Mar-29-21

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

March 29, 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

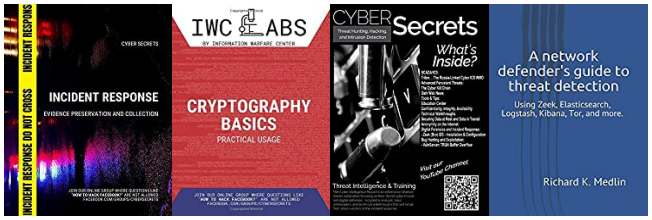
Internet Storm Center Infocon Status

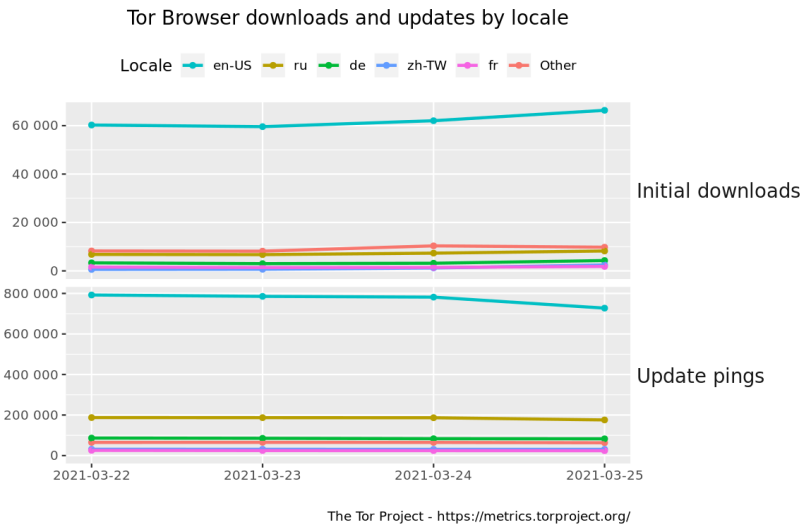
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* Manufacturing's Cloud Migration Opens Door To Major Cyber Risk
* OpenSSL Fixes High-Severity Flaw That Allowed DoS
* Hades Ransomware Operators Are Hunting Big Game In The US
* Buffer Overruns, License Violations, And Bad Code: FreeBSD 13's Close Call
* Active Exploits Hit WordPress Sites Vulnerable To Thrive Themes Flaws
* Microsoft Teams Now Has Its Own Bug Bounty For Researchers
* Facebook Removes Accounts Of China-Based Hackers Targeting Uighurs
* Facial Recognition Beats The Covid Mask Challenge
* Purple Fox Malware Has Propagated To Windows
* Ransomware Now Hitting Hacked Exchange Servers
* Chrome 90 Goes HTTPS By Default While Firefox Injects Substitute Scripts To Foil Tech Tracking
* Tesla Cars Can Now Be Bought In Bitcoin
* Encrypted Phone Firm Encrochat Used Signal Protocol
* Ransomwared Bank Tells Customers It Lost Their SSNs
* Energy Giant Shell Is Latest Victim Of Accellion Attacks
* CISA Warns Of Security Flaws In GE Power Management Devices
* Netop Vision Pro Can Be Hacked To Attack Student PCs
* Russian Pleads Guilty To Tesla Ransomware Plot
* Trump Plans To Build His Own Social Media Platform
* U.S. Supreme Court Rebuffs Facebook Appeal In User Tracking Lawsuit
* Apple Devs Targeted By Malicious Xcode Project
* Zoom Screen Sharing Glitch Briefly Leaks Sensitive Data
* Swiss Hacker Indicted After Claiming Credit For Breaching Nissan, Intel
* Expert Hackers Used 11 Zero Days To Infect Windows, iOS, And Android Users
* State-Sponsored Threat Groups Target Telcos, Steal 5G Secrets

Krebs on Security

* 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?
* WeLeakInfo Leaked Customer Payment Info
* Microsoft Patch Tuesday, March 2021 Edition
* Warning the World of a Ticking Time Bomb
* A Basic Timeline of the Exchange Mass-Hack
* At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

Dark Reading

* SolarWinds Experimenting With New Software Build System in Wake of Breach
* 40% of Apps Leaking Information
* Apple Patches iOS Zero-Day
* Microsoft Shares Exchange Server Post-Compromise Attack Activity
* A Day in the Life of a DevSecOps Manager
* Data Bias in Machine Learning: Implications for Social Justice
* Moving from DevOps to CloudOps: The Four-Box Problem
* Exec Order Could Force Software Vendors to Disclose Breaches to Federal Gov't Customers
* CISA Adds Two Web Shells to Exchange Server Guidance
* In Secure Silicon We Trust
* Nearly Half of Popular Android Apps Built With High-Risk Components
* Security Operations in the World We Live in Now
* The CIO's Shifting Role: Improving Security With Shared Responsibility
* How Personally Identifiable Information Can Put Your Company at Risk
* 6 Tips for Limiting Damage From Third-Party Attacks
* Sierra Wireless Website Still Down After Ransomware Attack
* California State Controller's Office Suffers Data Breach
* Ransomware Incidents Continue to Dominate Threat Landscape
* Facebook Reports China-Linked Cyberattack Targeting Uyghurs
* What a Federal Data Privacy Law Would Mean for Consumers

The Hacker News

* How to Effectively Prevent Email Spoofing Attacks in 2021?
* PHP's Git Server Hacked to Insert Secret Backdoor to Its Source code
* Watch Out! That Android System Update May Contain A Powerful Spyware
* Apple Issues Urgent Patch Update for Another Zero‑Day Under Attack
* OpenSSL Releases Patches for 2 High-Severity Security Vulnerabilities
* New 5G Flaw Exposes Priority Networks to Location Tracking and Other Attacks
* Another Critical RCE Flaw Discovered in SolarWinds Orion Platform
* Black Kingdom Ransomware Hunting Unpatched Microsoft Exchange Servers
* Forcing Self-Service Password Reset (SSPR) Registration to Increase ROI
* Critical Cisco Jabber Bug Could Let Attackers Hack Remote Systems
* Chinese Hackers Used Facebook to Hack Uighur Muslims Living Abroad
* Purple Fox Rootkit Can Now Spread Itself to Other Windows Computers
* Critical Flaws Affecting GE's Universal Relay Pose Threat to Electric Utilities
* WARNING: A New Android Zero-Day Vulnerability Is Under Active Attack
* Popular Netop Remote Learning Software Found Vulnerable to Hacking

Security Week

* Apple Patches Under-Attack iOS Zero-Day
* 'Russian Hackers' Again Target German MPs: Report
* Report: US Gov Executive Order to Mandate Data Breach Disclosure
* EU, US Make New Attempt for Data Privacy Deal
* Kaspersky Sees Rise in Ransomware Attacks on ICS Devices in Developed Countries
* Severe Flaws in Official 'Facebook for WordPress' Plugin
* QNAP Urges Users to Secure Devices Against Brute-Force Attacks
* 5G Security Flaw Allows Data Access, DoS Attacks
* Vulnerabilities Can Allow Attackers to Remotely Gain Control of Weintek HMIs
* Endpoint Security Provider Morphisec Bags $31 Million Investment
* General Says Attacks by Foreign Hackers Are 'Clarion Call'
* Critical Flaw in Jabber for Windows Could Lead to Code Execution
* New Code Execution Flaws In Solarwinds Orion Platform
* The Growing Need for a New Security Platform
* US Cyber Experts Conducted Operations to Safeguard Election
* New Slack Connect DM Feature Raises Security Concerns
* Mamba Ransomware Leverages DiskCryptor for Encryption, FBI Warns
* Feedzai Lands $200M in Series C Funding
* OpenSSL 1.1.1k Patches Two High-Severity Vulnerabilities
* Hackers Start Exploiting Recent Vulnerabilities in Thrive Theme WordPress Plugins

Infosecurity Magazine

* #IMOS21: Infosecurity Magazine Spring Online Summit Now Available On-Demand
* UK's CNI Security Threatened by Staff Burnout
* German MPs Hit by Russian-Backed Phishing Attacks
* Aussie TV Network Taken Off Air by Ransomware
* Phished Healthcare Provider Takes Legal Action Against Amazon
* NGA Picks Four States for Academy on Cybersecurity Policy
* FBI Issues Mamba Alert
* UK Security Chief: CEOs Must Get Closer to Their CISOs
* Burned Out Employees Put Corporate Security at Risk
* Patch Facebook for WordPress to Fix Site Takeover Bugs
* Kroll Acquires Redscan to Expand Cyber-Risk Offering
* Activist Denies Facebook Fraud

KnowBe4 Security Awareness Training Blog RSS Feed

* Average Ransoms Triple while Ransomware Incident Response Costs Pile On
* REvil Ransomware Now Helps with Extortion by Offering to Call the Victim's Contractors and the Media
* Security Awareness is the Key to Cybersecurity Behavior Change
* New Release: 2021 Remote Workforce Security Report
* New UK National Cyber Security Centre Head Warns that Cybersecurity Should be Taken More Seriously
* [UPDATE] What is SOAR? What Are The Pros And Potential Pitfalls?
* Forensically Investigating Phishing To Better Protect Your Organization
* Avoid Being Influenced by Instagram Scams
* KPMG: Cyber Security Risk Is Now No. 1 Threat To Growth
* A Can of Phishbait: from Surveys to Rule Changes to Your Boss's Boss

ISC2.org Blog

* Why would a lawyer ever need an Information Security Professional?
* How To Get It Right With Cybersecurity Training
* Tips for Building a Career in Cybersecurity from Women Who've Been There
* Healthcare Security - Security with Life and Death Consequences
* How Cloud Security Certification Can Give Your Career a Buzz

HackRead

* New Android malware poses as "System Update" to steal your data
* Apex Legend players banned for winning via DDoS attacks
* Firm calls cops on researcher for responsibly disclosing data leak
* Facebook removes 100s of accounts for spreading iOS, Android malware
* Major vulnerability exposes 5G core network slicing to DoS attacks
* Google removes ClearURLs Chrome extension from its store
* SpaceX employee admits security fraud, insider trading on dark web

Koddos

* New Android malware poses as "System Update" to steal your data
* Apex Legend players banned for winning via DDoS attacks
* Firm calls cops on researcher for responsibly disclosing data leak
* Facebook removes 100s of accounts for spreading iOS, Android malware
* Major vulnerability exposes 5G core network slicing to DoS attacks
* Google removes ClearURLs Chrome extension from its store
* SpaceX employee admits security fraud, insider trading on dark web

Naked Security

* Serious Security: OpenSSL fixes two high-severity crypto bugs
* Apple devices get urgent patch for zero-day exploit - update now!
* Alan Turing's Â£50 banknote officially unveiled
* S3 Ep25: Drained accounts, ransomware attacks and Linux badware [Podcast]
* BlackKingdom ransomware still exploiting insecure Exchange servers
* Naked Security Live - "XcodeSpy" takes aim at Mac and iOS developers
* Instagram scams and how to avoid them
* Serious Security: Mac "XcodeSpy" backdoor takes aim at Xcode devs
* S3 Ep24: How not to get snooped, scammed or hoaxed [Podcast]
* Serious Security: The Linux kernel bugs that surfaced after 15 years

Threat Post

* Executive Order Would Strengthen Cybersecurity Requirements for Federal Agencies
* Employee Lockdown Stress May Spark Cybersecurity Risk
* Insurance Giant CNA Hit with Novel Ransomware Attack
* Fleeceware Apps Bank $400M in Revenue
* Microsoft Offers Up To $30K For Teams Bugs
* Facebook Disrupts Spy Effort Aimed at Uyghurs
* Manufacturing's Cloud Migration Opens Door to Major Cyber-Risk
* ProtonVPN CEO Blasts Apple for 'Aiding Tyrants' in Myanmar
* Active Exploits Hit WordPress Sites Vulnerable to Thrive Themes Flaws
* Ransomware Attack Foils IoT Giant Sierra Wireless

Null-Byte

* 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
* This Master Course Bundle on Coding Is Just $34.99
* How to Automate Remote SSH Control of Computers with Expect Scripts

IBM Security Intelligence

* Consent Management: Picking the Right CIAM Strategy
* 5 Cloud Security Must-Haves in 2021
* Women in Cybersecurity: Why Diversity Matters
* Health Care Cybersecurity: Costly Data Breaches, Ensuring PII Security and Beyond
* The Next-Gen Cyber Range: Bringing Incident Response Exercises to the Cloud
* Loving the Algorithm: User Risk Management and Good Security Hygiene
* Reaching Strategic Outcomes With an MDR Service Provider: Part 5
* Retail Cybersecurity: How to Protect Your Customer Data
* Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts
* Top 10 Cybersecurity Vulnerabilities of 2020

InfoWorld

* Artillery: Finding open source success between dev and ops
* How to improve application reliability with observability and monitoring
* 10 top-notch libraries for C++ programming
* Microsoft, Google address browser compatibility issues
* 3 surefire ways to kill your multicloud deployment
* What's new in Rust 1.51
* Ruby-like Crystal 1.0 makes its debut
* Ensuring that citizen developers build AI responsibly
* How to send emails with graphics from R
* Adam Selipsky returns to AWS as CEO. Now what?

C4ISRNET - Media for the Intelligence Age Military

* Pentagon tech office asks industry for 'leap-ahead capabilities'
* Google ex-CEO has a plan for US to stay ahead of China's government-backed tech
* US military conducted 2 dozen cyber operations to head off 2020 election meddling
* Special Operations team in Pacific will confront Chinese information campaigns
* Space Force begins loaning anti-jamming GPS tech to allies
* 'Accelerate change or lose': Applying Gen. Brown's action orders to cyberspace education and training
* Bluestaq wins $280 million contract for space situational awareness library
* Defense official: US must invest more in innovation to compete with China
* Rocket Lab launches Army satellite
* Weather for the war fighter: How the US military can outmaneuver adversaries from space

The Hacker Corner

Conferences

* 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
* We've Moved!

Google Zero Day Project

* In-the-Wild Series: October 2020 0-day discovery
* Déjà vu-lnerability

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.

* ALLES! CTF 2021 HW Edition
* ångstromCTF 2021
* Shakti CTF
* JUST CTF Finals 2021
* b01lers CTF
* BSides Canberra 2021 CTF
* RITSEC CTF 2021
* Midnight Sun CTF 2021 Quals
* _EVENT CHANGED_
* HackPack CTF 2021

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

* Orasi: 1
* Crossroads: 1
* Grotesque: 1
* Gigachad: 1
* DriftingBlues: 3

Tools & Techniques

Packet Storm Security Tools Links

* OpenSSL Toolkit 1.1.1k
* American Fuzzy Lop plus plus 3.12c
* Global Socket 1.4.27
* TOR Virtual Network Tunneling Tool 0.4.5.7
* American Fuzzy Lop plus plus 3.11c
* Hydra Network Logon Cracker 9.2
* Wireshark Analyzer 3.4.4
* scanlogd 2.2.8
* Raptor WAF 0.62
* SQLMAP - Automatic SQL Injection Tool 1.5.3

Kali Linux Tutorials

* Subcert : Finds All The Subdomains From Certificate Transparency Logs
* Mole : A Framework For Identifying & Exploiting Out-Of-Band Application Vulnerabilities
* Invoke SocksProxy : Socks Proxy & Reverse Socks Server Using Powershell
* Reverse Shell Generator : Hosted Reverse Shell Generator With A Ton Of Functionality
* OffensivePipeline : Tool To Download, Compile & Obfuscate C# Tools For Red Team Exercises
* Diceware Password Generator : Generate High Entropy Passwords
* Darkdump : Search The Deep Web Straight From Your Terminal
* Rafel Rat : Android Rat Written In Java
* AnonX : An Encrypted File Transfer Via AES-256-CBC
* Strafer : A Tool To Detect Potential Infections In Elasticsearch Instances

GBHackers Analysis

* Facebook Blocks Chinese Hackers Using Fake Person as Targeting Uyghur Activists
* Google Warns of a New Android Zero-Day Vulnerability Is Under Active Attack
* RCE Flaw in Apache OFBiz Allowed An Attackers to Take Over The ERP System
* MuddyWater Hacker Group Utilize Legitimate File-Sharing Service to Distribute Malware
* Netgear JGS516PE Ethernet Switch Flaws let Attackers Execute Remote Code

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 189: Formatting a Drive as HFS+
* Episode 188: When to Stop Looking for Evidence - Part 4
* SANS Technology Institute Graduate Program: An Insider's View
* Episode 187: When to Stop Looking for Evidence - Part 3

Defcon Conference

* DEF CON 2020 NYE MISS JACKALOPE DJ Music Video
* DEF CON 2020 NYE ZEE DJ Music Video
* DEF CON 2020 NYE Yesterday & Tomorrow DJ Music Video
* DEF CON 2020 NYE Skittish & Bus DJ Music Video

Hak5

* Biggest Ransom Yet?! $50 Million Ransomware Reportedly Hits Acer - ThreatWire
* Thousands of Enterprise Surveillance Cameras Hacked - ThreatWire
* Building DIY Lithium Battery Packs w/Glytch Pt1

The PC Security Channel [TPSC]

* Ryuk Ransomware: Live Demo and Analysis
* Cyberpunk's Company Hacked by HelloKitty Ransomware: Live Demo

Eli the Computer Guy

* TWITTER SURRENDERS to TURKEY
* MOVIE THEATERS are DEAD - BLACK WIDOW on VOD
* TWITTER WIN - NEW EMOJI REACTIONS
* BOX BEING SOLD to PRIVATE EQUITY - RUN AWAY NOW

Security Now

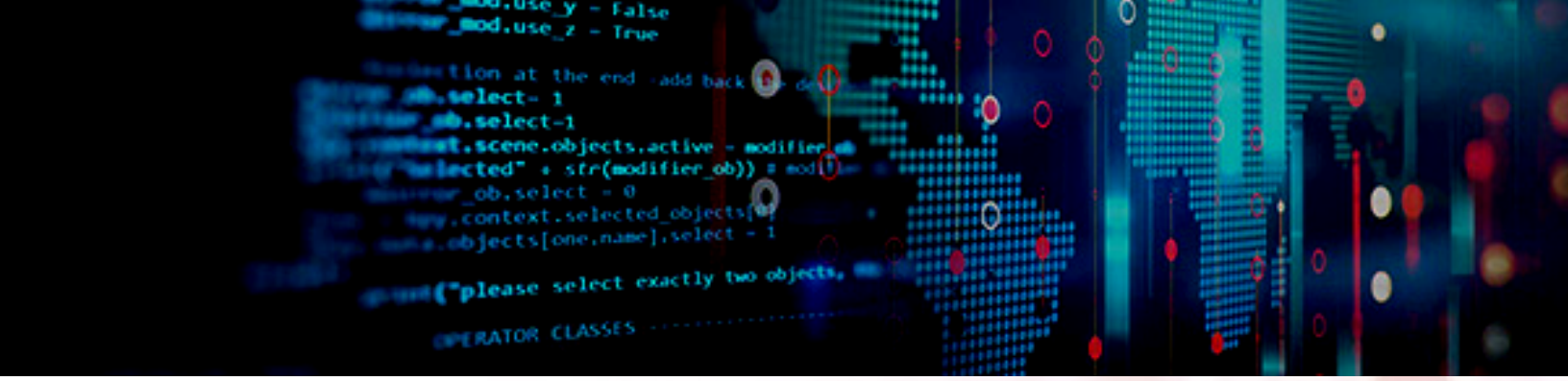
* What the FLoC? - Automatic Fix for Exchange Server Flaw, Firefox 87 Features, MyBB Patch
* ProxyLogon - New Chrome 0-Day, Patch Tuesday Redux, Spectre Comes to Chrome

Troy Hunt

* Weekly Update 236

Intel Techniques: The Privacy, Security, & OSINT Show

* 211-Privacy Security & OSINT Potpourri
* 210-Lessons in Online Purchases & Domain Expiration



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

* 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
* LogoKit: Simple, Effective, and Deceptive

FireEye

* Metasploit Wrap-Up
* DivvyCloud Adds Support for IAM Analyzer Policy Recommendations
* Attack vs. Data: What You Need to Know About Threat Hunting
* Rapid7 Recognized as a Strong Performer in the Inaugural Forrester Waveâ„¢ for MDR, Q1 2021
* MDR Vendor Must-Haves, Part 1: Deep Observation of Real-Time Endpoint Data
* Defending Against the Zero Day: Analyzing Attacker Behavior Post-Exploitation of Microsoft Exchange
* SOC Automation with InsightIDR and InsightConnect: Three Key Use Cases to Explore to Optimize Your Se
* Metasploit Wrap-Up
* Top Security Trends Driving Threat Detection and Response Priorities Today
* F5 Discloses Eight Vulnerabilities-Including Four Critical Ones-in BIG-IP Systems

Proof of Concept (PoC) & Exploits

Packet Storm Security

* SAP Solution Manager 7.2 Remote Command Execution
* Backdoor.Win32.Kwak.12 Authentication Bypass / Code Execution
* TP-Link Cross Site Scripting
* Backdoor.Win32.Kwak.12 Authentication Bypass
* Regis Inventory And Monitoring System 1.0 Cross Site Scripting
* GetSimple CMS Custom JS 0.1 Cross Site Request Forgery / Cross Site Scripting
* Backdoor.Win32.Kwak.12 Authentication Bypass / Man-In-The-Middle
* Backdoor.Win32.Kwak.12 Denial Of Service
* Development Kamel KCFinder 1.7 Shell Upload
* Moodle Atto Editor Cross Site Scripting
* FortiLogger Arbitrary File Upload
* Linksys EA7500 2.0.8.194281 Cross Site Scripting
* Backdoor.Win32.DarkKomet.gozu Insecure Permissions
* Genexis Platinum-4410 P4410-V2-1.31A Cross Site Scripting
* Worm.Win32.Ngrbot.acno Insecure Permissions
* Worm.Win32.Recyl.dp Insecure Permissions
* Ovidentia 6 SQL Injection
* Dolibarr ERP/CRM 11.0.4 Bypass / Code Execution
* Worm.Win32.Ngrbot.abpr Insecure Permissions
* Online Faculty Clearance System 1.0 Shell Upload
* Online Faculty Clearance System 1.0 Cross Site Scripting
* Trojan-Dropper.Win32.Dycler.yhb Insecure Permissions
* Intel RST User Interface / Driver Privilege Escalation
* Codiad 2.8.4 Remote Code Execution
* Worm.Win32.Detnat.c Insecure Permissions

CXSecurity

* FortiLogger Arbitrary File Upload
* SAP Solution Manager 7.2 Remote Command Execution
* Microsoft Exchange ProxyLogon Remote Code Execution
* Codiad 2.8.4 Remote Code Execution (Authenticated)
* VMware View Planner 4.6 Remote Code Execution
* Win32k ConsoleControl Offset Confusion
* Profiling System For Human Resource Management 1.0 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

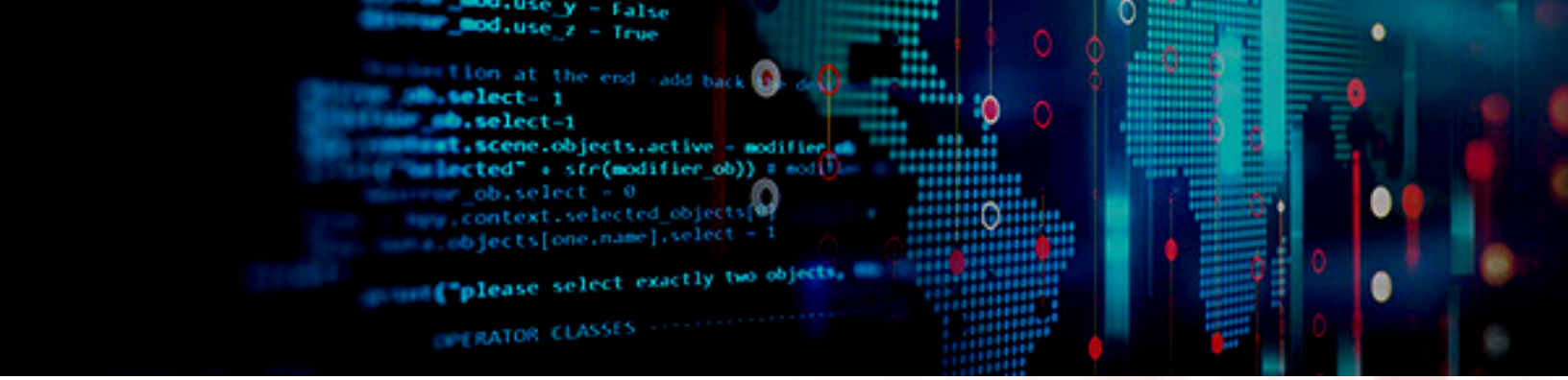
* [webapps] SyncBreeze 10.1.16 - XML Parsing Stack-based Buffer Overflow
* [webapps] Novel Boutique House-plus 3.5.1 - Arbitrary File Download
* [webapps] Budget Management System 1.0 - 'Budget title' Stored XSS
* [webapps] Equipment Inventory System 1.0 - 'multiple' Stored XSS
* [webapps] Concrete5 8.5.4 - 'name' Stored XSS
* [webapps] TP-Link Devices - 'setDefaultHostname' Stored Cross-site Scripting (Unauthenticated)
* [remote] vsftpd 3.0.3 - Remote Denial of Service
* [webapps] WordPress Plugin WP Super Cache 1.7.1 - Remote Code Execution (Authenticated)
* [webapps] Moodle 3.10.3 - 'label' Persistent Cross Site Scripting
* [webapps] Regis Inventory And Monitoring System 1.0 - 'Item List' Stored XSS
* [webapps] GetSimple CMS Custom JS Plugin 0.1 - CSRF to Persistent XSS
* [webapps] Dolibarr ERP/CRM 11.0.4 - File Upload Restrictions Bypass (Authenticated RCE)
* [webapps] Genexis Platinum-4410 P4410-V2-1.31A - 'start_addr' Persistent Cross-Site Scripting
* [webapps] Linksys EA7500 2.0.8.194281 - Cross-Site Scripting
* [webapps] Ovidentia 6 - 'id' SQL injection (Authenticated)
* [local] Ext2Fsd v0.68 - 'Ext2Srv' Unquoted Service Path
* [webapps] Codiad 2.8.4 - Remote Code Execution (Authenticated)
* [local] Elodea Event Collector 4.9.3 - 'ElodeaEventCollectorService' Unquoted Service Path
* [local] ActivIdentity 8.2 - 'ac.sharedstore' Unquoted Service Path
* [local] ELAN Touchpad 15.2.13.1_X64_WHQL - 'ETDService' Unquoted Service Path
* [local] Hi-Rez Studios 5.1.6.3 - 'HiPatchService' Unquoted Service Path
* [webapps] Hotel And Lodge Management System 1.0 - 'Customer Details' Stored XSS
* [webapps] MyBB 1.8.25 - Poll Vote Count SQL Injection
* [local] OSAS Traverse Extension 11 - 'travextensionhostsvc' Unquoted Service Path

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*

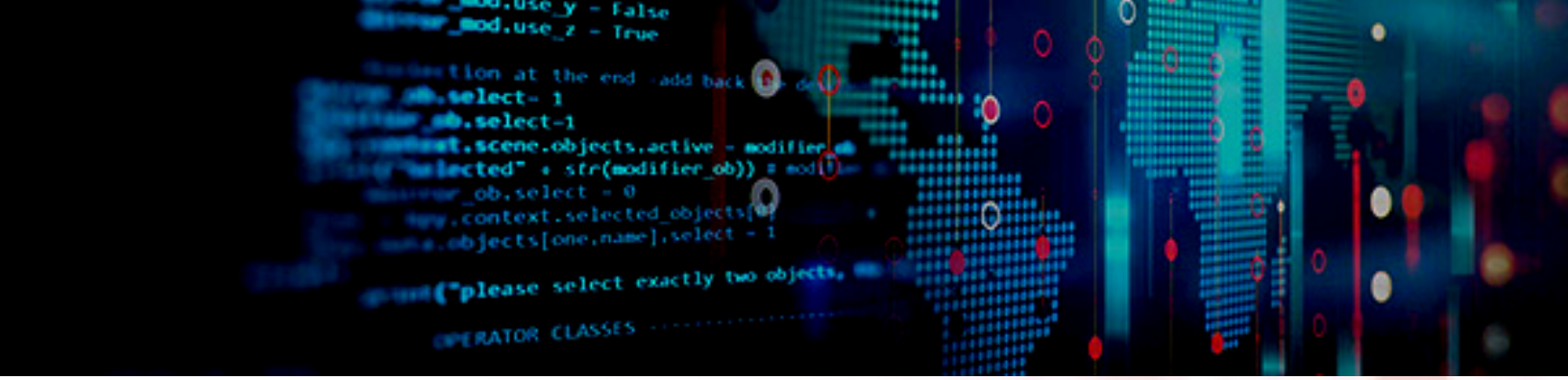
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://dukcapil.baritokualakab.go.id/indo.htm
https://dukcapil.baritokualakab.go.id/indo.htm notified by No_Identity
https://bringin.semarangkab.go.id
https://bringin.semarangkab.go.id notified by limit[ed]
http://shodh.gov.in/rn.html
http://shodh.gov.in/rn.html notified by Ren4Sploit
http://www.thungchanghan.go.th
http://www.thungchanghan.go.th notified by Xyp3r2667
http://www.krabungnok.go.th
http://www.krabungnok.go.th notified by Xyp3r2667
https://ifsca.gov.in/rn.html
https://ifsca.gov.in/rn.html notified by Ren4Sploit
http://www.tasaban-maemoh.go.th/silence.html
http://www.tasaban-maemoh.go.th/silence.html notified by retard
http://www.pa-ngew.go.th/silence.html
http://www.pa-ngew.go.th/silence.html notified by retard
https://rsud.katingankab.go.id/z.htm
https://rsud.katingankab.go.id/z.htm notified by retard
http://angthong.nfe.go.th/iran.html
http://angthong.nfe.go.th/iran.html notified by retard
https://www.maeyom.go.th/content-24-286.html
https://www.maeyom.go.th/content-24-286.html notified by retard
http://yangkhum.go.th/poop.php
http://yangkhum.go.th/poop.php notified by retard
https://www.rangam.go.th
https://www.rangam.go.th notified by retard
https://www.srilakor.go.th
https://www.srilakor.go.th notified by retard
https://www.dnp.go.th/National_park.asp
https://www.dnp.go.th/National_park.asp notified by retard
http://www.mkb-ph.go.th/poop.php
http://www.mkb-ph.go.th/poop.php notified by retard
http://phutthaisonglocal.go.th/pentest.php
http://phutthaisonglocal.go.th/pentest.php notified by /Rayzky_



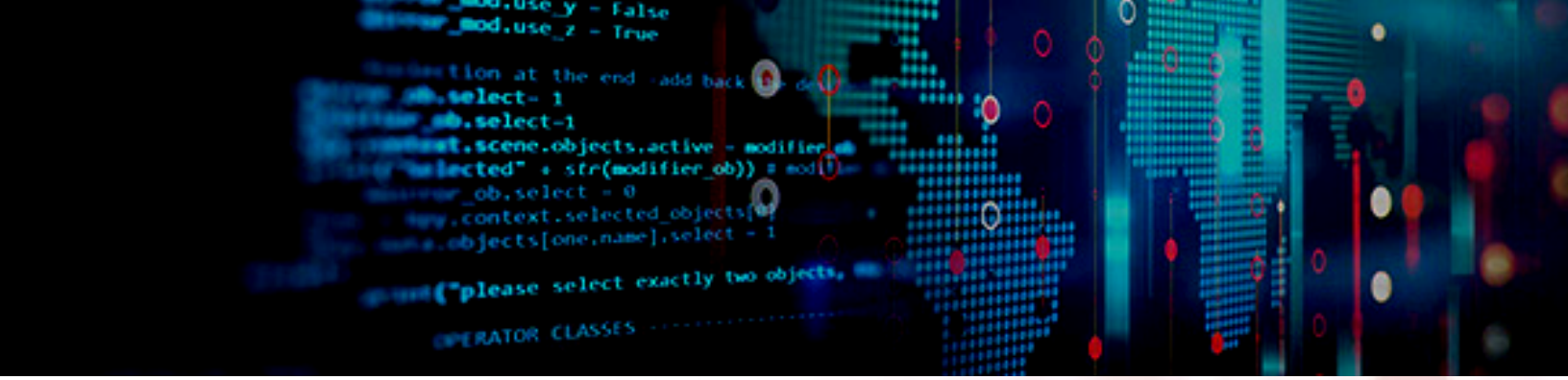
Dark Web News

Darknet Live

[Three Arrested in Germany for Selling on the Darkweb]
German authorities arrested three people for allegedly large quantities of drugs through a darkweb market. (via darknetlive.com)
[Idaho Man Sentenced to Prison for MDMA Trafficking Scheme]
An Idaho man was sentenced to federal prison for distributing MDMA and Ketamine purchased on the darkweb. (via darknetlive.com)
[Netherlands Man Tried to Hire a Hitman on the Darkweb]
A man from The Netherlands admitted paying a hitman on the darkweb to kill his ex-wife. (via darknetlive.com)
[Man Bought MDMA on the Darkweb and Sold It to an Informant]
A Bay Area man, while out on bond after buying MDMA on the darkweb, sold MDMA to a confidential informant. (via darknetlive.com)

Dark Web Link

[Contract Killing On Darknet Caused Life Imprisonment For Finnish Men]
On Friday, A Finnish court had handed a life sentence to two Finnish men for actively taking part in the contract killing. The accused duo had used the dark web platform to plan the murder of one of the men's father. The accused duo had been identified as Aatu Viljami Halonen, aged 20 years and [...] The post Contract Killing On Darknet Caused Life Imprisonment For Finnish Men appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Guns.com Spilled Gun Owner's Data On The Dark Web]
A weaponry website Guns.com had lately been suffering a dreadful data breach where the personal information of the gun owners had been compromised and put up on the dark web. This website is a place where American firearm lovers can go and choose their desired stylish guns. They receive their ordered item(s) straight at their [...] The post Guns.com Spilled Gun Owner's Data On The Dark Web appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Covid Vaccines Ads On The Dark Web Rises By 300%]
In the last three months, there has been a sudden increase of 300% in the dark web advertisements for Covid vaccines, fake negative coronavirus test results and fake vaccination certificates, as the Check Point Research report states. Back in January, the cyber threat intelligence unit of Check Point Research began tracking vaccine sales' underground economy. [...] The post Covid Vaccines Ads On The Dark Web Rises By 300% appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* Apple Releases Security Updates
* OpenSSL Releases Security Update
* Samba Releases Security Updates
* Cisco Releases Security Updates
* Webshells Observed in Post-Compromised Exchange Servers
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* Adobe Releases Security Updates for ColdFusion
* Cisco 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 15, 2021
* Vulnerability Summary for the Week of March 8, 2021

Zero Day Initiative Advisories

ZDI-CAN-13263: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13255: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13141: Advantech
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Selim Enes Karaduman @enesdex' was reported to the affected vendor on: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13260: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13252: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13267: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13137: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Selim Enes Karaduman @enesdex' was reported to the affected vendor on: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13502: Microsoft

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 'Anthony Fuller of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13358: Microsoft

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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13143: Cisco

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'peterjson of RedTeam@VNG Corporation' was reported to the affected vendor on: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13254: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13253: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13257: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13256: 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: 2021-03-26, 3 days ago. The vendor is given until 2021-07-24 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-13173: 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 'Quynh Le of

VNPT ISC' was reported to the affected vendor on: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13065: Oracle

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Jang Laptop of VNPT ISC' was reported to the affected vendor on: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13067: Oracle

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Jang Laptop of VNPT ISC' was reported to the affected vendor on: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13246: Parallels

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Jeonghoon Shin(@singi21a) of THEORI' was reported to the affected vendor on: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13168: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13480: Cisco

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: 2021-03-24, 5 days ago. The vendor is given until 2021-07-22 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-13029: 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: 2021-03-18, 11 days ago. The vendor is given until 2021-07-16 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-12978: 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: 2021-03-18, 11 days ago. The vendor is given until 2021-07-16 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-13028: 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: 2021-03-18, 11 days ago. The vendor is given until 2021-07-16 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-13030: 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: 2021-03-18, 11 days ago. The vendor is given until 2021-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-4888-2

Ubuntu Security Notice 4888-2 - USN-4888-1 fixed several vulnerabilities in ldb. This update provides the corresponding update for Ubuntu 14.04 ESM. Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain LDAP attributes. A remote attacker could possibly use this issue to cause the LDAP server to crash, resulting in a denial of service. Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain DN strings. A remote attacker could use this issue to cause the LDAP server to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-3685-2

Ubuntu Security Notice 3685-2 - USN-3685-1 fixed a vulnerability in Ruby. The fix for CVE-2017-0903 introduced a regression in Ruby. This update fixes the problem.

Ubuntu Security Notice USN-4891-1

Ubuntu Security Notice 4891-1 - It was discovered that OpenSSL incorrectly handled certain renegotiation ClientHello messages. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2021-0992-01

Red Hat Security Advisory 2021-0992-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.9.0 ESR. Issues addressed include a spoofing vulnerability.

Ubuntu Security Notice USN-4890-1

Ubuntu Security Notice 4890-1 - Piotr Krysiuk discovered that the BPF subsystem in the Linux kernel did not properly compute a speculative execution limit on pointer arithmetic in some situations. A local attacker could use this to expose sensitive information. 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. Various other issues were also addressed.

Red Hat Security Advisory 2021-0996-01

Red Hat Security Advisory 2021-0996-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.9.0. Issues addressed include a spoofing vulnerability.

Ubuntu Security Notice USN-4889-1

Ubuntu Security Notice 4889-1 - 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. Adam Nichols discovered that the iSCSI subsystem in the Linux kernel did not properly restrict access to iSCSI transport handles. A local attacker could use this to cause a denial of service or expose sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-4888-1

Ubuntu Security Notice 4888-1 - Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain LDAP attributes. A remote attacker could possibly use this issue to cause the LDAP server to crash, resulting in a denial of service. Douglas Bagnall discovered that ldb, when used with Samba, incorrectly handled certain DN strings. A remote attacker could use this issue to cause the LDAP server to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-0991-01

Red Hat Security Advisory 2021-0991-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.9.0 ESR. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0994-01

Red Hat Security Advisory 2021-0994-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.9.0. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0989-01

Red Hat Security Advisory 2021-0989-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.9.0 ESR. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0993-01

Red Hat Security Advisory 2021-0993-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.9.0. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0995-01

Red Hat Security Advisory 2021-0995-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.9.0. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0990-01

Red Hat Security Advisory 2021-0990-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.9.0 ESR. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2021-0988-01

Red Hat Security Advisory 2021-0988-01 - The RHV-M Virtual Appliance automates the process of installing and configuring the Red Hat Virtualization Manager. The appliance is available to download as an OVA file from the Customer Portal. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0833-01

Red Hat Security Advisory 2021-0833-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 3.11.404. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2021-0986-01

Red Hat Security Advisory 2021-0986-01 - The release of Red Hat AMQ Online 1.7.0 serves as a replacement for earlier AMQ Online releases, and includes bug fixes and enhancements, which are documented in the Release Notes document linked in the References. Issues addressed include information leakage and traversal vulnerabilities.

Ubuntu Security Notice USN-4887-1

Ubuntu Security Notice 4887-1 - De4dCr0w of 360 Alpha Lab discovered that the BPF verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker could use this to expose sensitive information or possibly execute arbitrary code. 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. Various other issues were also addressed.

Red Hat Security Advisory 2021-0976-01

Red Hat Security Advisory 2021-0976-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. The ovirt-node-ng packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include denial of service and memory leak vulnerabilities.

Red Hat Security Advisory 2021-0975-01

Red Hat Security Advisory 2021-0975-01 - The Public Key Infrastructure Core contains fundamental packages required by Red Hat Certificate System. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2021-0974-01

Red Hat Security Advisory 2021-0974-01 - Red Hat Single Sign-On 7.4 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.4.6 serves as a replacement for Red Hat Single Sign-On 7.4.5, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include bypass, cross site scripting, and information leakage vulnerabilities.

Ubuntu Security Notice USN-4886-1

Ubuntu Security Notice 4886-1 - It was discovered that Privoxy incorrectly handled CGI requests. An attacker could possibly use this issue to cause a denial of service or obtain sensitive information. It was discovered that Privoxy incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service or obtain sensitive information. Various other issues were also addressed.

Red Hat Security Advisory 2021-0969-01

Red Hat Security Advisory 2021-0969-01 - Red Hat Single Sign-On is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.4.6 on RHEL 8 serves as a replacement for Red Hat Single Sign-On 7.4.5, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2021-0968-01

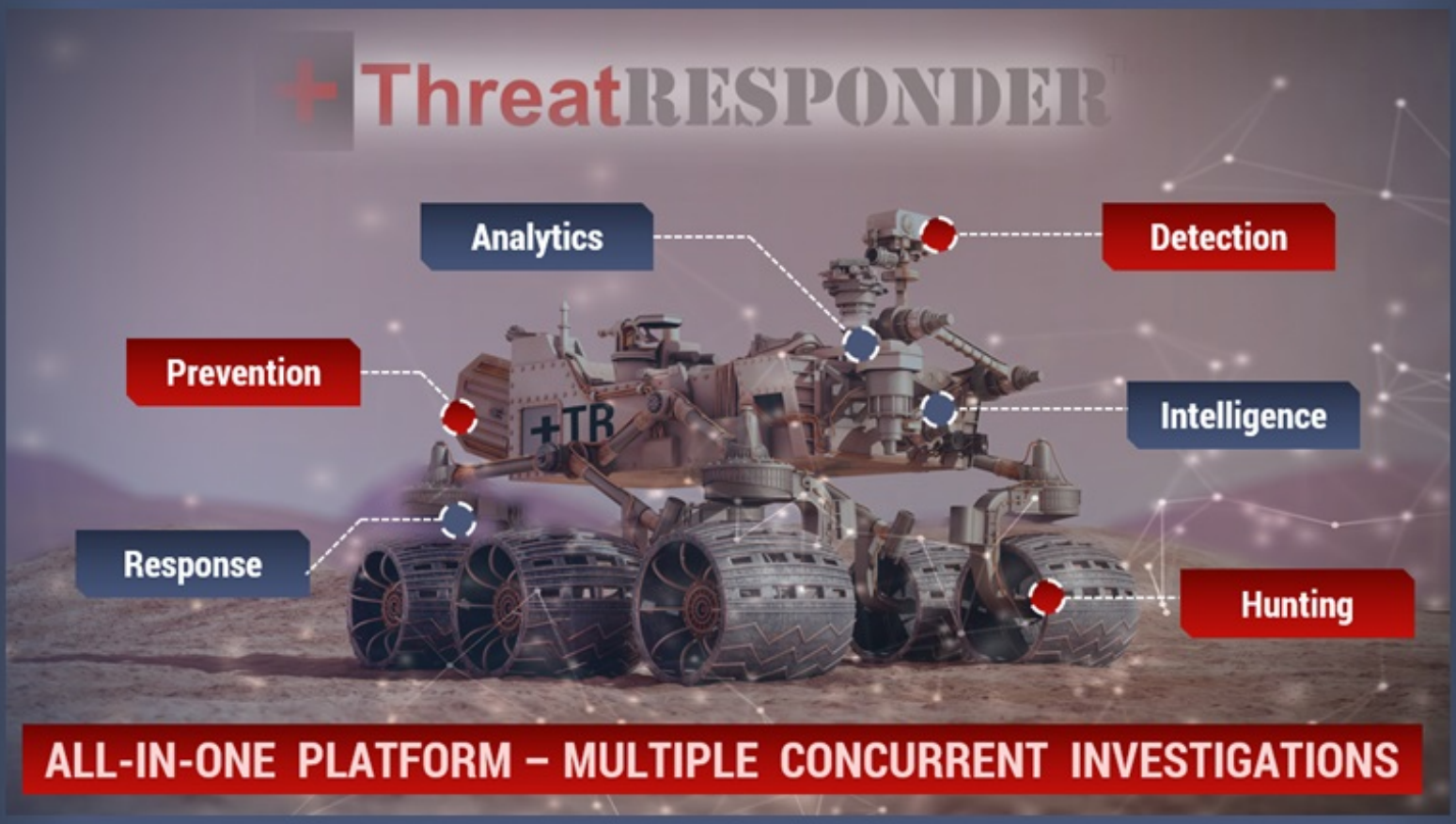
Red Hat Security Advisory 2021-0968-01 - Red Hat Single Sign-On is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.4.6 on RHEL 7 serves as a replacement for Red Hat Single Sign-On 7.4.5, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a cross site scripting 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 Tutorials for 2021.1:

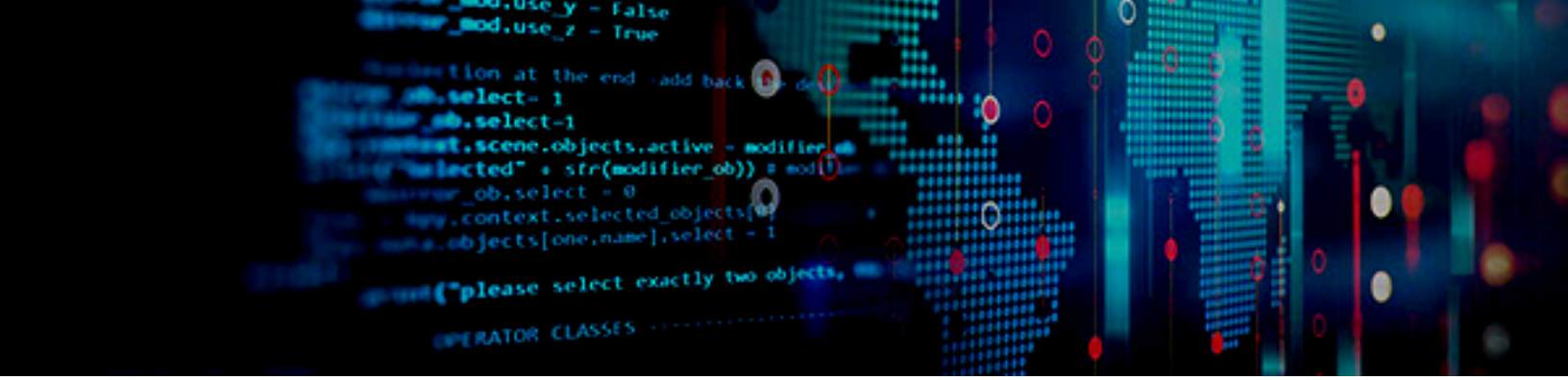
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

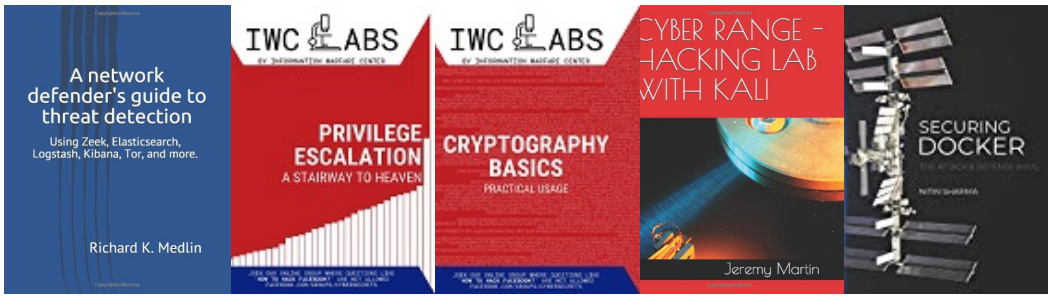


The Cyber Secrets publications on Amazon

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