Apr-12-21

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

April 12, 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

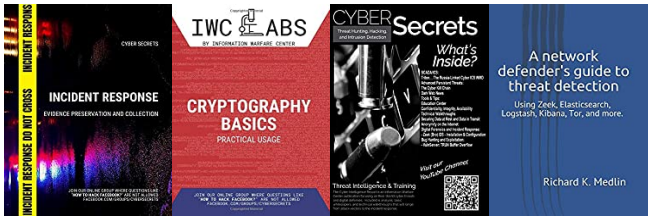
Internet Storm Center Infocon Status

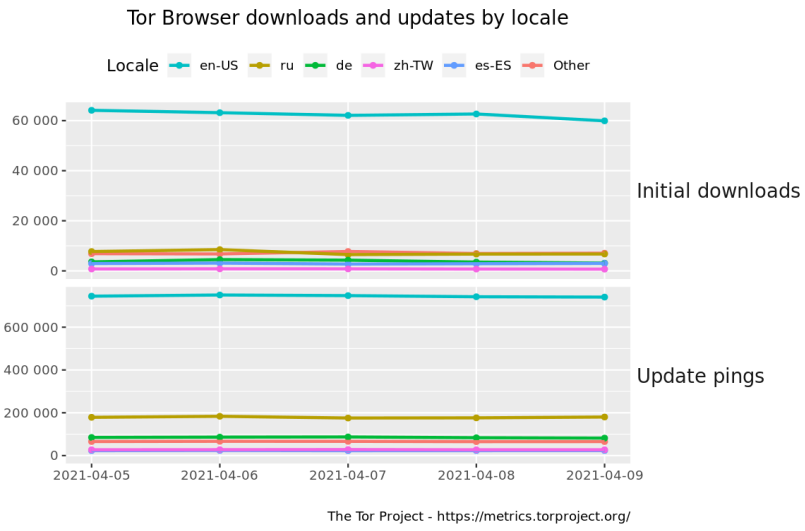
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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 is working on an updated set of tools. If you have any suggestions for additional capability or cahnges, please let the team know at support@csilinux.com

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

Index of Sections

Packet Storm Security

* Windows And Linux Devices Are Under Attack By A New Cryptomining Worm
* Facebook Says Data From 530M Users Was Obtained By Scraping
* Hackers Hit 9 Countries, Expose 623,036 Payment Card Records
* How Your Phone Can Be Hacked For $16
* Data From 500M LinkedIn Users Posted For Sale Online
* Critical Zoom Vulnerability Triggers Remote Code Execution Without User Input
* Tons Of PII Leaked Due To Swarmshop Hack
* Attackers Blowing Up Discord, Slack With Malware
* Should Firms Be More Worried About Firmware Cyber-Attacks?
* Ransomware Crooks Are Targeting Vulnerable VPN Devices
* Update On PHP Code Compromise: User Database Leak Suspected
* Apple Looking To Close Gap Between Web And App Privacy
* New Wormable Android Malware Poses As Netflix To Hijack WhatsApp Sessions
* San Jose Easter Church Service Hacked By Racist Hackers
* SAP Issues Advisory On Old Vulns Being Exploited
* LinkedIn Spear-Phishing Campaign Targets Job Hunters
* Fifteen Cybersecurity Pitfalls And Fixes For SMBs
* Encryption Debate Could Have Enterprise Security Implications
* The Cesspool Of The Internet Is To Be Found In A Village In North Holland
* Facebook Data For Over 500M Users Reportedly Leaks Online
* Technology Could Make Fighting COVID Less Restrictive But Privacy Will Take A Hit
* FBI: APTs Actively Exploiting Fortinet VPN Security Holes
* How To Check If Your Phone Number Is In The Huge Facebook Leak
* Dutch Watchdog Fines Booking.com 475,000 Euros For Keeping Customer Data Theft Quiet
* Legacy QNAP NAS Devices Vulnerable To Zero-Day Attack

Krebs on Security

* Are You One of the 533M People Who Got Facebooked?
* Ransom Gangs Emailing Victim Customers for Leverage
* Ubiquiti All But Confirms Breach Response Iniquity
* New KrebsOnSecurity Mobile-Friendly Site
* Whistleblower: Ubiquiti Breach "Catastrophic"
* No, I Did Not Hack Your MS Exchange Server
* Phish Leads to Breach at Calif. State Controller
* RedTorch Formed from Ashes of Norse Corp.
* Fintech Giant Fiserv Used Unclaimed Domain
* Can We Stop Pretending SMS Is Secure Now?

Dark Reading

* Wake Up and Smell the JavaScript
* Omdia Research Spotlight: XDR
* Unofficial Android App Store APKPure Infected With Malware
* CISA Launches New Threat Detection Dashboard
* Battle for the Endpoint
* 8 Security & Privacy Apps to Share With Family and Friends
* Women Are Facing an Economic Crisis & the Cybersecurity Industry Can Help
* Zoom Joins Microsoft Teams on List of Enterprise Tools Hacked at Pwn2Own
* Fraudsters Use HTML Legos to Evade Detection in Phishing Attack
* 600K Payment Card Records Leaked After Swarmshop Breach
* Handcuffs Over AI: Solving Security Challenges With Law Enforcement
* SecOps and DevOps: From Cooperation to Automation
* Did 4 Major Ransomware Groups Truly Form a Cartel?
* Voice-Changing Software Found on APT Attackers' Server
* Cring Ransomware Used in Attacks on European Industrial Firms
* Fortune 500 Security Shows Progress and Pitfalls
* Rethinking Cyberattack Response: Prevention & Preparedness
* 5 Ways to Transform Your Phishing Defenses Right Now
* Attackers Actively Seeking, Exploiting Vulnerable SAP Applications
* Cartoon Caption Winner: Something Seems Afoul

The Hacker News

* What Does It Take To Be a Cybersecurity Researcher?
* Windows, Ubuntu, Zoom, Safari, MS Exchange Hacked at Pwn2Own 2021
* Hackers Tampered With APKPure Store to Distribute Malware Apps
* Alert - There's A New Malware Out There Snatching Users' Passwords
* [WHITEPAPER] How to Achieve CMMC Security Compliance for Your Business
* Cisco Will Not Patch Critical RCE Flaw Affecting End-of-Life Business Routers
* Gigaset Android Update Server Hacked to Install Malware on Users' Devices
* Researchers uncover a new Iranian malware used in recent cyberattacks
* Hackers Exploit Unpatched VPNs to Install Ransomware on Industrial Targets
* NIST and HIPAA: Is There a Password Connection?
* PHP Site's User Database Was Hacked In Recent Source Code Backdoor Attack
* Android to Support Rust Programming Language to Prevent Memory Flaws
* WhatsApp-based wormable Android malware spotted on the Google Play Store
* 11 Useful Security Tips for Securing Your AWS Environment
* Critical Auth Bypass Bug Found in VMware Data Center Security Product

Security Week

* Iran Blames Israel for Sabotage at Natanz Nuclear Site
* Cybersecurity M&A Roundup for April 1-11, 2021
* Fed Chair Says Cyberattacks Main Risk to US Economy
* Zerodium Offering $300,000 for WordPress Exploits
* Iran Calls Natanz Atomic Site Blackout 'Nuclear Terrorism'
* Microsoft Open-Sources 'CyberBattleSim' Enterprise Environment Simulator
* CISA Releases Tool to Detect Microsoft 365 Compromise
* Security Automation Firm Tines Raises $26 Million at $300 Million Valuation
* LG Promises Three Years of OS Updates for Premium Android Smartphones
* Pwn2Own 2021 Participants Earn Over $1.2 Million for Their Exploits
* Collaboration Platforms Increasingly Abused for Malware Distribution, Data Exfiltration
* Cisco Patches Critical Flaw in SD-WAN vManage
* Cost of Sandboxing Prompts Shift to Memory-Safe Languages. A Little Too Late?
* Library Dependencies and the Open Source Supply Chain Nightmare
* Belden Says Health-Related Information Exposed in Data Breach
* Cring Ransomware Targets Industrial Organizations
* PHP Developers Share Update on Recent Breach
* $200,000 Awarded for Zero-Click Zoom Exploit at Pwn2Own
* Vulnerability in 'Domain Time II' Could Lead to Server, Network Compromise
* Open Source Security Management Firm WhiteSource Raises $75 Million

Infosecurity Magazine

* Europol: "Virtually All" Crime Now Has a Digital Element
* Brits Still Confused by Multi-Factor Authentication
* Over 90% of Organizations Hit by a Mobile Malware Attack in 2020
* Man Arrested After Failed AWS Bomb Plot
* Facebook Removes 16k Groups for Trading Fake Reviews
* US Jails Cyber-stalker Who Targeted Attack Survivor
* LifeLabs Launches Vulnerability Disclosure Program
* NCSC: Large Number of Brits Are Using Easily Guessable Passwords
* Learning from Recent Insider Data Breaches
* #COVID19 Fraud Surge Threatens to Overwhelm Banks
* Hackers Hacked as Underground Carding Site is Breached
* UK Firms Suffer Record Number of Cyber-Attacks in Q1

KnowBe4 Security Awareness Training Blog RSS Feed

* [HEADS UP] DocuSign Issues Alert of Malicious New Hacking Tool
* H Layer Credentialing Announces Security Awareness and Culture Professional (SACP)Â® Certification
* Australian Organizations Increase Cyber Security Spend to Nearly A$5B in 2021
* The Digital Workplace is a Cybersecurity Disaster!
* APT Group Use Voice-Changing Software to Impersonate Women as Part of Espionage Attacks
* New Phishing Attacks Bypass Secure Email Gateways Using Some Very Creative Methods
* LinkedIn Data of 500 Million Users Hacked, Up For Sale: Report
* Phishing Attacks Using PDF Files Have Skyrocketed
* The Clop #Ransomware gang is now pressuring customers of victims threatening that their persona
* The Growing WeTransfer Phishing Campaign Can Put Your Users at Risk

ISC2.org Blog

* Wanted: Software Developers with a Security Mindset
* Deadline is Extended for 2021(ISC)² Global Achievement Awards Nominations!
* Hush - This Data Is Secret
* Under the Hood: Inside (ISC)² Exam Development Cycle
* CISSPs from Around the Globe: An Interview with Mari Aoba

HackRead

* 6-year-old Moodle flaw exposed millions to account takeover attack
* Scraped data of 1.3 million Clubhouse users published online
* Android apps on APKPure store caught spreading malware
* 2 scraped LinkedIn databases with 500m and 827m records sold online
* Facebook ads dropped malware posing as Clubhouse app for PC
* Hackers leak data, 600k card info from Swarmshop cybercrime forum
* Unpatched vulnerable VPN servers hit by Cring ransomware

Koddos

* 6-year-old Moodle flaw exposed millions to account takeover attack
* Scraped data of 1.3 million Clubhouse users published online
* Android apps on APKPure store caught spreading malware
* 2 scraped LinkedIn databases with 500m and 827m records sold online
* Facebook ads dropped malware posing as Clubhouse app for PC
* Hackers leak data, 600k card info from Swarmshop cybercrime forum
* Unpatched vulnerable VPN servers hit by Cring ransomware

Naked Security

* Naked Security Live - How to spot "government" scammers
* Pwn2Own 2021: Zoom, Teams, Exchange, Chrome and Edge "fully owned"
* Italian charged with hiring "dark web hitman" to murder his ex-girlfriend
* S3 Ep27: Census scammers, beg bounties and data breach fines [Podcast]
* Too slow! Booking.com fined for not reporting data breach fast enough
* Criminals send out fake "census form" reminder - don't fall for it!
* S3 Ep26: Apple 0-day, crypto vulnerabilities and PHP backdoor [Podcast]
* PHP web language narrowly avoids "backdoor" supply chain attack
* Naked Security Live - Lessons beyond ransomware
* Serious Security: OpenSSL fixes two high-severity crypto bugs

Threat Post

* DOJ: Creep Coach Finagles Nude Athlete Photos
* 623M Payment Cards Stolen from Cybercrime Forum
* Network Detection & Response: The Next Frontier in Fighting the Human Problem
* Data from 500M LinkedIn Users Posted for Sale Online
* Adware Spreads via Fake TikTok App, Laptop Offers
* Zero-Day Bug Impacts Problem-Plagued Cisco SOHO Routers
* IcedID Banking Trojan Surges: The New Emotet?
* Azure Functions Weakness Allows Privilege Escalation
* Hackers Exploit Fortinet Flaw in Sophisticated Cring Ransomware Attacks
* Attackers Blowing Up Discord, Slack with Malware

Null-Byte

* Master Python, Linux & More with This Training Bundle
* Make Spoofed Calls Using Any Phone Number You Want Right from Your Smartphone
* Master Excel with This Certification Bundle
* Play Wi-Fi Hacking Games Using Microcontrollers to Practice Wi-Fi Attacks Legally
* This Python Bundle Can Teach You Everything You Need to Know
* How to Use a Directional Antenna with ESP8266-Based Microcontroller
* Master the Internet of Things with This Certification Bundle
* There Are Hidden Wi-Fi Networks All Around You - These Attacks Will Find Them
* Rank Up in Google Searches with This SEO Couse Bundle
* How to Generate Crackable Wi-Fi Handshakes with an ESP8266-Based Test Network

IBM Security Intelligence

* New Ransomware Threats Are Getting Bolder: How to Rewrite the Script
* How Vulnerability Management Can Stop a Data Breach
* Why E-Commerce Security Matters Now More Than Ever
* Using the Threat Modeling Manifesto to Get Your Team Going
* What Does Modern Even Mean? How to Evaluate Data Security Solutions for the Hybrid Cloud and Beyond
* Perpetual Disruption Part 1: What is Good Cybersecurity Governance in Health Care?
* Cookie Hijacking: More Dangerous Than it Sounds
* Software Composition Analysis: Developers' Security Silver Bullet
* IBM Named a Strong Performer in The Forrester Waveâ„¢: External Threat Intelligence Services, Q1 2021
* Clean Sweep: A 30-Day Guide to a New Cybersecurity Plan

InfoWorld

* Packing safety intelligence into robots' AI brains
* How to excel with data analytics
* 5 perspectives on modern data analytics
* What's new in Microsoft .NET 6
* Google Android team embraces Rust for Android OS development
* 3 multicloud architecture mistakes
* Microsoft open sources C# standards work
* The pesky reality of multicloud
* What is unified policy as code, and why do you need it?
* The decline of Heroku

C4ISRNET - Media for the Intelligence Age Military

* US sanctions makers of supercomputers linked to Chinese military
* 7 allies sign onto polar research project
* JAIC director: With flat budgets, turn to AI to save money
* Space Force unveils plans for Space Systems Command
* Perspecta Labs wins $8.1 million in 5G contracts
* Raytheon awarded $15.5 million to upgrade laser weapon
* Defense Intelligence Agency continues progress on MARS database
* US Cyber Command looks for networking support from industry
* CAES signs exclusive agreement for 3D-printed radio frequency parts
* Valkyrie drone launches even smaller drone from inside payload bay

The Hacker Corner

Conferences

* 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
* The State of AI in Cybersecurity | Interview with Jessica Gallagher
* AWSN Women in Security Awards | Interview with Abigail Swabey
* An Introduction to Cybersecurity Call for Papers

Google Zero Day Project

* Who Contains the Containers?
* In-the-Wild Series: October 2020 0-day discovery

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.

* _EVENT CHANGED_
* HackPack CTF 2021
* Incognito 2.0
* PlaidCTF 2021
* UMDCTF 2021
* Bambi CTF #5
* Cyber Apocalypse 2021
* Securebug.se CTF Odin 2021
* S4CTF 2021
* TAMUctf 2021

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

* BlueMoon: 2021
* Bluesmoke: devrandom2
* shenron: 2
* hacksudo: aliens
* blogger: 1

Tools & Techniques

Packet Storm Security Tools Links

* GRAudit Grep Auditing Tool 2.9
* Clam AntiVirus Toolkit 0.103.2
* Global Socket 1.4.29
* SQLMAP - Automatic SQL Injection Tool 1.5.4
* Global Socket 1.4.28
* Faraday 3.14.3
* Scapy Packet Manipulation Tool 2.4.5rc1
* OpenSSL Toolkit 1.1.1k
* American Fuzzy Lop plus plus 3.12c
* Global Socket 1.4.27

Kali Linux Tutorials

* DefenderCheck : Identifies The Bytes That Microsoft Defender Flags On
* SharpGPOAbuse : Tool To Take Advantage Of A User's Edit Rights On A Group Policy Object (GPO)
* TUF : A Framework For Securing Software Update Systems
* SecretScanner : Find Secrets & Passwords In Container Images And File Systems
* InveighZero : Windows C# LLMNR/mDNS/NBNS/DNS/DHCPv6 Spoofer/Man-In-The-Middle Tool
* ClearURLs : Automatically Remove Tracking Elements From URLs
* Android_Hid : Use Android As Rubber Ducky Against Another Android Device
* Kics : Find Security Vulnerabilities & Compliance Issues
* Boomerang : A Tool To Expose Multiple Internal Servers To Web/Cloud
* BadOutlook : Malicious Outlook Reader

GBHackers Analysis

* New Malicious Document Builder Named "EtterSilent" Used by Top Hackers Groups
* Flaws with Ovarro's TBox Remote Terminal Units Opens Industrial Systems For Remote Attacks
* Critical "Netmask" npm Package Flaw Affects Hundreds of Thousands of Applications
* Facebook Blocks Chinese Hackers Using Fake Person as Targeting Uyghur Activists
* Google Warns of a New Android Zero-Day Vulnerability Is Under Active Attack

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 193: Fixing the Internet - Feedback Responses 2
* iOS Third Party Apps Analysis how to use the new reference guide poster
* Episode 192: Fixing the Internet - Feedback Responses 1
* Episode 191: SANS DFIR Summit 2021 Call For Papers

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

* Powering All The Things w/USB Type C -GlytchTips
* IoT-less IP Cameras - Hack Across America 2021
* 553 Million Affected In Facebook Leak, Call of Duty: Warzone Cheats are Actually Malware- ThreatWire

The PC Security Channel [TPSC]

* Bitdefender vs Kaspersky: Ransomware Test
* Best Firewall for Windows

Eli the Computer Guy

* YOUTUBE FAIL - TEACHING KIDS TO MAKE DRUGS is MONETIZABLE
* AMAZON FAIL - TWITTER ACCOUNT not HACKED
* INTEL FAIL - TSMC INVESTING 100 BILLION in CHIPS
* RUBY on RAILS FAIL - GPL Licensing Screw Up

Security Now

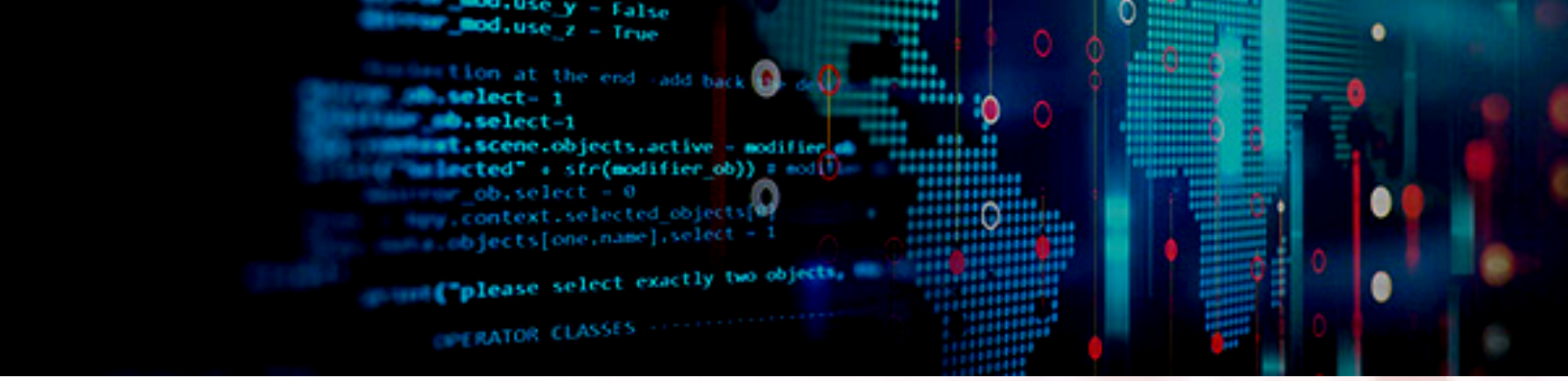
* A Spy in Our Pocket - Ubiquity Coverup, Facebook Data Dump, Malicious Call of Duty Cheats
* GIT Me Some PHP - Spectre Returns to Linux, API Security, OpenSSL Flaws, SolarWinds

Troy Hunt

* Weekly Update 238

Intel Techniques: The Privacy, Security, & OSINT Show

* 213-Hashes 101
* 212-Vital Privacy, Security, & OSINT Updates



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

* Yanbian Gang Malware Continues with Wide-Scale Distribution and C2
* Agent Tesla: Software-as-a-Service Enables Trend Analysis
* RiskIQ Named a Strong Performer in The Forrester Waveâ„¢: External Threat Intelligence Services, Q1 2
* A Vulnerable World: RiskIQ's Unique View of the Microsoft Exchange Landscape
* Cryptocurrency: A Boom in Value Begets a Boom in Crime
* Microsoft Exchange Server Remote Code Execution Vulnerability: RiskIQ's Response
* Turkey Dog Continues to Target Turkish Speakers with RAT Trojans via COVID Lures
* Threat Hunting in a Post-WHOIS World
* The Business of LogoKit: The Actors and Marketing Behind a Popular Phishing Tool
* 2020 Mobile App Threat Landscape: New Threats Arise, But the Ecosystem Got Safer

FireEye

* MDR Must-Haves, Part 6: Threat Validation and Detailed Reporting
* Metasploit Wrap-Up
* MDR Vendor Must-Haves, Part 5: Multiple Threat Detection Methodologies, Including Deep Attacker Behav
* What's New in InsightIDR: Q1 2021 in Review
* Attackers Targeting Fortinet Devices and SAP Applications
* Kubernetes Namespaces Are Not as Secure as You Think
* Looking Back and Moving Forward With Rapid7's Cloud Security Solution
* MDR Vendor Must-Haves, Part 4: Ingestion of Authentication Data Across Local, Domain, and Cloud Sourc
* Rapid7 Releases New Industry Cyber-Exposure Report (ICER): Fortune 500
* InsightIDR's Log Search: Recent Enhancements and Upcoming Investments

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Google Chrome SimplfiedLowering Integer Overflow
* PrestaShop 1.7.6.7 SQL Injection
* Tableau Server Open Redirection
* Backdoor.Win32.Small.n Code Execution
* DMA Radius Manager 4.4.0 Cross Site Request Forgery
* Check Point Identity Agent Arbitrary File Write
* D-Link DSL-320B-D1 Pre-Authentication Buffer Overflow
* Backdoor.Win32.Hupigon.das Unauthenticated Open Proxy
* Linux Kernel 5.4 BleedingTooth Remote Code Execution
* Trojan.Win32.Hotkeychick.d Insecure Permissions
* Composr 10.0.36 Shell Upload
* Trojan-Downloader.Win32.Genome.qiw Insecure Permissions
* Trojan-Downloader.Win32.Genome.omht Insecure Permissions
* Trojan.Win32.Hosts2.yqf Insecure Permissions
* CMSimple 5.2 Cross Site Scripting
* Gogs Git Hooks Remote Code Execution
* Gitea Git Hooks Remote Code Execution
* iOS / macOS Radio Proximity Kernel Memory Corruption
* Monospace Directus Headless CMS File Upload / Rule Bypass
* Ignition 2.5.1 Remote Code Execution
* Composr CMS 10.0.36 Cross Site Scripting
* Dell OpenManage Server Administrator 9.4.0.0 File Read
* Atlassian Jira Service Desk 4.9.1 Cross Site Scripting
* Google Chrome 86.0.4240 V8 Remote Code Execution
* Google Chrome 81.0.4044 V8 Remote Code Execution

CXSecurity

* Ignition 2.5.1 Remote Code Execution
* PrestaShop 1.7.6.7 SQL Injection
* Linux Kernel 5.4 BleedingTooth Remote Code Execution
* F5 iControl Server-Side Request Forgery / Remote Command Execution
* ScadaBR 1.0 Arbitrary File Upload Authenticated
* vsftpd 3.0.3 Denial Of Service
* Project Expense Monitoring System 1.0 SQL Injection

Proof of Concept (PoC) & Exploits

Exploit Database

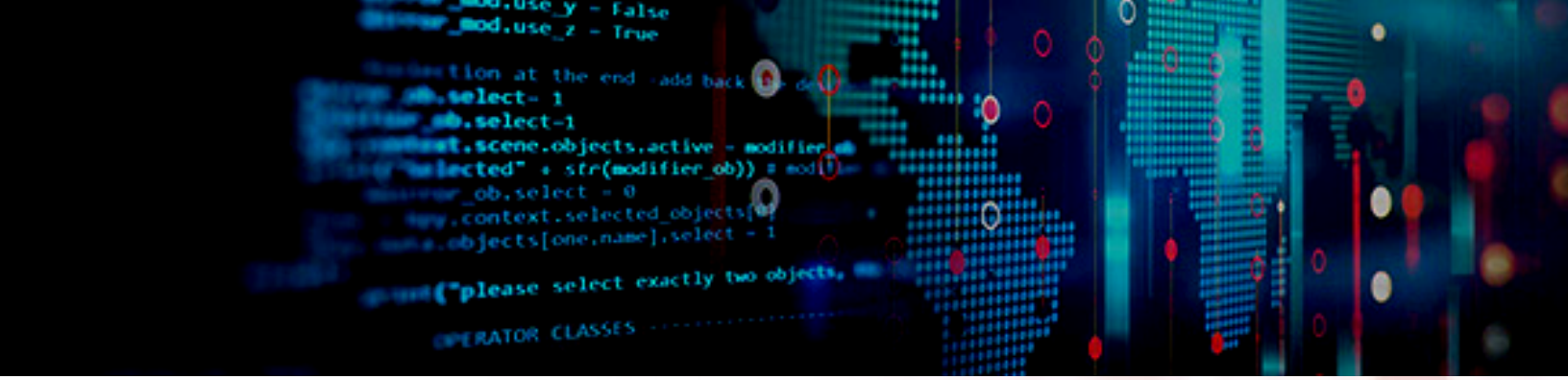
* [remote] vsftpd 2.3.4 - Backdoor Command Execution
* [webapps] PrestaShop 1.7.6.7 - 'location' Blind Sql Injection
* [remote] Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution
* [webapps] Composr 10.0.36 - Remote Code Execution
* [webapps] DMA Radius Manager 4.4.0 - Cross-Site Request Forgery (CSRF)
* [webapps] CMSimple 5.2 - 'External' Stored XSS
* [webapps] Dell OpenManage Server Administrator 9.4.0.0 - Arbitrary File Read
* [webapps] Composr CMS 10.0.36 - Cross Site Scripting
* [webapps] Atlassian Jira Service Desk 4.9.1 - Unrestricted File Upload to XSS
* [webapps] Mini Mouse 9.3.0 - Local File inclusion / Path Traversal
* [remote] Google Chrome 81.0.4044 V8 - Remote Code Execution
* [remote] Google Chrome 86.0.4240 V8 - Remote Code Execution
* [webapps] Mini Mouse 9.2.0 - Path Traversal
* [webapps] Mini Mouse 9.2.0 - Remote Code Execution
* [webapps] OpenEMR 4.1.0 - 'u' SQL Injection
* [webapps] Basic Shopping Cart 1.0 - Authentication Bypass
* [webapps] Simple Food Website 1.0 - Authentication Bypass
* [local] Rockstar Service - Insecure File Permissions
* [webapps] F5 BIG-IP 16.0.x - iControl REST Remote Code Execution (Unauthenticated)
* [webapps] ZBL EPON ONU Broadband Router 1.0 - Remote Privilege Escalation
* [webapps] phpPgAdmin 7.13.0 - COPY FROM PROGRAM Command Execution (Authenticated)
* [webapps] ScadaBR 1.0 - Arbitrary File Upload (Authenticated) (2)
* [webapps] ScadaBR 1.0 - Arbitrary File Upload (Authenticated) (1)
* [webapps] Latrix 0.6.0 - 'txtaccesscode' SQL Injection

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*

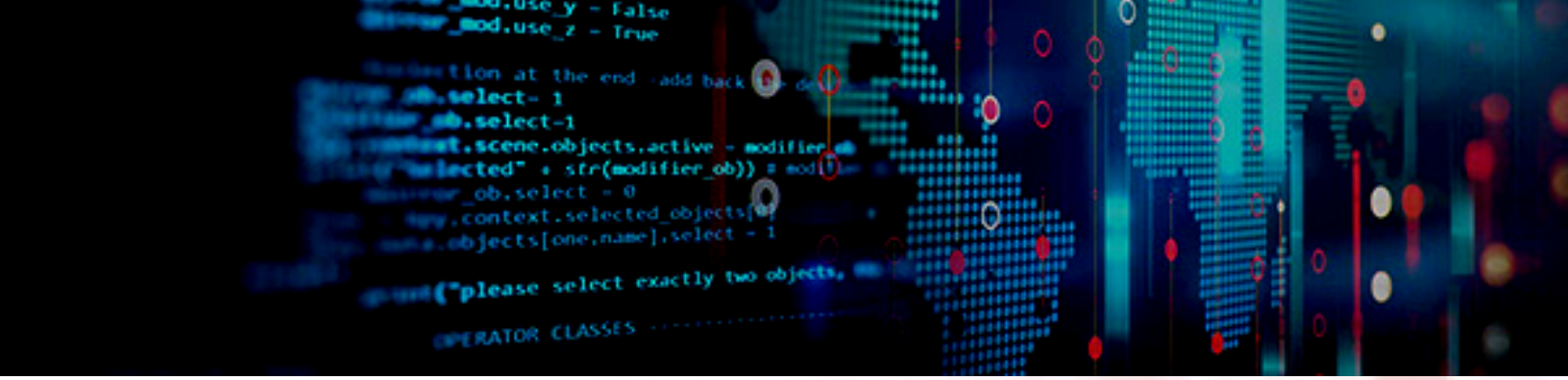
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.lajeado.to.gov.br
https://www.lajeado.to.gov.br notified by Paraná Cyber Mafia
https://www.natividade.to.gov.br
https://www.natividade.to.gov.br notified by Paraná Cyber Mafia
https://www.centenario.to.gov.br
https://www.centenario.to.gov.br notified by Paraná Cyber Mafia
https://www.pugmil.to.gov.br
https://www.pugmil.to.gov.br notified by Paraná Cyber Mafia
https://difcuencame.gob.mx/o.txt
https://difcuencame.gob.mx/o.txt notified by Black_X12
http://rsap.palukota.go.id
http://rsap.palukota.go.id notified by Moroccan Revolution
https://dnbc.gov.co/aex.html
https://dnbc.gov.co/aex.html notified by ./KeyzNet
https://hukum.bondowosokab.go.id/e.htm
https://hukum.bondowosokab.go.id/e.htm notified by /Rayzky_
https://dprd.bondowosokab.go.id/e.htm
https://dprd.bondowosokab.go.id/e.htm notified by /Rayzky_
https://www.konya.bel.tr/bldfoto/index.php
https://www.konya.bel.tr/bldfoto/index.php notified by Ren4Sploit
http://www.municipiotuxtepec.gob.mx/v.html
http://www.municipiotuxtepec.gob.mx/v.html notified by Mr V
http://phpmyadmin.ketapangkab.go.id
http://phpmyadmin.ketapangkab.go.id notified by KAKEGURAI
http://inspektorat.ketapangkab.go.id
http://inspektorat.ketapangkab.go.id notified by KAKEGURAI
http://dispora.ketapangkab.go.id
http://dispora.ketapangkab.go.id notified by KAKEGURAI
http://bpbd.ketapangkab.go.id
http://bpbd.ketapangkab.go.id notified by KAKEGURAI
http://bkpsdm.ketapangkab.go.id
http://bkpsdm.ketapangkab.go.id notified by KAKEGURAI
http://satpolpp.ketapangkab.go.id
http://satpolpp.ketapangkab.go.id notified by KAKEGURAI



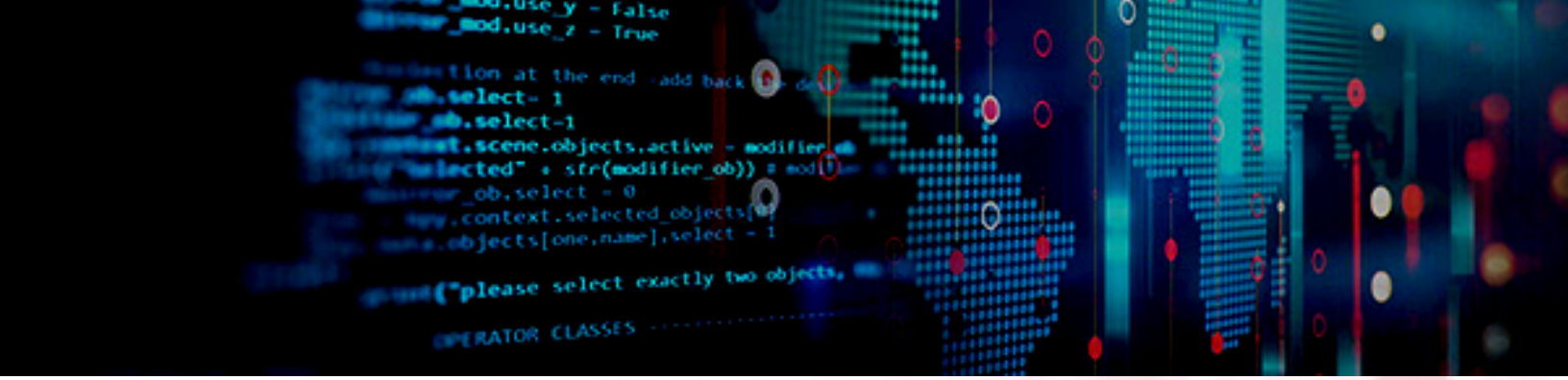
Dark Web News

Darknet Live

Signal's Cryptocurrency Integration Seems Suspicious
Signal has partnered with a cryptocurrency organization that believes the government has a role in regulating crypto transactions. (via darknetlive.com)
Hacked EncroChat Messages Used in MDMA Vendor Bust
Police in the United Kingdom analyzed hacked EncroChat messages to identify a prolific darkweb vendor. (via darknetlive.com)
Finnish MDMA Vendor Sentenced for Selling on Darkweb Markets
The Helsinki District Court imprisoned a Finnish man for conspiring with others to import drugs and sell them through darkweb markets. (via darknetlive.com)
Irish Drug Dealer Avoids Prison in Marijuana Distribution Case
An Irish man was given a suspended prison sentence after he admitted purchasing marijuana on the darkweb to resell. He also admitted laundering â,¬26,000. (via darknetlive.com)

Dark Web Link

SwarmShop Hack: Over 600,000 Stolen Credit Card Details Leaked
Hacking the underground marketplaces is nothing new, and this time it has acquired its latest victim, SwarmShop. A massive database from the SwarnShop carding market on the clearnet containing more than 600,000stolen credit card details have been leaked on another forum. The data leak contains the records of the whole SwarmShop community, adding to which all the [...] The post SwarmShop Hack: Over 600,000 Stolen Credit Card Details Leaked appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Man Arrested Trying To Cripple Ex-Girlfriend Using Dark Web Hitman
The Italian police had mentioned on Wednesday that they had prevented a nightmare plot. The police had arrested a man who deliberately wanted his ex-girlfriend disfigured with acid and crippled by a dark web hitman. The Roman police believe the hitman-for-hire plan could be based on a "contemporary thriller movie”. They are said to have [...] The post Man Arrested Trying To Cripple Ex-Girlfriend Using Dark Web Hitman appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Darknet Chemical Weapon: Missouri Man Attempts To Murder 300 People
A Missouri resident who had been accused of attempting to buy a darknet chemical weapon capable of taking the lives of hundreds of people had received his sentencing. The Columbian man, identified as Jason Siesser and aged 46 years, had pleaded the previous year for attempting to acquire a darknet chemical weapon alongside aggravated identity theft. He [...] The post Darknet Chemical Weapon: Missouri Man Attempts To Murder 300 People appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Using Aviary to Analyze Post-Compromise Threat Activity in M365 Environments
* Cisco Releases Security Updates for Multiple Products
* Malicious Cyber Activity Targeting Critical SAP Applications
* VMware Releases Security Update
* FBI-CISA Joint Advisory on Exploitation of Fortinet FortiOS Vulnerabilities
* CISA Releases Supplemental Direction on Emergency Directive for Microsoft Exchange Server Vulnerabili
* Google Releases Security Updates for Chrome
* VMware Releases Security Updates
* AA21-077A: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
* AA21-076A: TrickBot Malware
* Vulnerability Summary for the Week of March 29, 2021
* Vulnerability Summary for the Week of March 22, 2021

Zero Day Initiative Advisories

ZDI-CAN-13574: Foxit
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: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13497: Microsoft
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 'L4' was reported to the affected vendor on: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13573: Foxit
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: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13582: 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: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13572: Foxit
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: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13448: Adobe

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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13583: 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: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13088: Adobe

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13454: Adobe

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 'Anonymous' was reported to the affected vendor on: 2021-04-02, 10 days ago. The vendor is given until 2021-07-31 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-13525: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13529: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13527: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13528: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13530: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13526: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13538: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13537: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13524: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13539: Adobe

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 (@mrpowell) & Joshua Smith (@kernelsmith) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-12683: D-Link

A CVSS score 8.8 (AV:A/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: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13333: 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 'cor3sm4sh3r working with Volon Cyber Security Pvt Ltd' was reported to the affected vendor on: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-12686: D-Link

A CVSS score 8.8 (AV:A/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: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13469: Fuji Electric

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: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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-13495: Fuji Electric

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: 2021-03-31, 12 days ago. The vendor is given until 2021-07-29 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 2021-1145-01

Red Hat Security Advisory 2021-1145-01 - 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-4896-2

Ubuntu Security Notice 4896-2 - USN-4896-1 fixed a vulnerability in lxml. This update provides the corresponding update for Ubuntu 14.04 ESM. It was discovered that lxml incorrectly handled certain HTML attributes. A remote attacker could possibly use this issue to perform cross-site scripting attacks. Various other issues were also addressed.

Red Hat Security Advisory 2021-1135-01

Red Hat Security Advisory 2021-1135-01 - Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects. Issues addressed include a HTTP request smuggling vulnerability.

Red Hat Security Advisory 2021-1129-01

Red Hat Security Advisory 2021-1129-01 - Red Hat 3scale API Management delivers centralized API management features through a distributed, cloud-hosted layer. It includes built-in features to help in building a more successful API program, including access control, rate limits, payment gateway integration, and developer experience tools. This advisory is intended to use with container images for Red Hat 3scale API Management 2.10.0.

Kernel Live Patch Security Notice LSN-0075-1

Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly apply speculative execution limits on some pointer types. A local attacker could use this to expose sensitive information (kernel memory). It was discovered that the memory management subsystem in the Linux kernel did not properly handle copy-on-write operations in some situations. A local attacker could possibly use this to gain unintended write access to read-only memory pages. Various other issues were also addressed.

Ubuntu Security Notice USN-4903-1

Ubuntu Security Notice 4903-1 - Viktor Szakats discovered that curl did not strip off user credentials from referrer header fields. A remote attacker could possibly use this issue to obtain sensitive information.

Ubuntu Security Notice USN-4901-1

Ubuntu Security Notice 4901-1 - Adam Nichols discovered that heap overflows existed in the iSCSI subsystem in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data. Various other issues were also addressed.

Red Hat Security Advisory 2021-1131-01

Red Hat Security Advisory 2021-1131-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2021-1125-01

Red Hat Security Advisory 2021-1125-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products.

Red Hat Security Advisory 2021-1093-01

Red Hat Security Advisory 2021-1093-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, out of bounds read, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-1086-01

Red Hat Security Advisory 2021-1086-01 - 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.

Red Hat Security Advisory 2021-1081-01

Red Hat Security Advisory 2021-1081-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include buffer overflow, out of

bounds read, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-4902-1

Ubuntu Security Notice 4902-1 - Dennis Brinkrolf discovered that Django incorrectly handled certain filenames. A remote attacker could possibly use this issue to create or overwrite files in unexpected directories.

Ubuntu Security Notice USN-4561-2

Ubuntu Security Notice 4561-2 - USN-4561-1 fixed vulnerabilities in Rack. This update provides the corresponding update for Ubuntu 16.04 LTS, Ubuntu 20.04 LTS and Ubuntu 20.10. It was discovered that Rack incorrectly handled certain paths. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. Various other issues were also addressed.

Red Hat Security Advisory 2021-1072-01

Red Hat Security Advisory 2021-1072-01 - The libldb packages provide an extensible library that implements an LDAP-like API to access remote LDAP servers, or use local TDB databases. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2021-1073-01

Red Hat Security Advisory 2021-1073-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux.

Red Hat Security Advisory 2021-1074-01

Red Hat Security Advisory 2021-1074-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux.

Red Hat Security Advisory 2021-1071-01

Red Hat Security Advisory 2021-1071-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow and out of bounds read vulnerabilities.

Red Hat Security Advisory 2021-1069-01

Red Hat Security Advisory 2021-1069-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include buffer overflow and out of bounds read vulnerabilities.

Red Hat Security Advisory 2021-1068-01

Red Hat Security Advisory 2021-1068-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux.

Red Hat Security Advisory 2021-1070-01

Red Hat Security Advisory 2021-1070-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include buffer overflow and out of bounds read vulnerabilities.

Red Hat Security Advisory 2021-1064-01

Red Hat Security Advisory 2021-1064-01 - Kernel-based Virtual Machine offers a full virtualization solution for Linux on numerous hardware platforms. The virt:rhel module contains packages which provide user-space components used to run virtual machines using KVM. The packages also provide APIs for managing and interacting with the virtualized systems.

SAP Java OS Remote Code Execution

A malicious authenticated attacker could abuse some particular services exposed by the SAP JAVA Netweaver allowing them to execute commands in the underlying operating system. SAP Netweaver JAVA versions 7.30 through 7.50 are affected.

SAP SMD Agent Unauthenticated Remote Code Execution

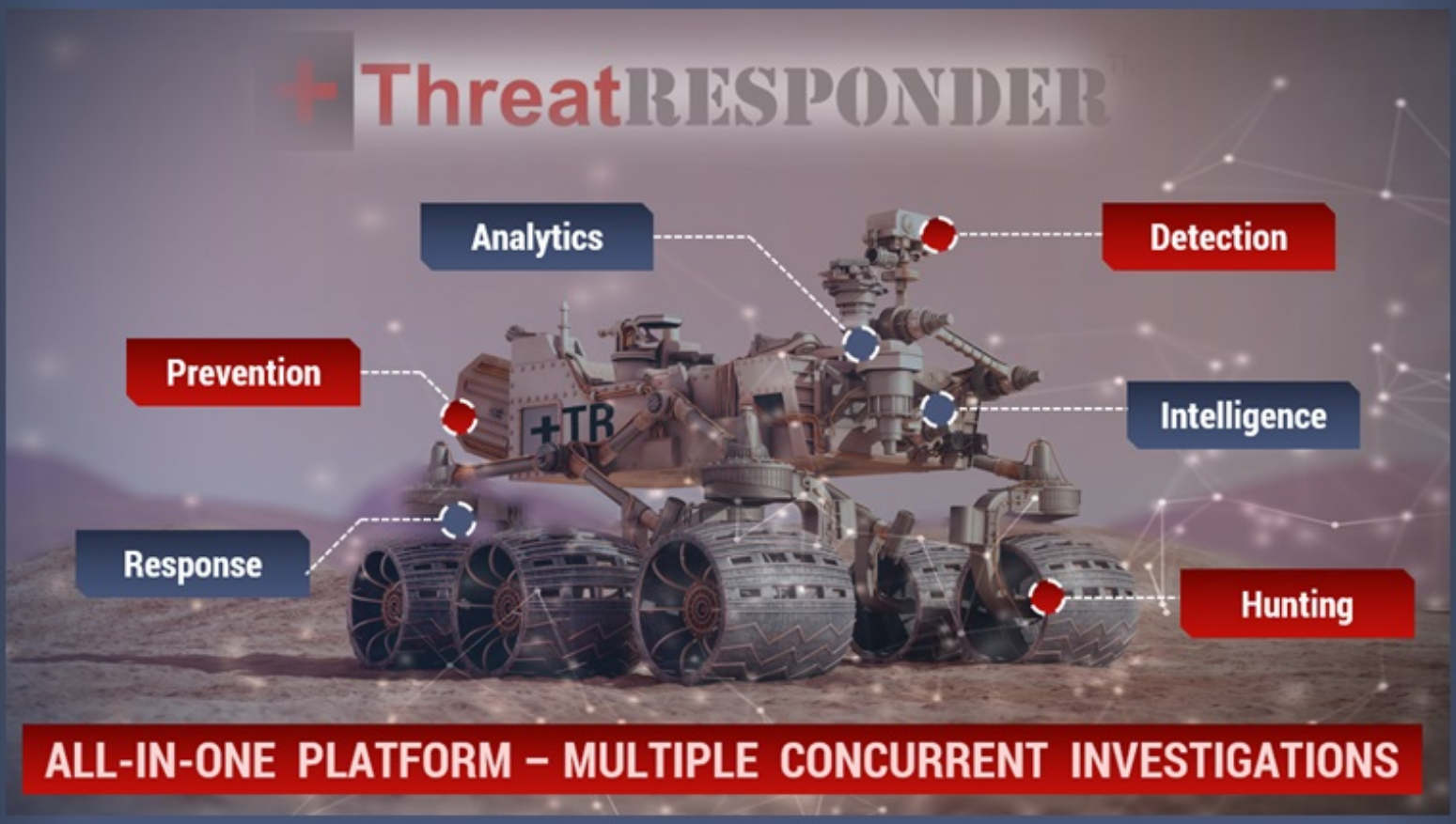
A malicious unauthenticated user could abuse the lack of authentication check on SAP Solution Manager User-Experience Monitoring web service, allowing them to remotely execute commands in all hosts connected to the targeted SolMan through these SMD Agents. Affected versions include SAP Solution Manager SP004 Patch 0011 and lower, SP005 Patch 0012 and lower, SP006 Patch 0013 and lower, SP007 Patch 0019 and lower, SP008 Patch 0015 and lower, SP009 Patch 0007 and lower, SP010 Patch 0001 and lower, and SP011 Patch 0003 and lower.

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 Tutorials for 2021.1:

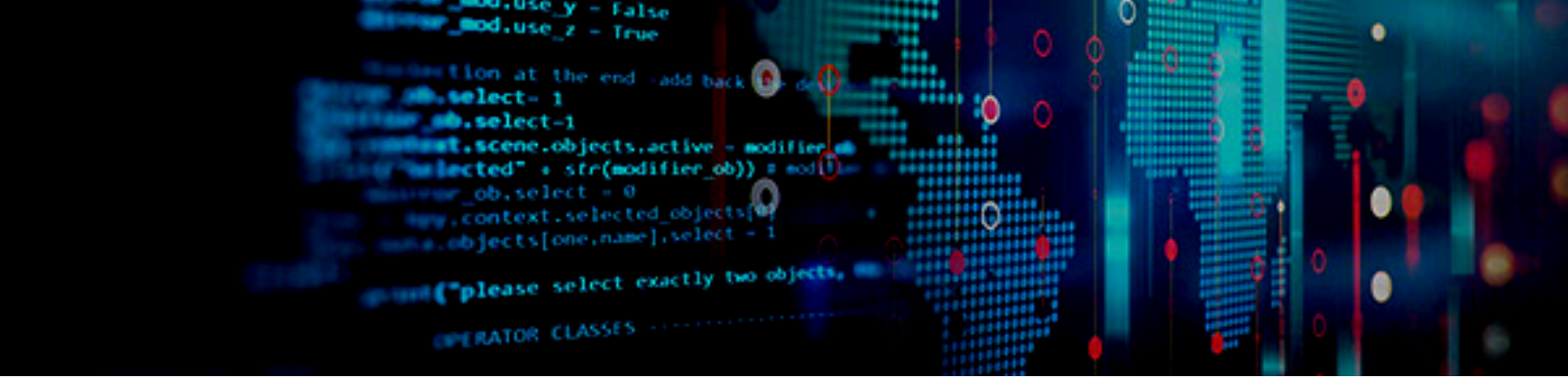
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

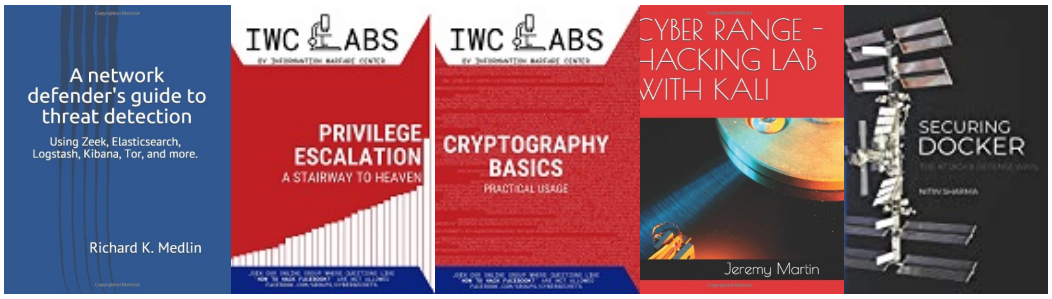


The Cyber Secrets publications on Amazon

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