Jun-09-21

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 9, 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

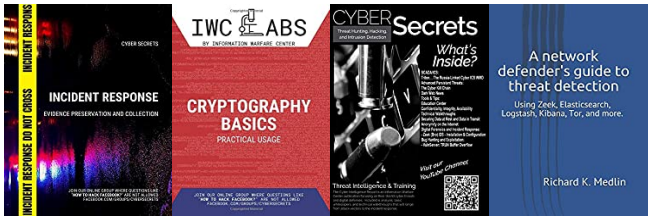
Internet Storm Center Infocon Status

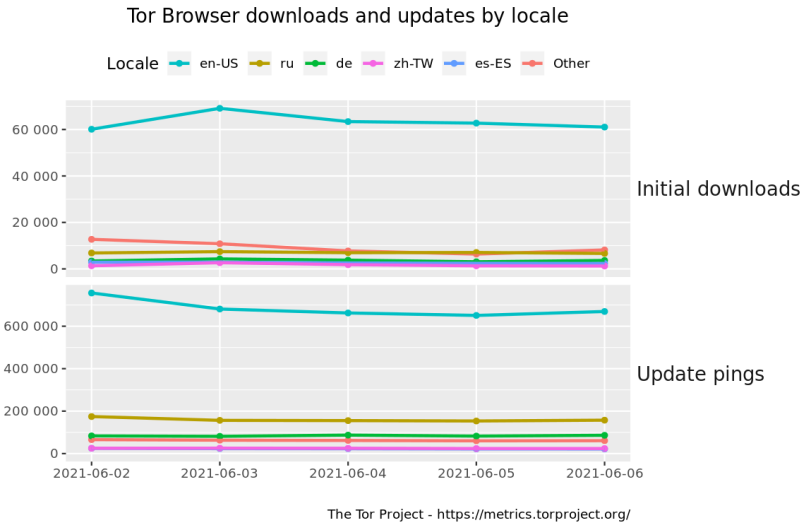
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

* CSI Linux 2021.2 Beta is now availible for those that have 2021.1 already installed. To upgrade, open a command line and type: wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh

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

Index of Sections

Packet Storm Security

* Phil Zimmerman Looks Back On 30 Years Of PGP
* An0m Encrypted-Chat Sting Leads To Arrest Of 800
* DHS Chooses Companies To Run Civilian Agency Vulnerability Disclosure Programs
* One Fastly Customer Triggered Internet Meltdown
* Windows Container Malware Targets Kubernetes Clusters
* Apple Continues Privacy War With App Tracker Reports
* Majority Of Ransom Paid By Colonial Pipeline Seized By DOJ
* How The FBI And AFP Accessed Encrypted Messages In TrojanShield Investigation
* REvil Ransomware Gang Spill Details On US Attacks
* WhatsApp Hijack Scam Continues To Spread
* Apple Updates AirTags After Stalking Fears
* Patch Now: Attackers Are Hunting For This Critical VMware vCenter Flaw
* Hacker Lexicon: What Is A Supply Chain Attack?
* Chrome 91 Will Warn Users When Installing Untrusted Extensions
* Supreme Court Narrows Interpretation Of CFAA, To The Relief Of Ethical Hackers
* Google PPC Ads Used To Deliver Infostealers
* FBI Says It Is Investigating About 100 Types Of Ransomware
* Check Out This Great RCE PoC Walkthrough For The VMware ESXi OpenSLP Heap Overflow Vulnerability
* White House Warns Companies To Step Up Cybersecurity
* Norton Antivirus Adds Ethereum Cryptocurrency Mining
* Necro Python Bot Revamped With New VMWare Server Exploits
* Attack On Meat Supplier Came From REvil, Ransomware's Most Cut Throat Gang
* Amazon US Customers Have A Week To Opt Out Of Mass Wifi Sharing
* JBS Ransomware Attack Likely The Work Of Russia
* Cyber-Insurance Fuels Ransomware Payment Surge

Krebs on Security

* 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
* Boss of ATM Skimming Syndicate Arrested in Mexico
* How to Tell a Job Offer from an ID Theft Trap
* Recycle Your Phone, Sure, But Maybe Not Your Number
* Try This One Weird Trick Russian Hackers Hate
* DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized
* Microsoft Patch Tuesday, May 2021 Edition

Dark Reading

* With Cloud, CDO and CISO Concerns Are Equally Important
* Hardening the Physical Security Supply Chain to Mitigate the Cyber-Risk
* Ransomware Is Not the Problem
* Phished Account Credentials Mostly Verified in Hours
* Microsoft Patches 6 Zero-Days Under Active Attack
* FBI Issued Encrypted Devices to Capture Criminals
* Colonial Pipeline CEO: Ransomware Attack Started via Pilfered 'Legacy' VPN Account
* Microsoft CISO Shares Remote Work Obstacles & Lessons Learned
* How Employees Can Keep Their 401(k)s Safe From Cybercriminals
* Cyber Resilience: The Emerald City of the Security World
* An Answer to APP Scams You Can Bank On
* First Known Malware Surfaces Targeting Windows Containers
* DoJ Seizes $2.3M in Bitcoin Paid to Colonial Pipeline Attackers
* Latvian Woman Charged for Role In Crafting Trickbot Malware
* CISA Warns Criminals Seek to Exploit Critical VMware Bug
* Cartoon Caption Winner: Road Trip
* Cyber Athletes Compete to Form US Cyber Team
* NortonLifeLock Criticized for New Cryptomining Feature
* How Can I Test the Security of My Home-Office Employees' Routers?
* The US Must Redefine Critical Infrastructure for the Digital Era

The Hacker News

* New TLS Attack Lets Attackers Launch Cross-Protocol Attacks Against Secure Sites
* Crypto-Mining Attacks Targeting Kubernetes Clusters via Kubeflow Instances
* EBook - Creating a Large Company Security Stack on a Lean Company Budget
* Update Your Windows Computers to Patch 6 New In-the-Wild Zero-Day Bugs
* Feds Secretly Ran a Fake Encrypted Chat App and Busted Over 800 Criminals
* New UAF Vulnerability Affecting Microsoft Office to be Patched Today
* Top 10 Privacy and Security Features Apple Announced at WWDC 2021
* U.S. Recovers $2.3 Million Ransom Paid to Colonial Pipeline Hackers
* Shifting the focus from reactive to proactive, with human-led secure coding
* Researchers Discover First Known Malware Targeting Windows Containers
* Hackers Breached Colonial Pipeline Using Compromised VPN Password
* Latvian Woman Charged for Her Role in Creating Trickbot Banking Malware
* GitHub Updates Policy to Remove Exploit Code When Used in Active Attacks
* Break Into Ethical Hacking With 18 Training Courses For Just $42.99
* TikTok Quietly Updated Its Privacy Policy to Collect Users' Biometric Data

Security Week

* Tough Fight Looms Against Ransomware 'Epidemic'
* Kubeflow Deployments Targeted in New Crypto-mining Campaign
* Amazon Sidewalk Mesh Network Raises Security, Privacy Concerns
* Cisco Smart Install Protocol Still Abused in Attacks, 5 Years After First Warning
* Intel Releases 29 Advisories to Describe 73 Vulnerabilities Affecting Its Products
* Cyber Risk Management Firm Bringa Raises $110 Million
* Pipeline CEO Defends Paying Ransom Amid Cyberattack
* Siemens, Schneider Electric Inform Customers About Tens of Vulnerabilities
* 'What's the Price Today?': FBI Phone App Reaped Secrets of Global Drug Networks
* Endpoint Management Startup Aiden Technologies Closes $2.9 Million Seed Round
* SAP Patches Critical Vulnerabilities in NetWeaver
* NYC's 1,000-Lawyer Law Department Targeted by Cyberattack
* Microsoft Raises Alarm for New Windows Zero-Day Attacks
* Adobe Patches Major Security Flaws in PDF Reader, Photoshop
* Organizations Warned About DoS Flaws in Popular Open Source Message Brokers
* CISA Announces Vulnerability Disclosure Policy Platform
* Critical Vulnerabilities Patched in Android With June 2021 Security Updates
* WAGO Controller Flaws Can Allow Hackers to Disrupt Industrial Processes
* Apple Unveils VPN-Like Service and New Privacy Features at WWDC 2021
* Hundreds Arrested in 'Staggering' FBI Encrypted Phone Sting
* US Recovers Most of Ransom Paid After Colonial Pipeline Hack
* Military Vehicles Maker Navistar Reports Data-Theft Cyberattack
* 'Siloscape' Malware Targets Windows Server Containers
* Cybersecurity M&A Roundup for June 1-6, 2021
* Energy Chief Cites Risk of Cyberattacks Crippling Power Grid

Infosecurity Magazine

* Pennsylvanian Charged over Trump Impersonation Fraud
* Single Fastly Customer Sparked Global Internet Meltdown
* #Infosec21: NCSC Outlines Biggest Cyber Threats During COVID19
* A Third of Execs Plan to Spy on Staff to Guard Trade Secrets
* Microsoft Fixes Seven Zero-Days This Patch Tuesday
* Police Access Encrypted Devices in Major Global Crime Bust
* MoviePass Operators Settle Data Security Allegations
* Cyber-attack on NYC Law Department
* Illinois County Stricken with Grief
* CISA and Bugcrowd to Launch Federal Crowdsourced VDP Platform
* #Infosec21: Cybersecurity to Become a "Matter of Life and Death"

* Large Parts of Internet Offline Following Cloud Provider Issue

KnowBe4 Security Awareness Training Blog RSS Feed

* Insights Into Credential Phishing
* FINRA Warns U.S. Brokerage Firms of New Phishing Campaign Threatening Penalties for Non-Compliance
* Ransomware Tops IBMs List of Most Observed Attack Types with Sodinokibi Maintaining the Lead
* 78% of CISOs Say Attacks Have Increased as a Result of More Employees Working from Home
* Chinese Hacker Group Debuts After 3 Years of Testing with a Previously Unseen Backdoor Exploit
* The Future Of Ransomware
* CyberheistNews Vol 11 #22 [Heads Up] The Cybersecurity Insurance Landscape Is Fundamentally Changing
* Phishing Trends Show X-Rated Themes Have Skyrocketed 974%
* KnowBe4 Fresh Content Updates from May: Including New Mobile-First Training Modules
* Ransomware Attacks Run Rampant as Fujifilm Becomes the Next Victim

ISC2.org Blog

* An Inside Look at Cloud Security from Industry Experts
* Make New Connections with (ISC)² Community
* Software Security Testing - Hidden Thoughts Can Cost You
* Hiring from Within and Retaining Cybersecurity Talent: Building Your Strategy
* Survey Now Open: What Differences Did the Year Make in Cybersecurity?

HackRead

* 800+ criminals arrested after FBI turned Anom app into honeypot
* How gamers should secure their accounts from cyber attacks
* FBI recovers millions in ransom from DarkSide ransomware gang
* Kubernetes Clusters Targeted by Siloscape Malware
* 4 Ways For Employees To Distinguish Phishing Attacks
* How to perform a website security check- 6 tools to check website security
* Influence of technology on gaming industry

Koddos

* 800+ criminals arrested after FBI turned Anom app into honeypot
* How gamers should secure their accounts from cyber attacks
* FBI recovers millions in ransom from DarkSide ransomware gang
* Kubernetes Clusters Targeted by Siloscape Malware
* 4 Ways For Employees To Distinguish Phishing Attacks
* How to perform a website security check- 6 tools to check website security
* Influence of technology on gaming industry

Naked Security

* How could the FBI recover BTC from Colonial's ransomware payment?
* Latvian woman charged with writing malware for the Trickbot Group
* How to hack into 5500 accounts… just using "credential stuffing"
* S3 Ep35: Apple chip flaw, Have I Been Pwned, and Covid tracker trouble [Podcast]
* "Have I Been Pwned" breach site partners with… the FBI!
* "Unpatchable" vuln in Apple's new Mac chip - what you need to know
* S3 Ep34: Apple bugs, scammers busted, and how crooks bypass 2FA [Podcast]
* Apple patches dangerous security holes, one in active use - update now!
* Eight suspects busted in raid on "home delivery" scamming operation
* Naked Security Live - Jacked and hacked: how safe are tracking tags?

Threat Post

* Mysterious Custom Malware Collects Billions of Stolen Data Points
* Intel Plugs 29 Holes in CPUs, Bluetooth, Security
* DarkSide Pwned Colonial With Old VPN Password
* Microsoft Patch Tuesday Fixes 6 In-The-Wild Exploits, 50 Flaws
* Lewd Phishing Lures Aimed at Business Explode
* TrickBot Coder Faces Decades in Prison
* Google Patches Critical Android RCE Bug
* 'An0m' Encrypted-Chat Sting Leads to Arrest of 800
* Billions of Compromised Records and Counting: Why the Application Layer is Still the Front Door for D
* Evil Corp Impersonates PayloadBin Group to Avoid Federal Sanctions

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

* 5 Global Supply Chain Security Threats (and How to Handle Them)
* Thoughts From a Data Security Expert: 3 Things That Keep Me Up at Night
* Cyber Gangs: Who Are They in 2021 and What Do They Want?
* Learning the Building Blocks You Need for Consumer Identity and Access Management Part 2: Engage
* Critical Business Operations Are At Risk, and Companies Are Not Making This a Priority
* Securing Your Cloud Transformation Journey
* Driving the Desire for FAIR: What Is Your 'Why' for Security Risk Quantification?
* The OSI Model and You Part 3: Stopping Threats at the OSI Network Layer
* How to Get on the CISO Certification Path
* Ransomware Attack Response Should Extend Beyond Money to Your Team's Morale

InfoWorld

* How to perform validation using PostSharp in C#
* Apple Xcode 13 supports teams, Swift concurrency
* Power Platform becomes the new Visual Basic
* How to choose a cloud-based CI/CD platform
* Apple Xcode Cloud brings CI/CD to Xcode IDE
* The public cloud could evolve like streaming services
* IBM Python toolkit measures AI uncertainty
* Go fuzz to catch hard-to-find bugs in Go
* 3 AI startups revolutionizing NLP
* Snowflake pushes back at… whom?

C4ISRNET - Media for the Intelligence Age Military

* DARPA's newest system kills drones with stringy streamers
* Army research budget focuses on tactical electronic warfare architecture
* With Austin's signature on JADC2 strategy, top general says it's 'delivery time'
* Cyber Command plans bigger budget for mission planning tool
* Space Force seeks $832 million in classified spending, new missions and more in annual wish list
* Multibeam antenna to improve communication passes first Air Force trials
* Now boarding: Space Force wants to turn launch ranges into rocket 'airports'
* Space Force will set up one office for commercial services, including SATCOM and satellite imagery
* The Air Force wants rocket deliveries to anywhere on Earth in under an hour
* Boeing bullish on battlefield communications market

The Hacker Corner

Conferences

* 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
* How To Secure Earned Cybersecurity Speaking Engagements
* World RPA & AI Summit | Interview with Ashley Pena

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.

* BCACTF 2.0
* Circle City Con CTF 2021
* THC CTF 2021
* FAUST CTF 2021
* HSCTF 8
* The Threat Interceptors Challenge
* CTF InterIUT 2021
* WeCTF 2021
* CTFZone 2021
* Hack-A-Sat 2 Qualifiers

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

* hacksudo: L.P.E.
* hacksudo: FOG
* Prime (2021): 2
* DriftingBlues: 9 (final)
* AdmX: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

* SQLMAP - Automatic SQL Injection Tool 1.5.6
* Flawfinder 2.0.17
* Wireshark Analyzer 3.4.6
* Zeek 4.0.2
* American Fuzzy Lop plus plus 3.13c
* Flawfinder 2.0.16
* Unicorn 1.0.3
* Sifter 12
* GRR 3.4.3.1
* I2P 0.9.50

Kali Linux Tutorials

* DivideAndScan : Divide Full Port Scan Results And Use It For Targeted Nmap Runs
* Endpoint Detection and Response: 6 Best Practices You Must Know About
* Qvm-Create-Windows-Qube : Spin Up New Windows Qubes Quickly, Effortlessly And Securely
* SQLFluff : A SQL Linter And Auto-Formatter For Humans
* AutoPentest DRL : Automated Penetration Testing Using Deep Reinforcement Learning
* ABPTTS : TCP Tunneling Over HTTP/HTTPS For Web Application Servers
* Etherblob Explorer : Search And Extract Blob Files On The Ethereum Blockchain Network
* Best WordPress Appointment Booking Plugins
* IPED : Digital Forensic Tool - Process And Analyze Digital Evidence
* Ghidra-Evm : Module For Reverse Engineering Smart Contracts

GBHackers Analysis

* Russian Hacker Jailed for Running a Darkweb Market Place that Sells Stolen Credit card Details
* Russian Hacker Group Nobelium Attack U.S Gov Agencies By Targeting 3,000 Email Accounts
* Hackers Exploited Fortinet Vulnerabilities to Gain Access of a U.S. Municipal Government Webserver
* 13 Vulnerabilities in Nagios Server Let Hackers Compromises The IT Infrastructure
* Scheme Flooding Let Hackers Identifying Users While Browsing Websites Including the Tor

Weekly Cyber Security Video and Podcasts

SANS DFIR

* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course
* Why take FOR500: Windows Forensic Analysis course OnDemand
* iOS Third Party Apps Analysis how to use the new reference guide poster

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

* Amazon Sidewalk is LIVE - Opt Out Now! - ThreatWire
* Hacking Hardware with @_MG_
* Cyber Crime, How Bad Can it Be? w/ Retia

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

* DNS for Cybersecurity
* Apply to Jobs You are UNDER QUALIFIED for - Tech Career Advice
* YOUR Addressable Market - Startup Life
* POLITICS in TECH is DANGEROUS - Startup Life

Security Now

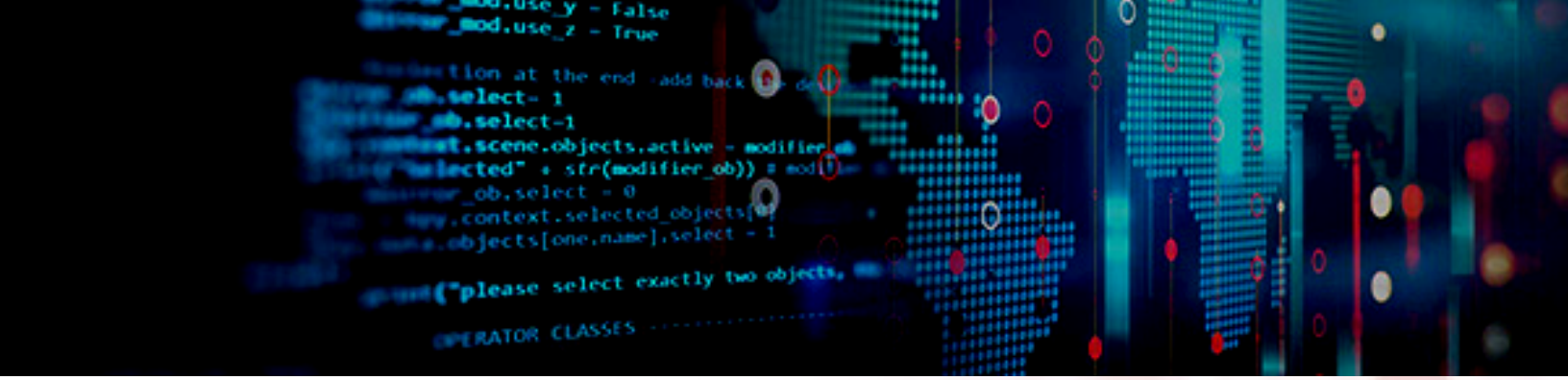
* Extrinsic Password Managers - Great CyberSecurity Awakening of 2021, NAT vs IPv6, Tavis Ormandy
* Epsilon Red - Chrome 91, Emsisoft's Ransomware Decryption Tool, Revisiting Amazon Sidewalk

Troy Hunt

* Weekly Update 246

Intel Techniques: The Privacy, Security, & OSINT Show

* 219-Tracking (Or Getting Tracked) with AirTags
* 218-Rebate Tracking (Privacy & OSINT)



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

* 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
* RiskIQ is Illuminating the Global Attack Surface With Next-Gen Security Intelligence
* Yanbian Gang Malware Continues with Wide-Scale Distribution and C2

FireEye

* [Security Nation] Jeff Man on Mapping the MITRE ATT&CK Framework Against PCI
* Akkadian Provisioning Manager Multiple Vulnerabilities Disclosure
* Patch Tuesday - June 2021
* Action! Start putting automation into practice.
* Kill chains: Part 2→Strategic and tactical use cases
* Metasploit Wrap-Up
* All about the boundaries: The cloud IAM lifecycle approach
* Proposed security researcher protection under CFAA
* Supreme Court narrows CFAA
* CVE-2021-3198 and CVE-2021-3540: MobileIron Shell Escape Privilege Escalation Vulnerabilities

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Internet Explorer jscript9.dll Memory Corruption
* WordPress Visitors-App 0.3 Cross Site Scripting
* FreeFloat FTP Server 1.0 Denial Of Service
* Backdoor.Win32.XRat.d Code Execution
* OpenCart 3.0.3.7 Cross Site Request Forgery
* Intelbras Router RF 301K Cross Site Request Forgery
* Backdoor.Win32.Wuca.nz Insecure Permissions
* COVID-19 Testing Management System 1.0 SQL Injection
* WordPress wpDiscuz 7.0.4 Remote Code Execution
* SAMI FTP Server 2.0.2 Denial Of Service
* Backup Key Recovery 2.2.7 Denial Of Service
* Nsauditor 3.2.3 Denial Of Service
* NBMonitor 1.6.8 Denial Of Service
* Trojan-Dropper.Win32.Googite.a Unauthenticated Open Proxy
* Rocket.Chat 3.12.1 NoSQL Injection / Code Execution
* IcoFX 2.6 Buffer Overflow
* OptiLink ONT1GEW GPON 2.1.11_X101 Remote Code Execution
* Backdoor.Win32.Wollf.12 Code Execution
* Sticky Notes And Color Widgets 1.4.2 Denial Of Service
* Grav CMS 1.7.10 Server-Side Template Injection
* Backdoor.Win32.Neakse.bit Insecure Permissions
* WordPress wpDiscuz 7.0.4 Shell Upload
* WordPress Smart Slider-3 3.5.0.8 Cross Site Scripting
* HealthForYou 1.11.1 / HealthCoach 2.9.2 Account Takeover
* HealthForYou 1.11.1 / HealthCoach 2.9.2 User Enumeration

CXSecurity

* FreeFloat FTP Server 1.0 Denial Of Service
* Rocket.Chat 3.12.1 NoSQL Injection / Code Execution
* IcoFX 2.6 Buffer Overflow
* SAMI FTP Server 2.0.2 Denial Of Service
* OptiLink ONT1GEW GPON 2.1.11_X101 Remote Code Execution
* Grav CMS 1.7.10 Server-Side Template Injection
* Microsoft RDP Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

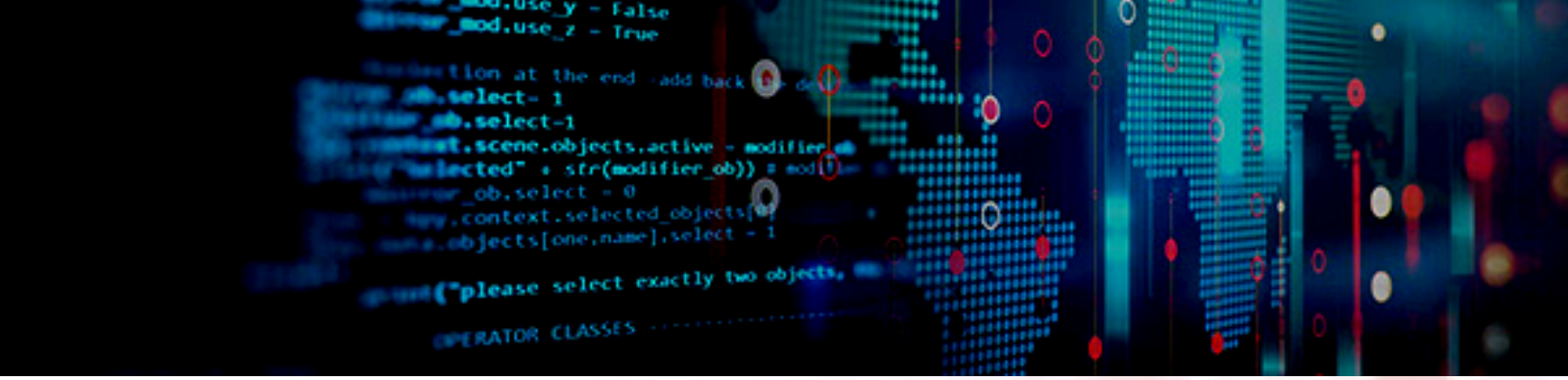
* [webapps] GravCMS 1.10.7 - Arbitrary YAML Write/Update (Unauthenticated) (2)
* [webapps] WordPress Plugin visitors-app 0.3 - 'user-agent' Stored Cross-Site Scripting (XSS)
* [webapps] OpenCart 3.0.3.6 - 'subject' Stored Cross-Site Scripting
* [webapps] OpenCart 3.0.3.7 - 'Change Password' Cross-Site Request Forgery (CSRF)
* [webapps] Intelbras Router RF 301K - 'DNS Hijacking' Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin wpDiscuz 7.0.4 - Remote Code Execution (Unauthenticated)
* [local] Backup Key Recovery 2.2.7 - Denial of Service (PoC)
* [dos] Nsauditor 3.2.3 - Denial of Service (PoC)
* [dos] NBMonitor 1.6.8 - Denial of Service (PoC)
* [webapps] Wordpress Plugin wpDiscuz 7.0.4 - Arbitrary File Upload (Unauthenticated)
* [webapps] Grav CMS 1.7.10 - Server-Side Template Injection (SSTI) (Authenticated)
* [webapps] Rocket.Chat 3.12.1 - NoSQL Injection to RCE (Unauthenticated)
* [local] IcoFX 2.6 - '.ico' Buffer Overflow SEH + DEP Bypass using JOP
* [webapps] WordPress Plugin Smart Slider-3 3.5.0.8 - 'name' Stored Cross-Site Scripting (XSS)
* [dos] Sticky Notes & Color Widgets 1.4.2 - Denial of Service (PoC)
* [webapps] OptiLink ONT1GEW GPON 2.1.11_X101 Build 1127.190306 - Remote Code Execution (Authenticated)
* [dos] My Notes Safe 5.3 - Denial of Service (PoC)
* [dos] Macaron Notes great notebook 5.5 - Denial of Service (PoC)
* [dos] Color Notes 1.4 - Denial of Service (PoC)
* [webapps] Gitlab 13.10.2 - Remote Code Execution (Authenticated)
* [webapps] Monstra CMS 3.0.4 - Remote Code Execution (Authenticated)
* [dos] Inkpad Notepad & To do list 4.3.61 - Denial of Service (PoC)
* [webapps] 4Images 1.8 - 'redirect' Reflected XSS
* [webapps] Gitlab 13.9.3 - Remote Code Execution (Authenticated)

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

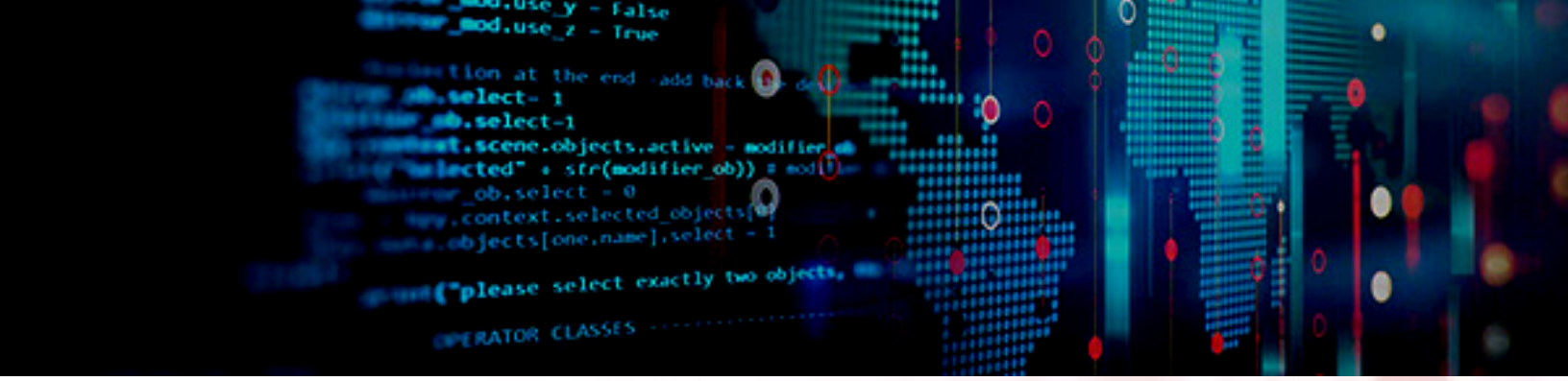
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://shpola-otg.gov.ua/er.php
http://shpola-otg.gov.ua/er.php notified by LahBodoAmat
http://nongthonmoihanoi.gov.vn/index.html
http://nongthonmoihanoi.gov.vn/index.html notified by Moroccan Revolution
https://rpp.pareparekota.go.id/index.htm
https://rpp.pareparekota.go.id/index.htm notified by 4nzeL4
https://humas.pareparekota.go.id/index.htm
https://humas.pareparekota.go.id/index.htm notified by 4nzeL4
https://ojs.stanford.edu/ojs/public/site/images/zabi/zabi.gif
https://ojs.stanford.edu/ojs/public/site/images/zabi/zabi.gif notified by Moroccan Revolution
http://www.iz.agricultura.sp.gov.br/bia/public/site/images/zabi/zabi.gif
http://www.iz.agricultura.sp.gov.br/bia/public/site/images/zabi/zabi.gif notified by Moroccan Revolution
http://www.publicaciones.inia.gob.ve/public/site/images/ksa/zabi.gif
http://www.publicaciones.inia.gob.ve/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://bagn.archivos.gob.mx/public/site/images/ksa/zabi.gif
https://bagn.archivos.gob.mx/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://revistaeletronica.fab.mil.br/public/site/images/ksa/zabi.gif
https://revistaeletronica.fab.mil.br/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://conferences.educ.ubc.ca/public/site/images/ksa/zabi.gif
https://conferences.educ.ubc.ca/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://www.iesalc.unesco.org/ess/public/site/images/ksa/zabi.gif
https://www.iesalc.unesco.org/ess/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://bm.akademisains.gov.my/asmsj/ojs/public/site/images/zbi/zabi.gif
https://bm.akademisains.gov.my/asmsj/ojs/public/site/images/zbi/zabi.gif notified by Moroccan Revolution
http://www.geosaberes.ufc.br/public/site/images/ksa/zabi.gif
http://www.geosaberes.ufc.br/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
http://revistaauditorium.jfrj.jus.br/public/site/images/ksa/zabi.gif
http://revistaauditorium.jfrj.jus.br/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://borobudur.kemdikbud.go.id/public/site/images/ksa/zabi.gif
https://borobudur.kemdikbud.go.id/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
https://www.review.neuroaro.gov.ng/public/site/images/ksa/zabi.gif
https://www.review.neuroaro.gov.ng/public/site/images/ksa/zabi.gif notified by Moroccan Revolution
http://www.mercator.ufc.br/public/site/images/ksa/zabi.gif
http://www.mercator.ufc.br/public/site/images/ksa/zabi.gif notified by Moroccan Revolution



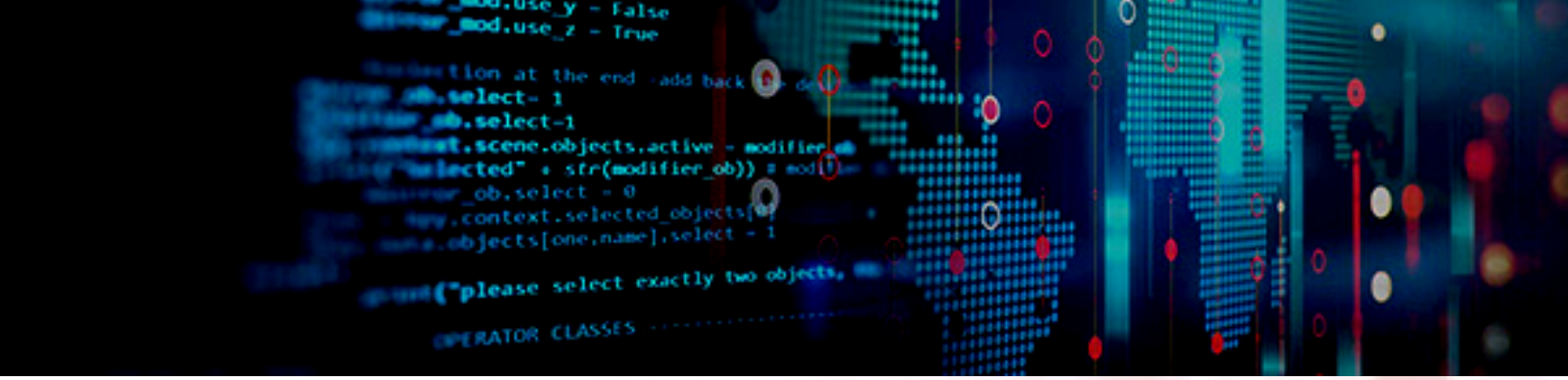
Dark Web News

Darknet Live

PayPal Closed Someone's Account for Running Tor Relays
PayPal apparently shut down a Tor supporter's account in response to activities supporting Tor, according to the EFF. (via darknetlive.com)
SK Police Arrest 500 for Alleged Darkweb Drug Transactions
The Seoul Metropolitan Police Agency apprehended more than 500 people suspected of buying or selling drugs on the darkweb. (via darknetlive.com)
Police Arrest an Alleged Meth Vendor in Sweden
Prosecutors in Skinnskatteberg, Sweden, have charged a man and woman from Uttersberg for manufacturing and selling methamphetamine on the darkweb. (via darknetlive.com)
Bitcoin ATM Owner Sentenced to Prison for Money Laundering
A man living in California was sentenced to federal prison for laundering up to $25 million through LocalBitcoins and a network of Bitcoin ATMs. (via darknetlive.com)

Dark Web Link

CP Possession Leads Nescopeck Man Face 100 Counts & Jail
A man from Nescopeck pleaded guilty in February to 100 counts of CP possession and he has been sentenced to complete up to two years in jail after his sentencing. The accused had been identified as Eric S. Williams of aged 41 years. He had appeared before Joseph F. Sklarosky Jr, Luzerne County Judge, for sentencing on [...] The post CP Possession Leads Nescopeck Man Face 100 Counts & Jail appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Dark Web Drug Dealing With Crypto Results In Suspects' Arrest
The Seoul police have revealed on Tuesday that they have recently cracked down on over 520 drug trafficking suspects involved in dark web drug dealing. The suspects are on the charges of buying, selling and distributing drugs over the darknet using the cryptocurrencies or digital coins. The Seoul Metropolitan Police Agency has stated that in [...] The post Dark Web Drug Dealing With Crypto Results In Suspects' Arrest appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Lotenal: Mexican Lottery Agency Keeps Mum On The Ransomware Attack
A group of malicious hackers have claimed that they have infiltrated the computer servers of Lotenal or National Lottery. They have also threatened to disclose confidential information in case the agency refuses to cooperate with the hackers. The hackers accessed the servers last Thursday, the 28th of May 2021. They had implemented the Avaddon ransomware. This malicious [...] The post Lotenal: Mexican Lottery Agency Keeps Mum On The Ransomware Attack appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* CISA Addresses the Rise in Ransomware Targeting Operational Technology Assets
* SAP Releases June 2021 Security Updates
* Adobe Releases Security Updates for Multiple Products
* Microsoft Releases June 2021 Security Updates
* Unpatched VMware vCenter Software
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Best Practices for Mapping to MITRE ATT&CKÂ®
* Mozilla Releases Security Updates for Firefox
* 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 May 31, 2021
* Vulnerability Summary for the Week of May 24, 2021

Zero Day Initiative Advisories

ZDI-CAN-13965: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13923: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13926: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13986: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13966: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13964: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13922: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13963: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13924: 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: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14022: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14033: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14034: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14024: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14020: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14014: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14021: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14016: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14018: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14015: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14017: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14023: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14019: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-14025: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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-13792: Delta Industrial Automation

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 'kimiya' was reported to the affected vendor on: 2021-06-09, 0 days ago. The vendor is given until 2021-10-07 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

Red Hat Security Advisory 2021-2360-01

Red Hat Security Advisory 2021-2360-01 - PostgreSQL is an advanced object-relational database management system. Issues addressed include an integer overflow vulnerability.

Ubuntu Security Notice USN-4986-1

Ubuntu Security Notice 4986-1 - It was discovered that rpcbind incorrectly handled certain large data sizes. A remote attacker could use this issue to cause rpcbind to consume resources, leading to a denial of service.

Red Hat Security Advisory 2021-2359-01

Red Hat Security Advisory 2021-2359-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2357-01

Red Hat Security Advisory 2021-2357-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2355-01

Red Hat Security Advisory 2021-2355-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, integer overflow, and out of bounds write vulnerabilities.

Red Hat Security Advisory 2021-2356-01

Red Hat Security Advisory 2021-2356-01 - Nettle is a cryptographic library that is designed to fit easily in almost any context: In crypto toolkits for object-oriented languages, such as C++, Python, or Pike, in applications like LSH or GNUPG, or even in kernel space.

Ubuntu Security Notice USN-4985-1

Ubuntu Security Notice 4985-1 - It was discovered that some Intel processors may not properly invalidate cache entries used by Intel Virtualization Technology for Directed I/O. This may allow a local user to perform a privilege escalation attack. Joseph Nuzman discovered that some Intel processors may not properly apply EIBRS mitigations and hence may allow unauthorized memory reads via sidechannel attacks. A local attacker could use this to expose sensitive information, including kernel memory. Various other issues were also addressed.

Red Hat Security Advisory 2021-2303-01

Red Hat Security Advisory 2021-2303-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2305-01

Red Hat Security Advisory 2021-2305-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2304-01

Red Hat Security Advisory 2021-2304-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2301-01

Red Hat Security Advisory 2021-2301-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2308-01

Red Hat Security Advisory 2021-2308-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2351-01

Red Hat Security Advisory 2021-2351-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.204 and .NET Runtime 5.0.7. Issues

addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2307-01

Red Hat Security Advisory 2021-2307-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2350-01

Red Hat Security Advisory 2021-2350-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 3.1.116 and .NET Runtime 3.1.16. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2306-01

Red Hat Security Advisory 2021-2306-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2300-01

Red Hat Security Advisory 2021-2300-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2353-01

Red Hat Security Advisory 2021-2353-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.204 and .NET Runtime 5.0.7. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2352-01

Red Hat Security Advisory 2021-2352-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 3.1.116 and .NET Runtime 3.1.16. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-2302-01

Red Hat Security Advisory 2021-2302-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2299-01

Red Hat Security Advisory 2021-2299-01 - The microcode_ctl packages provide microcode updates for Intel. Issues addressed include information leakage and privilege escalation vulnerabilities.

Red Hat Security Advisory 2021-2354-01

Red Hat Security Advisory 2021-2354-01 - The libwebp packages provide a library and tools for the WebP graphics format. WebP is an image format with a lossy compression of digital photographic images. WebP consists of a codec based on the VP8 format, and a container based on the Resource Interchange File Format. Webmasters, web developers and browser developers can use WebP to compress, archive, and distribute digital images more efficiently. Issues addressed include buffer overflow and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2328-01

Red Hat Security Advisory 2021-2328-01 - The Qt Image Formats in an add-on module for the core Qt Gui library that provides support for additional image formats including MNG, TGA, TIFF, WBMP, and WebP. Issues addressed include buffer overflow and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2323-01

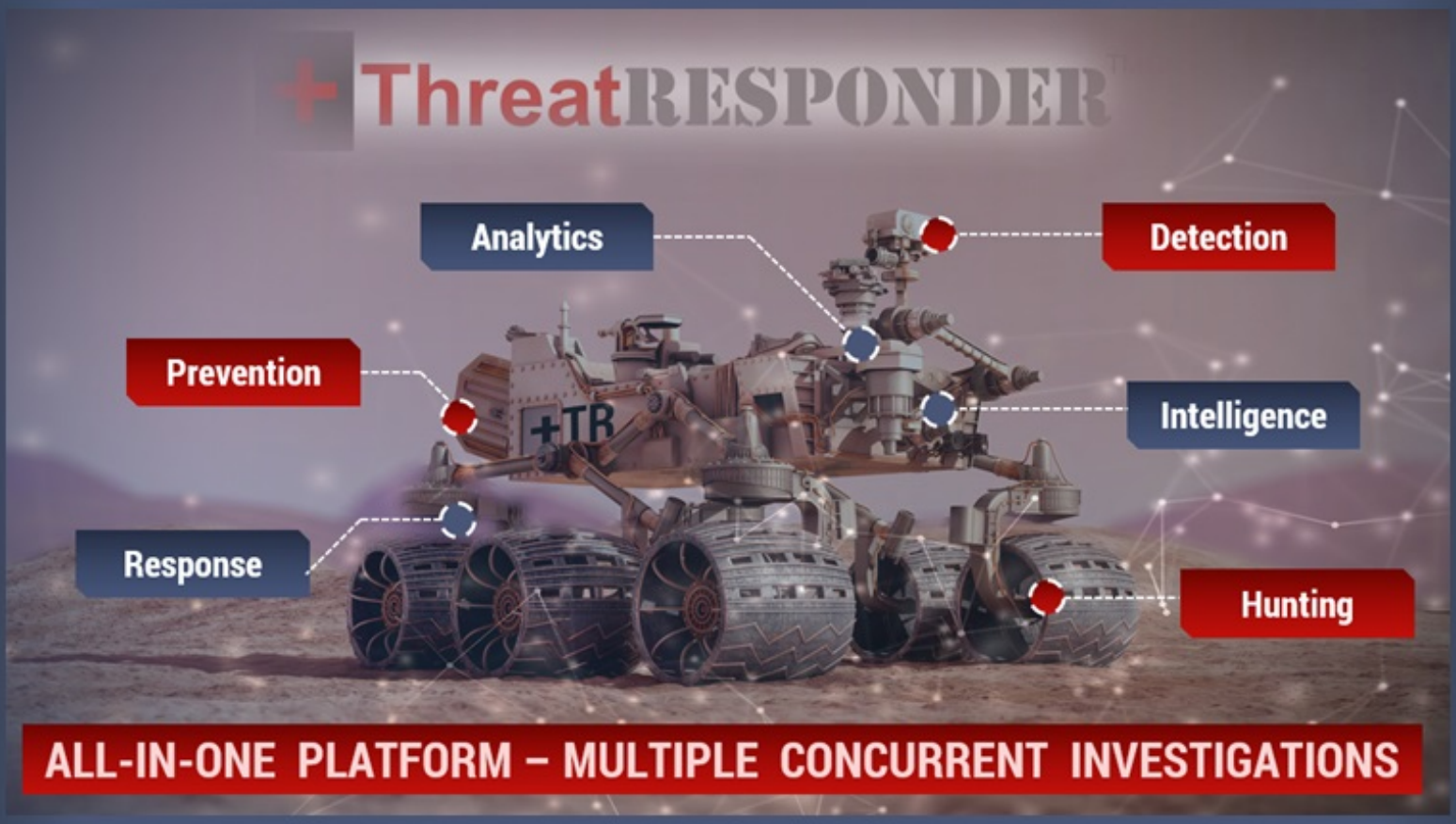
Red Hat Security Advisory 2021-2323-01 - 389 Directory Server is an LDAP version 3 compliant server. The base packages include the Lightweight Directory Access Protocol server and command-line utilities for server administration. Issues addressed include an information leakage vulnerability.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.1

Download here.

CSI Linux 2021.1 is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux 2021.1 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 2021.2 BETA Release:

CSI Linux 2021.2 Beta is now availible for those that have 2021.1 installed. To upgrade, open the CLI and type:
wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh

CSI Linux Tutorials for 2021.1:

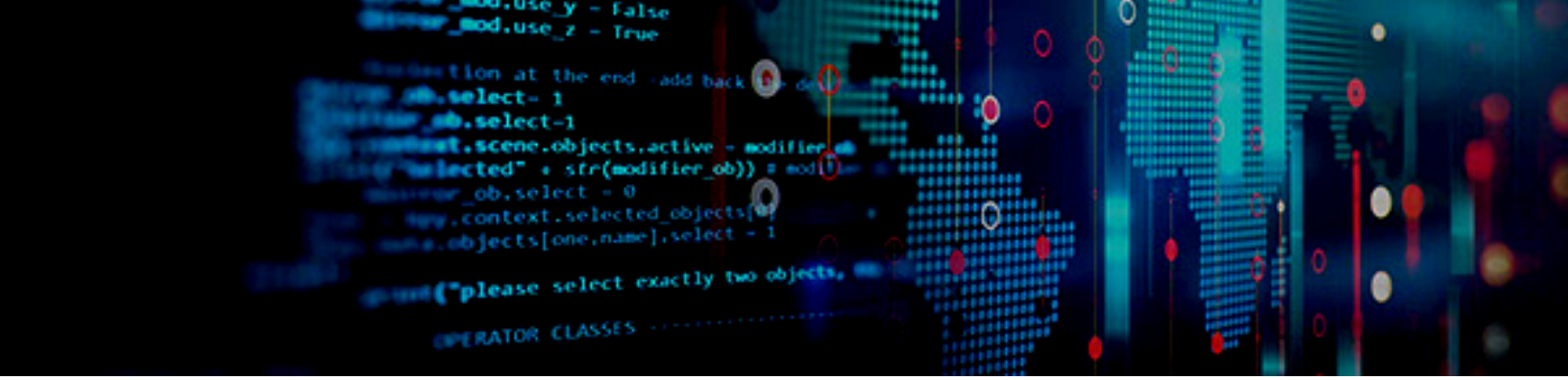
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

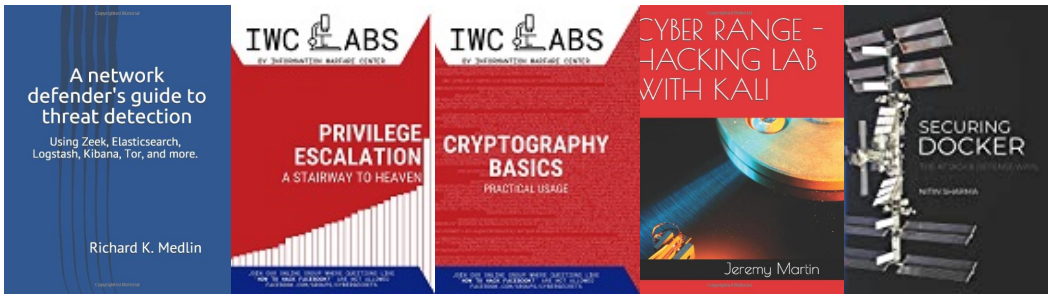


The Cyber Secrets publications on Amazon

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