Apr-05-21

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 5, 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

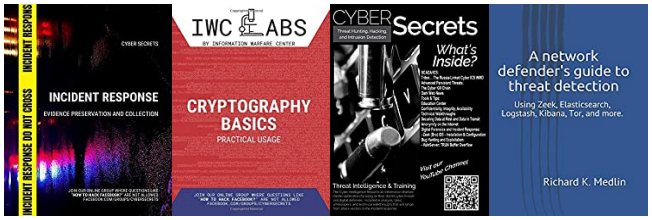
Internet Storm Center Infocon Status

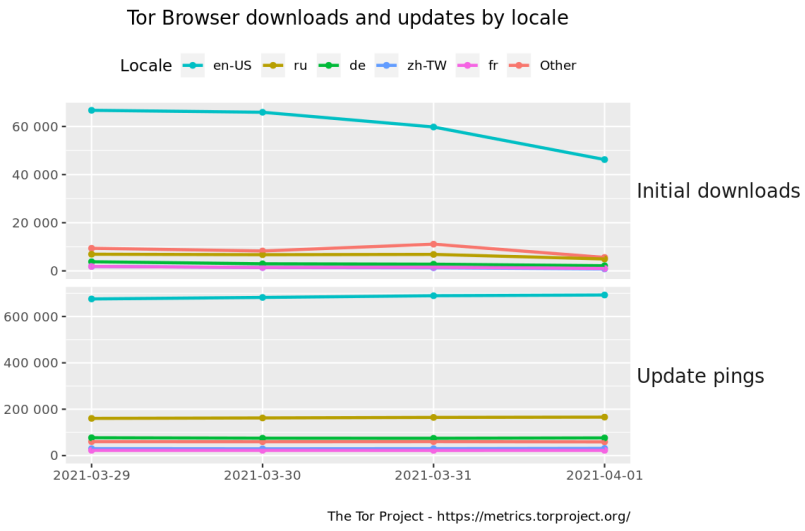
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* Dutch Watchdog Fines Booking.com 475,000 Euros For Keeping Customer Data Theft Quiet
* Legacy QNAP NAS Devices Vulnerable To Zero-Day Attack
* Feds Indict Kansas Man For Allegedly Hacking Into Water Supply
* DeepDotWeb Dark Web Admin Pleads Guilty To Drug, Gun Kickbacks
* Activision Reveals Malware Disguised As Call Of Duty: Warzone Cheats
* Fraud Ring Launders Money Via Fake Charity Donation
* North Korean Hackers Return Targeting Infosec Researchers
* Microsoft To Sell Augmented Reality Goggles To Army
* Hacker Exploits Bug In Doom To Run Snake
* Iranian Credential Thieves Target Medical Researchers
* Ziggy Ransomware Gang Offers Refunds To Victims
* Amazon Tweets Trolling Congress Were So Bad That IT Thought Account Was Hacked
* PayPal Launches Crypto Checkout Service
* Application Security Tactics Are Due For An Overhaul
* Hackers Backdoor PHP After Breaching Internal Git Server
* Intel Accused Of Wiretapping Because It Uses Analytics To Track Keystrokes, Mouse Movements On Its We
* Suspected Russian Hackers Gained Access To US Homeland Security Emails
* Channel Nine Cyber-Attack Disrupts Live Broadcasts In Australia
* US Charges Close To 500 Individuals For COVID-19 Fraud, Criminal Activity
* 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

Krebs on Security

* 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?
* WeLeakInfo Leaked Customer Payment Info
* Microsoft Patch Tuesday, March 2021 Edition

Dark Reading

* Name That Edge Toon: Rough Patch?
* Inside the Ransomware Campaigns Targeting Exchange Servers
* Hackers Demand $40M in Ransom From Florida School District
* FBI & CISA Warn of Active Attacks on FortiOS Vulnerabilities
* US Tech Dominance Rides on Securing Intellectual Property
* Enterprises Remain Riddled With Overprivileged Users -- and Attackers Know It
* 7 Security Strategies as Employees Return to the Office
* Kansas Man Indicted for Hacking, Tampering With Water Utility System
* NIST Publishes Guide for Securing Hotel Property Management Systems
* Solving the Leadership Buy-In Impasse With Data
* How to Build a Resilient IoT Framework
* The Role of Visibility in Securing Cloud Applications
* Top 5 Attack Techniques May Be Easier to Detect Than You Think
* Google Updates on Campaign Targeting Security Researchers
* What's So Great About XDR?
* 83% of Businesses Hit With a Firmware Attack in Past Two Years
* College Students Targeted in Newest IRS Scam
* Advice From Security Experts: How to Approach Security in the New Normal
* 3 Ways Vendors Can Inspire Customer Trust Amid Breaches
* Weakness in EDR Tools Lets Attackers Push Malware Past Them

The Hacker News

* 533 Million Facebook Users' Phone Numbers and Personal Data Leaked Online
* How Cyrebro Can Unify Multiple Cybersecurity Defenses to Optimize Protection
* Google limits which apps can access the list of installed apps on your device
* DeepDotWeb Admin Pleads Guilty to Money Laundering Charges
* 22-Year-Old Charged With Hacking Water System and Endangering Lives
* How to Vaccinate Against the Poor Password Policy Pandemic
* Hackers Using a Windows OS Feature to Evade Firewall and Gain Persistence
* Hackers Set Up a Fake Cybersecurity Firm to Target Security Experts
* Decided to move on from your NGAV/EDR? A Guide for Small Security Teams to What's Next
* Hackers are implanting multiple backdoors at industrial targets in Japan
* MobiKwik Suffers Major Breach - KYC Data of 3.5 Million Users Exposed
* Flaws in Ovarro TBox RTUs Could Open Industrial Systems to Remote Attacks
* New Bugs Could Let Hackers Bypass Spectre Attack Mitigations On Linux Systems
* How to Effectively Prevent Email Spoofing Attacks in 2021?
* PHP's Git Server Hacked to Insert Secret Backdoor to Its Source code

Security Week

* US lawmakers Press Online Ad Auctioneers Over User Data
* SecureDrop Workstation Gets Post-Audit Security Refresh
* Financial Sector Remains Most Targeted by Threat Actors: IBM
* Nine Critical Flaws in FactoryTalk Product Pose Serious Risk to Industrial Firms
* US Looks to Keep Critical Sectors Safe From Cyberattacks
* Large Florida School District Hit by Ransomware Attack
* DHS Gives Federal Agencies 5 Days to Identify Vulnerable MS Exchange Servers
* Unpatched RCE Flaws Affect Tens of Thousands of QNAP SOHO NAS Devices
* Kansas Man Charged with Tampering with Public Water System
* After Hack, Officials Draw Attention to Supply Chain Threats
* Molson Coors Cyberattack, Storms Could Cost Company $140 Million
* Ubiquiti Shares Dive After Reportedly Downplaying 'Catastrophic' Data Breach
* Administrator of Dark Web Portal Pleads Guilty to Money Laundering
* VMware vROps Flaws Can Provide 'Unlimited Opportunities' in Attacks on Companies
* Improve Data Utilization to Modernize the SOC
* Cybersecurity M&A Roundup: 40 Deals Announced in March 2021
* Websites of EU Mobile Providers Fail to Properly Secure User Data: Report
* Citrix Patches DoS Vulnerabilities in Hypervisor
* North Korean .Gov Hackers Back With Fake Pen-Test Company
* Microsoft Wins $22 Billion Deal Making Headsets for US Army

Infosecurity Magazine

* Intelligence Analyst Fed Secrets to Reporter
* Troll Fined $81 After Victim Kills Herself
* Microsoft Suffers Second Outage in Two Weeks
* Trustwave Uncovers Vulnerability in Popular Website CMS
* Cybersecurity Firm ReliaQuest Announces New Senior Appointments
* ACLU Files AI FOIA Request
* Forensic Audit of MobiKwik Ordered
* DeepDotWeb Administrator Admits Darknet Conspiracy
* DHS Secretary Outlines Biden Administration's Cybersecurity Vision
* Booking.com Fined $558,000 for Late Breach Notification
* North Korean Hackers Expand Targeting of Security Community
* Half of Global Retailers See Account Takeovers Surge

KnowBe4 Security Awareness Training Blog RSS Feed

* The Inside Man Season 1 Is Now Available on Amazon Prime Video
* [HEADS UP] Millions of Facebook Users' Personal Information Has Been Leaked Online
* Expect More Travel-Related Phishing as the Pandemic Subsides
* Office 365 Phishing Kits Are Being Used in a New Attack Targeting Execs and Finance
* Encryption, Exfiltration, and Extortion are the Name of the Game as PSYA Ransomware Attacks on Educat
* FBI Warns of "Almost Certain" Deepfake Attacks Over the Next 12-18 Months
* KnowBe4 Fresh Content Updates from March: Including New Optional Learning Feature for Your Users
* Cybercrime Skyrocketed in the US by 55%
* IRS Warns of Phishing for Dot EDU Email Users
* FBI's Newly Release Internet Crime Report Shows Cybercrime has Ramped Up in 2020

ISC2.org Blog

* CISSPs from Around the Globe: An Interview with Mari Aoba
* So Many Awards, So Little Time Left to Nominate. Complete Your Global Achievement Award Nomination To
* (ISC)2 and the Creation of the U.K. Cyber Security Council
* FBI: Cybercrime Shot Up in 2020 Amidst Pandemic
* Survey: Cybersecurity Community Increasingly Concerned About SolarWinds Breach

HackRead

* Facebook data of 500M+ users from 106 countries leaked online
* Hackers Setup Fake Cyber Security firm to Target InfoSec Experts
* DeepDotWeb admin pleads guilty to money laundering, kickbacks
* What are the future prospects of a Cloud architect?
* DoJ charges man for hacking, tempering with public water facility
* Gamers targeted in new malware attack with games cheat codes
* Study: Android sends more data to Google than iOS to Apple

Koddos

* Facebook data of 500M+ users from 106 countries leaked online
* Hackers Setup Fake Cyber Security firm to Target InfoSec Experts
* DeepDotWeb admin pleads guilty to money laundering, kickbacks
* What are the future prospects of a Cloud architect?
* DoJ charges man for hacking, tempering with public water facility
* Gamers targeted in new malware attack with games cheat codes
* Study: Android sends more data to Google than iOS to Apple

Naked Security

* 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
* 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

Threat Post

* FBI: APTs Actively Exploiting Fortinet VPN Security Holes
* Call of Duty Cheats Expose Gamers to Malware, Takeover
* From PowerShell to Payload: An Analysis of Weaponized Malware
* Robinhood Warns Customers of Tax-Season Phishing Scams
* 80% of Global Enterprises Report Firmware Cyberattacks
* Legacy QNAP NAS Devices Vulnerable to Zero-Day Attack
* Ragnarok Ransomware Hits Boggi Milano Menswear
* Building a Fortress: 3 Key Strategies for Optimized IT Security
* Google: North Korean APT Gearing Up to Target Security Researchers Again
* Apple, Google Both Track Mobile Telemetry Data, Despite Users Opting Out

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

* 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
* Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing and Energy
* Risk Management, C-Suite Shifts & Next-Gen Text Scams: Your March 2021 Security Intelligence Roundup
* Are Cloud-Native IAM Controls Good Enough for Your Enterprise?
* 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

InfoWorld

* Data lineage: What it is and why it's important
* 7 ways the cloud is changing
* Eclipse hosts Visual Studio Code extensions marketplace
* Are industry clouds an opportunity or a distraction?
* ECMAScript 2021 spec for JavaScript nears the finish line
* 4 key tests for your AI explainability toolkit
* What is functional programming? A practical guide
* Deno Company forms to back Node.js rival
* Microsoft inches closer to unified Windows SDK
* 8 ways to jump-start your machine learning

C4ISRNET - Media for the Intelligence Age Military

* America and its military need a blockchain strategy
* Pentagon seeks commercial solutions to get its data ready for AI
* Could Latvia become NATO's 5G military test hub?
* Report of Russian navigation gear on German submarines has lawmakers on alert
* Anduril buys tube-launched drone developer Area-I
* Biden's infrastructure plan includes billions to develop emerging tech the military needs
* Army moves ahead on 'mixed reality' goggle with Microsoft in $21.8 billion contract
* Army developing tool for US cities to practice cyberattack response
* JAIC director: Pentagon's biggest competitive threat? Obsolescence
* The US Army wants new software to make its logistics platform ready for multidomain operations

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

* 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.

* BSides Canberra 2021 CTF
* RITSEC CTF 2021
* Midnight Sun CTF 2021 Quals
* _EVENT CHANGED_
* HackPack CTF 2021
* Incognito 2.0
* PlaidCTF 2021
* UMDCTF 2021
* Bambi CTF #5
* Cyber Apocalypse 2021

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

* Grotesque: 2
* DriftingBlues: 6
* hacksudo: 3
* Wireless: 1
* ColddWorld: Immersion

Tools & Techniques

Packet Storm Security Tools Links

* 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
* TOR Virtual Network Tunneling Tool 0.4.5.7
* American Fuzzy Lop plus plus 3.11c
* Hydra Network Logon Cracker 9.2

Kali Linux Tutorials

* CTF-Party : A Ruby Library To Enhance & Speed Up Script/Exploit
* Godehashed : Tool That Uses The Dehashed.Com API To Search For Compromised Assets
* ProxyLogon : PoC Exploit for Microsoft Exchange
* Netmap.Js : Fast Browser-Based Network Discovery Module
* 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

GBHackers Analysis

* 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
* RCE Flaw in Apache OFBiz Allowed An Attackers to Take Over The ERP System

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 191: SANS DFIR Summit 2021 Call For Papers
* Episode 190: Forensic 4Cast Awards
* Episode 189: Formatting a Drive as HFS+
* Episode 188: When to Stop Looking for Evidence - Part 4

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

* The secret to making amazing change - Hak5 2901
* The IOT Security Nightmare: How bad could it be? w/Retia
* Biggest Ransom Yet?! $50 Million Ransomware Reportedly Hits Acer - ThreatWire

The PC Security Channel [TPSC]

* Best Firewall for Windows
* Ryuk Ransomware: Live Demo and Analysis

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

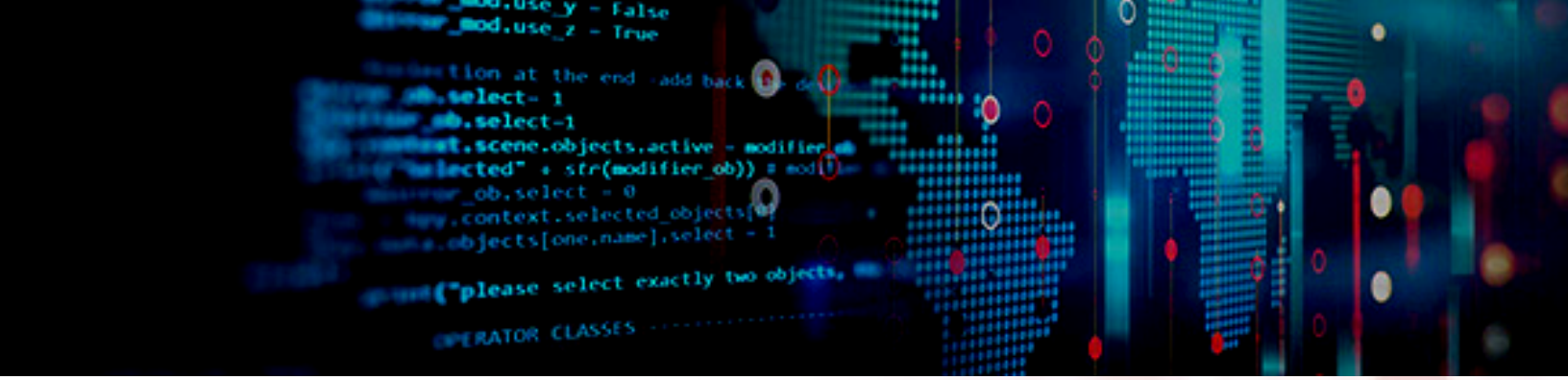
* GIT Me Some PHP - Spectre Returns to Linux, API Security, OpenSSL Flaws, SolarWinds
* What the FLoC? - Automatic Fix for Exchange Server Flaw, Firefox 87 Features, MyBB Patch

Troy Hunt

* Weekly Update 237

Intel Techniques: The Privacy, Security, & OSINT Show

* 212-Vital Privacy, Security, & OSINT Updates
* 211-Privacy Security & OSINT Potpourri



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
* MDR Vendor Must-Haves, Part 3: Ingestion of Other Technology Investments
* SolarWinds Patches Four New Vulnerabilities in Their Orion Platform
* MDR Vendor Must-Haves, Part 2: Ingestion of Network Device Data
* 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

Proof of Concept (PoC) & Exploits

Packet Storm Security

* F5 BIG-IP 16.0.x Remote Code Execution
* ZBL EPON ONU Broadband Router 1.0 Remote Privilege Escalation
* Trojan-Downloader.Win32.Delf.nzg Insecure Permissions
* Trojan-Downloader.Win32.Delf.ur Insecure Permissions
* Trojan-Downloader.Win32.Delf.oxz Insecure Permissions
* Packet Storm New Exploits For March, 2021
* F5 iControl Server-Side Request Forgery / Remote Command Execution
* SaltStack Salt API Unauthenticated Remote Command Execution
* ScadaBR 1.0 Shell Upload
* School Registration And Fee System 1.0 Cross Site Scripting
* School Registration And Fee System 1.0 SQL Injection
* phpPgAdmin 7.13.0 Command Execution
* Company Crime Tracking Software 1.0 Cross Site Scripting
* Latrix 0.6.0 SQL Injection
* Backdoor.Win32.Burbul.b Authentication Bypass / Man-In-The-Middle
* IRC-Worm.Win32.Silentium.a Insecure Permissions
* DD-WRT 45723 Buffer Overflow
* CourseMS 2.1 Cross Site Scripting
* Zabbix 3.4.7 Cross Site Scripting
* Openlitespeed 1.7.9 Cross Site Scripting
* IRC-Worm.Win32.Jane.a Authentication Bypass / Man-In-The-Middle
* GetSimple CMS 3.3.16 Cross Site Scripting / Shell Upload
* IRC-Worm.Win32.Jane.a Authentication Bypass / Code Execution
* Health Center Patient Record Management System 1.0 Cross Site Scripting
* Health Center Patient Record Management System 1.0 SQL Injection

CXSecurity

* 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
* FortiLogger Arbitrary File Upload
* SAP Solution Manager 7.2 Remote Command Execution
* Microsoft Exchange ProxyLogon Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

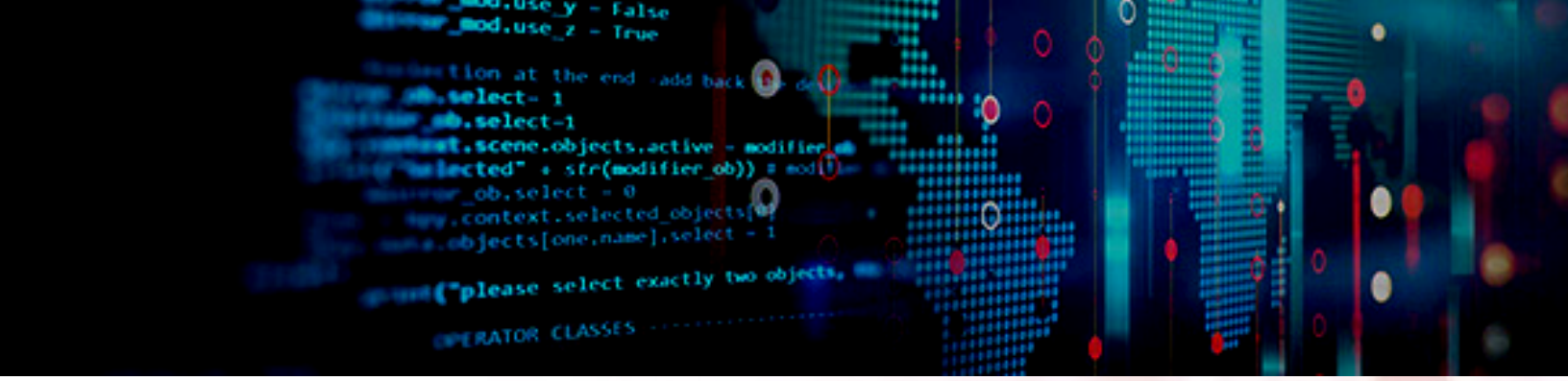
* [webapps] Mini Mouse 9.2.0 - Path Traversal
* [webapps] Mini Mouse 9.2.0 - Remote Code Execution
* [webapps] OpenEMR 4.1.0 - 'u' SQL Injection
* [webapps] Basic Shopping Cart 1.0 - Authentication Bypass
* [webapps] Simple Food Website 1.0 - Authentication Bypass
* [local] Rockstar Service - Insecure 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
* [webapps] CourseMS 2.1 - 'name' Stored XSS
* [dos] DD-WRT 45723 - UPNP Buffer Overflow (PoC)
* [webapps] Zabbix 3.4.7 - Stored XSS
* [webapps] Openlitespeed 1.7.9 - 'Notes' Stored Cross-Site Scripting
* [webapps] GetSimple CMS 3.3.16 - Reflected XSS to RCE
* [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

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

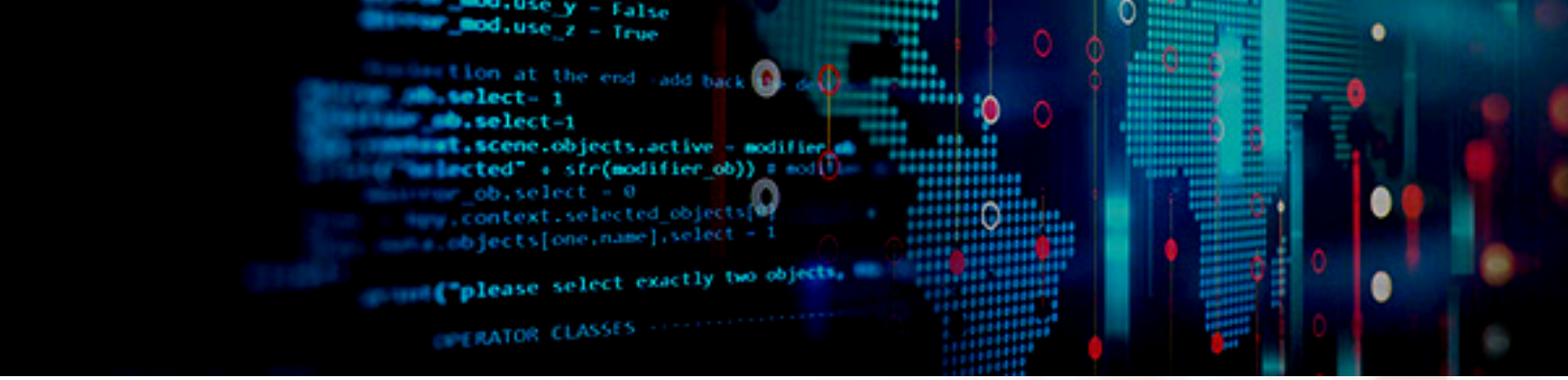
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.sanmartin.gov.ar/index_.php
http://www.sanmartin.gov.ar/index_.php notified by eRRoR 7rB
https://ppid.kaltimprov.go.id
https://ppid.kaltimprov.go.id notified by SKULL CYBER ARMY
http://pthp.gov.la/index.txt
http://pthp.gov.la/index.txt notified by aDriv4
http://ptodx.gov.la/index.txt
http://ptodx.gov.la/index.txt notified by aDriv4
https://bloodsafety.gov.bt/vz.txt
https://bloodsafety.gov.bt/vz.txt notified by aDriv4
http://www.cmdomcavati.mg.gov.br
http://www.cmdomcavati.mg.gov.br notified by Paraná Cyber Mafia
http://camara.pr.gov/rn.html
http://camara.pr.gov/rn.html notified by Ren4Sploit
http://baneh.gov.ir/idolsec.htm
http://baneh.gov.ir/idolsec.htm notified by IDOLSEC Team
https://www.vicosa.ce.gov.br/war.html
https://www.vicosa.ce.gov.br/war.html notified by MR.QLQ
http://isponre.gov.vn/1.php
http://isponre.gov.vn/1.php notified by -1
http://www.servidor.unir.br
http://www.servidor.unir.br notified by Paraná Cyber Mafia
http://www.dmejp.unir.br
http://www.dmejp.unir.br notified by Paraná Cyber Mafia
http://www.dti.unir.br
http://www.dti.unir.br notified by Paraná Cyber Mafia
http://www.procea.unir.br
http://www.procea.unir.br notified by Paraná Cyber Mafia
http://www.ncet.unir.br
http://www.ncet.unir.br notified by Paraná Cyber Mafia
http://www.ppghisec.unir.br
http://www.ppghisec.unir.br notified by Paraná Cyber Mafia
http://www.pgca.unir.br
http://www.pgca.unir.br notified by Paraná Cyber Mafia



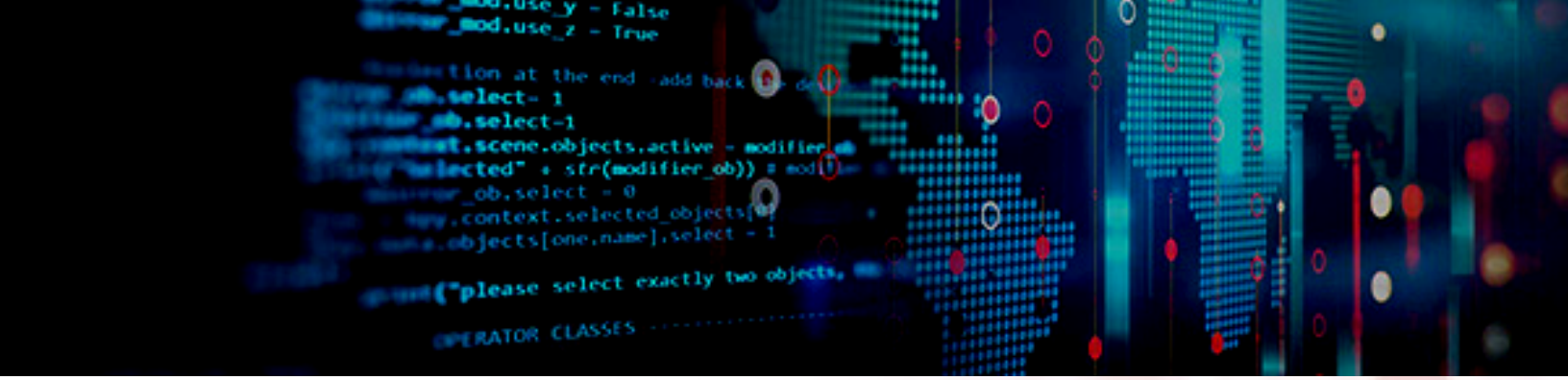
Dark Web News

Darknet Live

DeepDotWeb Admin Admits Laundering $8.4 Million in Bitcoin
Tal Prihar, the administrator of the defunct darkweb news site DeepDotWeb, admitted laundering $8.4 million in cryptocurrency. (via darknetlive.com)
French Drug Dealers Avoid Prison in Drug Importation Case
Three drug dealers in France received suspended sentences for their roles in a conspiracy to resell drugs purchased on the darkweb. (via darknetlive.com)
Italian Man Arrested for Buying Drugs on the Darkweb
Authorities in Turin arrested a man for importing and reselling drugs purchased on the darkweb. (via darknetlive.com)
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)

Dark Web Link

SmokersCo Vendor Shop: Top-Tier Smokeables Market On The Dark Web
Are you quite anxious to get into a dark web vendor shop that is solely dedicated to smokeables? Well, think of it, and SmokersCo vendor shop comes to mind. The darknet vendor shop is not a very old one established on the Tor network, and neither has it been created too recently. Standing somewhere around [...] The post SmokersCo Vendor Shop: Top-Tier Smokeables Market On The Dark Web appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
How To Set Up And Install Exodus In Linux Operating System?
Cleaning your coins or exchanging is a significant concern for most people involved in illicit activities, as most exchanges require KYC or Know Your Customer. Therefore, the dark web drug vendors and cybercriminals have to rely on expensive mixers and exchanges with patience because getting funds could take anywhere from a few hours to a [...] The post How To Set Up And Install Exodus In Linux Operating System? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
DeepDotWeb Admin Confesses To Have Laundered Whopping $8.4M Worth Bitcoin
DeepDotWeb admin Tal Prihar, who had aided in facilitating hundreds of millions of dollars in the dark web's illegal sales, has pleaded guilty to his part in a conspiracy. The federal court in Pittsburgh, U.S. Attorney's Office, has heard his confession. Tal Prihar, aged 39 years, belonging from Israel and based in Brazil, had confessed [...] The post DeepDotWeb Admin Confesses To Have Laundered Whopping $8.4M Worth Bitcoin appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Advisories

US-Cert Alerts & bulletins

* 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
* Citrix Releases Security Updates for Hypervisor
* Apple Releases Security Updates
* OpenSSL Releases Security Update
* AA21-077A: Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
* AA21-076A: TrickBot Malware
* Vulnerability Summary for the Week of March 22, 2021
* Vulnerability Summary for the Week of March 15, 2021

Zero Day Initiative Advisories

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, 3 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, 3 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, 3 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, 3 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, 3 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, 3 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, 3 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, 3 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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-13470: 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, 5 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

Ubuntu Security Notice USN-4899-1

Ubuntu Security Notice 4899-1 - Damian Lukowski discovered that SpamAssassin incorrectly handled certain CF files. If a user or automated system were tricked into using a specially- crafted CF file, a remote attacker could possibly run arbitrary code.

Red Hat Security Advisory 2021-1050-01

Red Hat Security Advisory 2021-1050-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include denial of service and memory leak vulnerabilities.

Red Hat Security Advisory 2021-1051-01

Red Hat Security Advisory 2021-1051-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include denial of service and memory leak vulnerabilities.

Gentoo Linux Security Advisory 202103-04

Gentoo Linux Security Advisory 202103-4 - A vulnerability in SQLite could lead to remote code execution. Versions less than 3.34.1 are affected.

Gentoo Linux Security Advisory 202103-03

Gentoo Linux Security Advisory 202103-3 - Multiple vulnerabilities have been found in OpenSSL, the worst of which could allow remote attackers to cause a Denial of Service condition. Versions less than 1.1.1k are affected.

Gentoo Linux Security Advisory 202103-02

Gentoo Linux Security Advisory 202103-2 - A vulnerability in Redis could lead to remote code execution. Versions less than 6.0.12 are affected.

Gentoo Linux Security Advisory 202103-01

Gentoo Linux Security Advisory 202103-1 - Multiple vulnerabilities have been found in Salt, the worst of which could allow remote attacker to execute arbitrary commands. Versions less than 3000.8 are affected.

Ubuntu Security Notice USN-4898-1

Ubuntu Security Notice 4898-1 - 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. Mingtao Yang discovered that curl incorrectly handled session tickets when using an HTTPS proxy. A remote attacker in control of an HTTPS proxy could use this issue to bypass certificate checks and intercept communications. This issue only affected Ubuntu 20.04 LTS and Ubuntu 20.10. Various other issues were also addressed.

Red Hat Security Advisory 2021-0943-01

Red Hat Security Advisory 2021-0943-01 - This release of Red Hat build of Eclipse Vert.x 4.0.3 includes security updates, bug fixes, and enhancements. For more information, see the release notes listed in the References section. Issues addressed include an information leakage vulnerability.

Ubuntu Security Notice USN-4897-1

Ubuntu Security Notice 4897-1 - Ben Caller discovered that Pygments incorrectly handled parsing certain files. If a user or automated system were tricked into parsing a specially crafted file, a remote attacker could cause Pygments to hang or consume resources, resulting in a denial of service.

Ubuntu Security Notice USN-4896-1

Ubuntu Security Notice 4896-1 - It was discovered that lxml incorrectly handled certain HTML attributes. A remote attacker could possibly use this issue to perform cross-site scripting attacks.

Red Hat Security Advisory 2021-0956-01

Red Hat Security Advisory 2021-0956-01 - ed 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 4.6.23. Issues addressed include a

denial of service vulnerability.

Red Hat Security Advisory 2021-1044-01

Red Hat Security Advisory 2021-1044-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management, and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This release of Red Hat Process Automation Manager 7.10.1 serves as an update to Red Hat Process Automation Manager 7.10.0, and includes bug fixes, which are documented in the Release Notes document linked to in the References.

Red Hat Security Advisory 2021-1039-01

Red Hat Security Advisory 2021-1039-01 - MariaDB is a community developed branch of MySQL. MariaDB is a multi-user, multi-threaded SQL database server. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2021-1031-01

Red Hat Security Advisory 2021-1031-01 - 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 a use-after-free vulnerability.

Red Hat Security Advisory 2021-1027-01

Red Hat Security Advisory 2021-1027-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-1026-01

Red Hat Security Advisory 2021-1026-01 - The nss-softokn package provides the Network Security Services Softoken Cryptographic Module. Issues addressed include out of bounds read and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-1030-01

Red Hat Security Advisory 2021-1030-01 - Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages technologies. Issues addressed include a HTTP request smuggling vulnerability.

Ubuntu Security Notice USN-4895-1

Ubuntu Security Notice 4895-1 - Alex Rousskov and Amit Klein discovered that Squid incorrectly handled certain Content-Length headers. A remote attacker could possibly use this issue to perform an HTTP request smuggling attack, resulting in cache poisoning. This issue only affected Ubuntu 20.04 LTS. Jianjun Chen discovered that Squid incorrectly validated certain input. A remote attacker could use this issue to perform HTTP Request Smuggling and possibly access services forbidden by the security controls. Various other issues were also addressed.

Ubuntu Security Notice USN-4894-1

Ubuntu Security Notice 4894-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Red Hat Security Advisory 2021-1032-01

Red Hat Security Advisory 2021-1032-01 - Perl is a high-level programming language that is commonly used for system administration utilities and web programming. Issues addressed include buffer overflow, denial of service, and integer overflow vulnerabilities.

Red Hat Security Advisory 2021-1028-01

Red Hat Security Advisory 2021-1028-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-0957-01

Red Hat Security Advisory 2021-0957-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. 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 container images for Red Hat OpenShift Container Platform 4.7.4.

Red Hat Security Advisory 2021-0958-01

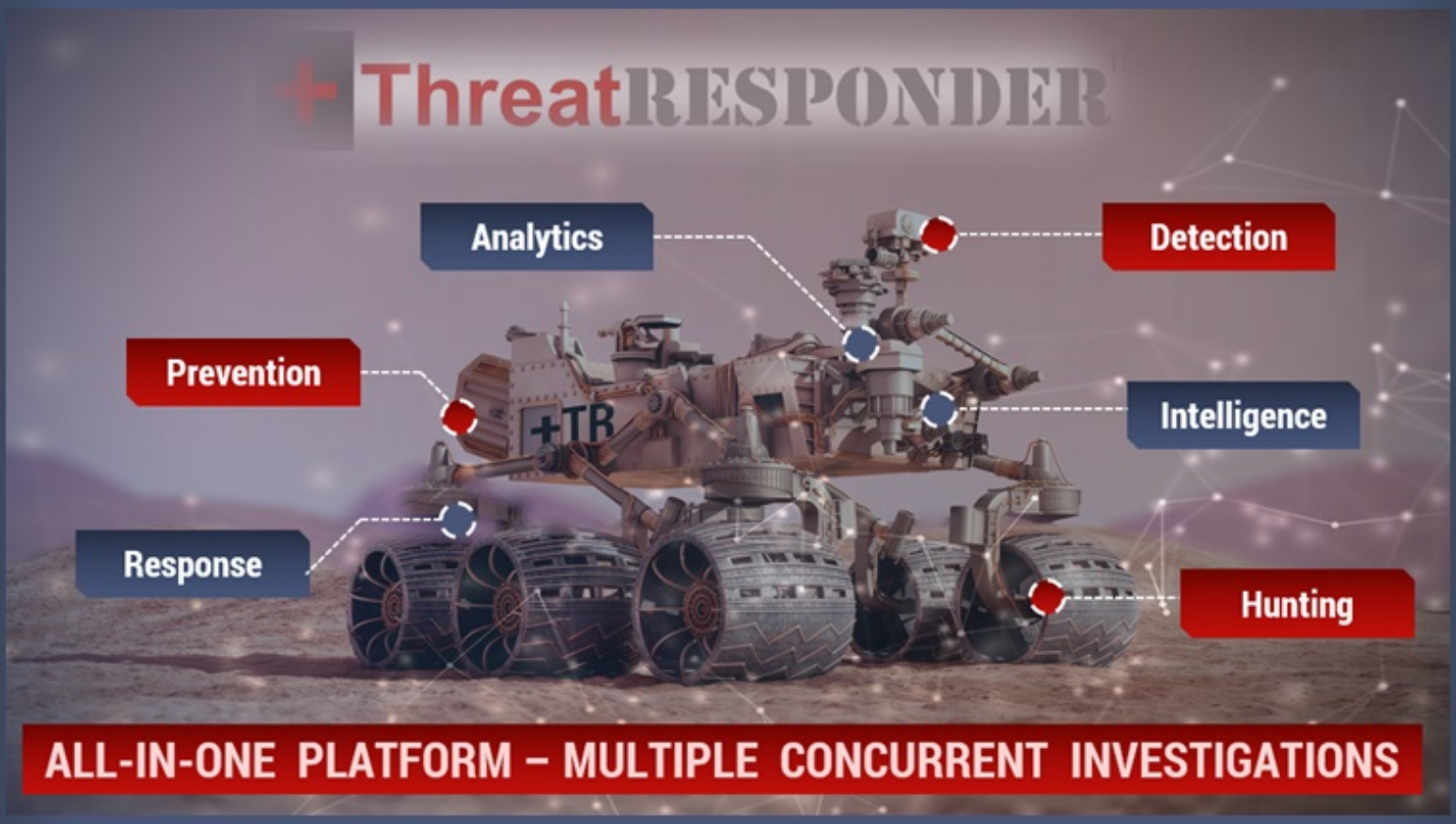
Red Hat Security Advisory 2021-0958-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.4.

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:

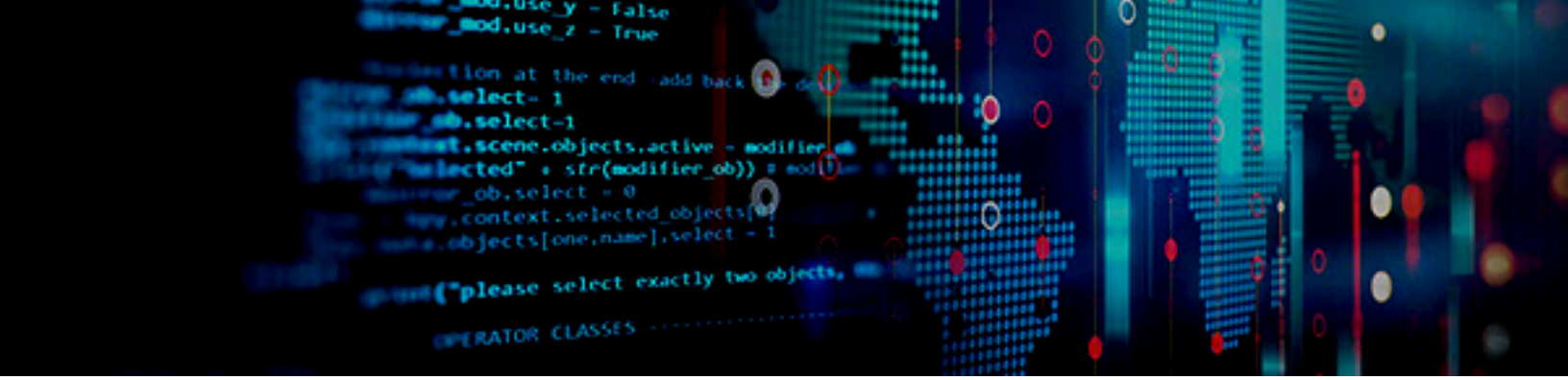
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

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

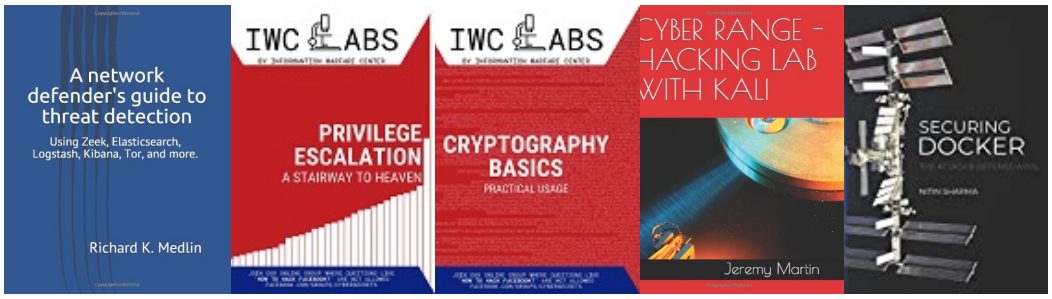


The Cyber Secrets publications on Amazon

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