedophile had worked as a babysitter and private tutor. He had acquired 1,000 images of the naked children. Apart from this, the Brit paedophile [...] The post Brit Paedophile Arrested After 70 Home Security Camera Hack appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Crypto Coin Exchanges: What Is Happening Right Now?
The majority of the top cryptocurrencies are lately trading in red, with Ethereum (ETH) and Bitcoin (BTC) down around 3% in the past 24 hours. The global crypto market capitalization is currently at $1.51 trillion, which is a sharp decline of 3.40% over the previous day. The world's largest cryptocurrency, Bitcoin, has dropped as much [...] The post Crypto Coin Exchanges: What Is Happening Right Now? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Clop Ransomware Gang Oozes Out Cash In The Ukrainian Raid
The Ukrainian cops have conducted almost two dozen raids that targeted the alleged associates of the Clop ransomware gang. The ransomware gang is a Russian-speaking group that has been blamed for a half-billion dollars cyber attack as well as extortion in the United States and South Korea. On Wednesday, a police statement mentioned that 21 [...] The post Clop Ransomware Gang Oozes Out Cash In The Ukrainian Raid appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Citrix Releases Security Updates for Hypervisor
* VMware Releases Security Updates
* Google Releases Security Updates for Chrome
* Cisco Releases Security Updates for Multiple Products
* Apple Releases Security Updates for iOS 12.5.4
* CISA Releases Advisory on ZOLL Defibrillator Dashboard
* Google Releases Security Updates for Chrome
* CISA Addresses the Rise in Ransomware Targeting Operational Technology Assets
* AA21-148A: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* Vulnerability Summary for the Week of June 14, 2021
* Vulnerability Summary for the Week of June 7, 2021

Zero Day Initiative Advisories

ZDI-CAN-14256: Autodesk
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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14243: Autodesk
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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14245: Autodesk
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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14255: Autodesk
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14248: Autodesk
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until

2021-10-23 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-13880: Apple

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'parkminchan' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14244: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14241: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14247: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14380: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14257: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14251: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14377: Bitdefender

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14246: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14239: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until

2021-10-23 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-14254: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14253: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14238: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14249: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14250: Autodesk

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14242: Autodesk

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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14041: Microsoft

A CVSS score 7.0 (AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Wenguang Jiao' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14064: ICONICS

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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-14060: ICONICS

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-06-25, 3 days ago. The vendor is given until 2021-10-23 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

Ubuntu Security Notice USN-4995-2

Ubuntu Security Notice 4995-2 - USN-4995-1 fixed vulnerabilities in Thunderbird. This update provides the corresponding updates for Ubuntu 18.04 LTS. Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass security restrictions, or execute arbitrary code. It was discovered that extensions could open popup windows with control of the window title in some circumstances. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to spoof a website and trick the user into providing credentials. Multiple security issues were discovered in Thunderbird's OpenPGP integration. If a user were tricked into importing a specially crafted key in some circumstances, an attacker could potentially exploit this to cause a denial of service or confuse the user. A use-after-free was discovered when Responsive Design Mode was enabled. If a user were tricked into opening a specially crafted website with Responsive Design Mode enabled, an attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. It was discovered that Thunderbird mishandled ftp URLs with encoded newline characters. If a user were tricked into clicking on a specially crafted link, an attacker could potentially exploit this to send arbitrary FTP commands. It was discovered that Thunderbird wrote signatures to disk and read them back during verification. A local attacker could potentially exploit this to replace the data with another signature file. It was discovered that Thunderbird might load an alternative OTR library. If a user were tricked into copying a specially crafted library to one of Thunderbird's search paths, an attacker could potentially exploit this to execute arbitrary code. It was discovered that secret keys imported into Thunderbird were stored unencrypted. A local attacker could potentially exploit this to obtain private keys. It was discovered that Thunderbird did not indicate when an inline signed or encrypted message contained additional unprotected parts. Various other issues were also addressed.

Ubuntu Security Notice USN-5004-1

Ubuntu Security Notice 5004-1 - It was discovered that RabbitMQ incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. Jonathan Knudsen discovered RabbitMQ incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2021-2543-01

Red Hat Security Advisory 2021-2543-01 - Red Hat OpenShift Jaeger is Red Hat's distribution of the Jaeger project, tailored for installation into an on-premise OpenShift Container Platform installation. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2021-2532-01

Red Hat Security Advisory 2021-2532-01 - Red Hat OpenShift Jaeger is Red Hat's distribution of the Jaeger project, tailored for installation into an on-premise OpenShift Container Platform installation.

Ubuntu Security Notice USN-5003-1

Ubuntu Security Notice 5003-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when performing div and mod operations. A local attacker could use this to possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-5002-1

Ubuntu Security Notice 5002-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code.

Red Hat Security Advisory 2021-2529-01

Red Hat Security Advisory 2021-2529-01 - KVM is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm-rhev packages provide the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include an out of bounds access vulnerability.

Red Hat Security Advisory 2021-2130-01

Red Hat Security Advisory 2021-2130-01 - Windows Container Support for Red Hat OpenShift allows you to deploy Windows container workloads running on Windows Server containers. Issues addressed include a man-in-the-middle vulnerability.

Ubuntu Security Notice USN-5001-1

Ubuntu Security Notice 5001-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Mathy Vanhoef discovered that the Linux kernel's WiFi implementation did not properly clear received fragments from memory in some situations. A physically proximate attacker could possibly use this issue to inject packets or expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5000-1

Ubuntu Security Notice 5000-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Piotr Krysiuk discovered that the eBPF implementation in the Linux kernel did not properly enforce limits for pointer operations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4999-1

Ubuntu Security Notice 4999-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Piotr Krysiuk discovered that the eBPF implementation in the Linux kernel did not properly enforce limits for pointer operations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4997-1

Ubuntu Security Notice 4997-1 - Norbert Slusarek discovered a race condition in the CAN BCM networking protocol of the Linux kernel leading to multiple use-after-free vulnerabilities. A local attacker could use this issue to execute arbitrary code. Piotr Krysiuk discovered that the eBPF implementation in the Linux kernel did not properly enforce limits for pointer operations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2523-01

Red Hat Security Advisory 2021-2523-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include integer overflow and use-after-free vulnerabilities.

Ubuntu Security Notice USN-4995-1

Ubuntu Security Notice 4995-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, spoof the UI, bypass security restrictions, or execute arbitrary code. It was discovered that extensions could open popup windows with control of the window title in some circumstances. If a user were tricked into installing a specially crafted extension, an attacker could potentially exploit this to spoof a website and trick the user into providing credentials. Various other issues were also addressed.

Ubuntu Security Notice USN-4996-2

Ubuntu Security Notice 4996-2 - USN-4996-1 fixed several vulnerabilities in OpenEXR. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-2522-01

Red Hat Security Advisory 2021-2522-01 - 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 integer overflow and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2519-01

Red Hat Security Advisory 2021-2519-01 - 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 buffer overflow, integer overflow, and privilege escalation vulnerabilities.

Ubuntu Security Notice USN-4996-1

Ubuntu Security Notice 4996-1 - It was discovered that OpenEXR incorrectly handled certain malformed EXR image files. If a user were tricked into opening a crafted EXR image file, a remote attacker could cause a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-4994-2

Ubuntu Security Notice 4994-2 - USN-4994-1 fixed several vulnerabilities in Apache. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Antonio Morales discovered that the Apache mod_auth_digest module incorrectly handled certain Digest nonces. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4994-1

Ubuntu Security Notice 4994-1 - Marc Stern discovered that the Apache mod_proxy_http module incorrectly handled certain requests. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. This issue only affected Ubuntu 20.04 LTS, Ubuntu 20.10, and Ubuntu 21.04. Antonio Morales discovered that the Apache mod_auth_digest module incorrectly handled certain Digest nonces. A remote attacker could possibly use this issue to cause Apache to crash, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4993-1

Ubuntu Security Notice 4993-1 - Kirin discovered that Dovecot incorrectly escaped kid and azp fields in JWT tokens. A local attacker could possibly use this issue to validate tokens using arbitrary keys. This issue only affected Ubuntu 20.10 and Ubuntu 21.04. Fabian Ising and Damian Poddebniak discovered that Dovecot incorrectly handled STARTTLS when using the SMTP submission service. A remote attacker could possibly use this issue to inject plaintext commands before STARTTLS negotiation. Various other issues were also addressed.

Ubuntu Security Notice USN-4992-1

Ubuntu Security Notice 4992-1 - Máté Kukri discovered that the acpi command in GRUB 2 allowed privileged users to load crafted ACPI tables when secure boot is enabled. An attacker could use this to bypass UEFI Secure Boot restrictions. Chris Coulson discovered that the rmmod command in GRUB 2 contained a use- after-free vulnerability. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. Chris Coulson discovered that a buffer overflow existed in the command line parser in GRUB 2. A local attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. Various other issues were also addressed.

Protectimus SLIM NFC Time Manipulation

When analyzing the Protectimus SLIM TOTP hardware token, Matthias Deeg found out that the time used by the Protectimus SLIM TOTP hardware token can be set independently from the used seed value for generating time-based one-time passwords without requiring any authentication.

Ubuntu Security Notice USN-4991-1

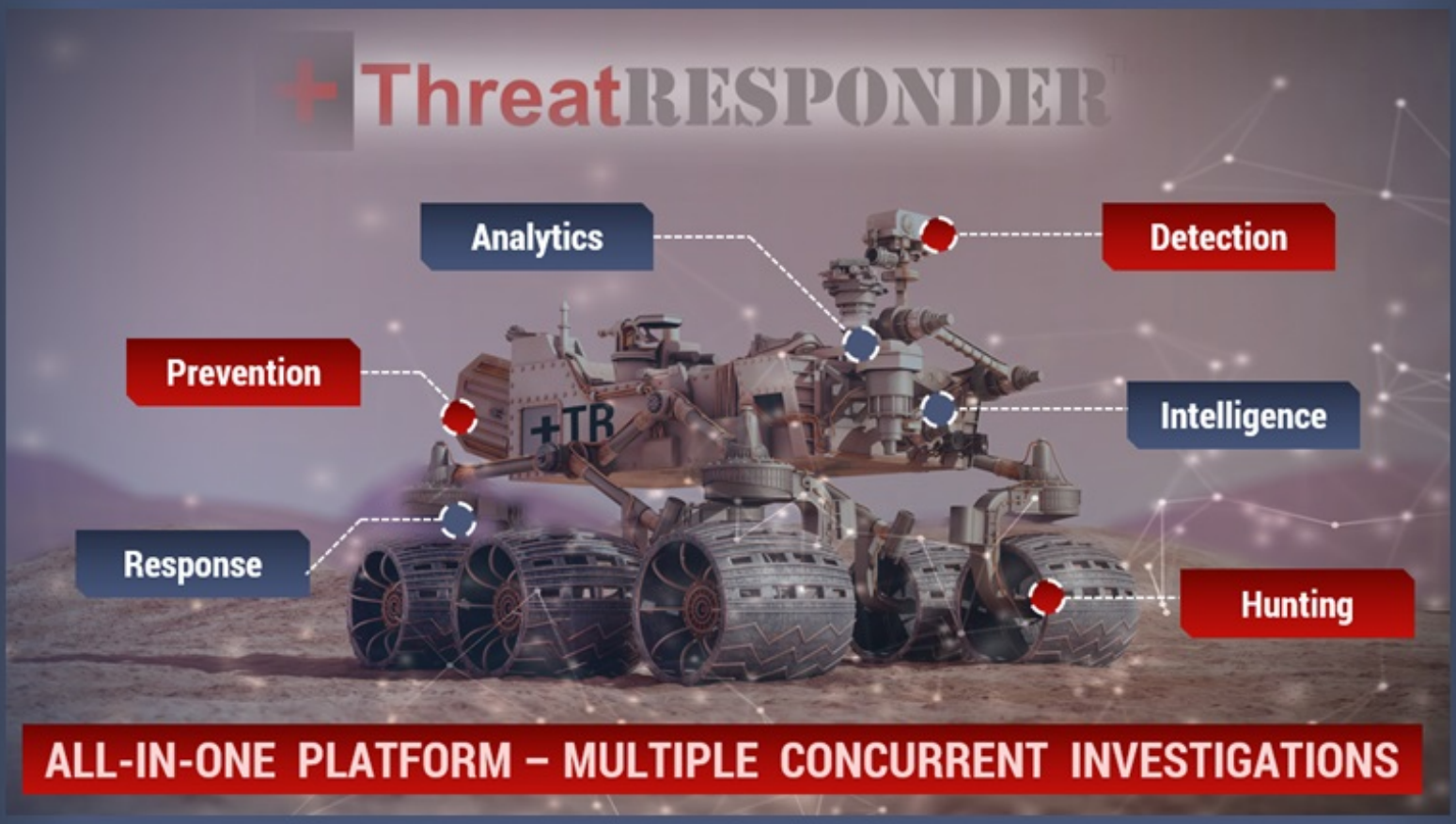
Ubuntu Security Notice 4991-1 - Yunho Kim discovered that libxml2 incorrectly handled certain error conditions. A remote attacker could exploit this with a crafted XML file to cause a denial of service, or possibly cause libxml2 to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, and Ubuntu 16.04 ESM. Zhipeng Xie discovered that libxml2 incorrectly handled certain XML schemas. A remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS. 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



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:

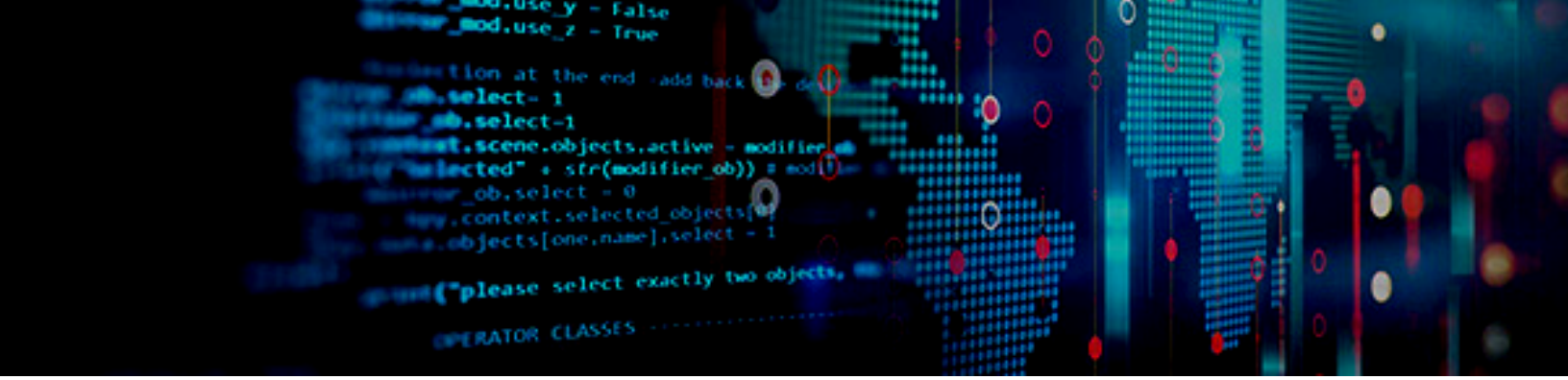
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

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

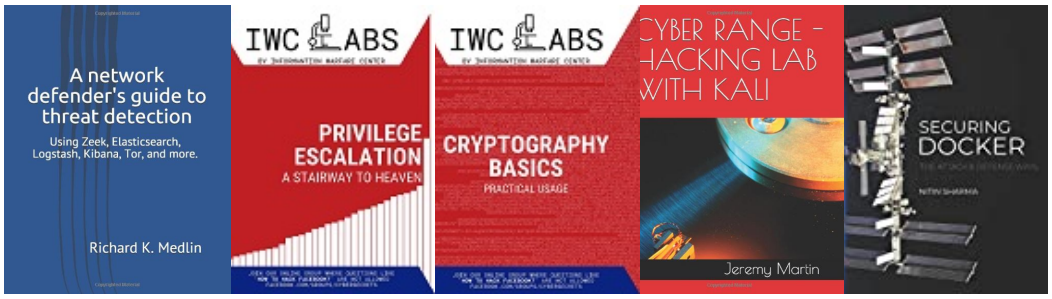


The Cyber Secrets publications on Amazon

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.

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