Feb-22-21

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

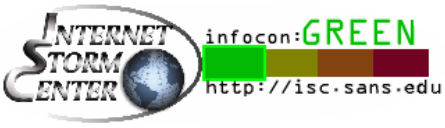
LINUX

netSecurity

February 22, 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



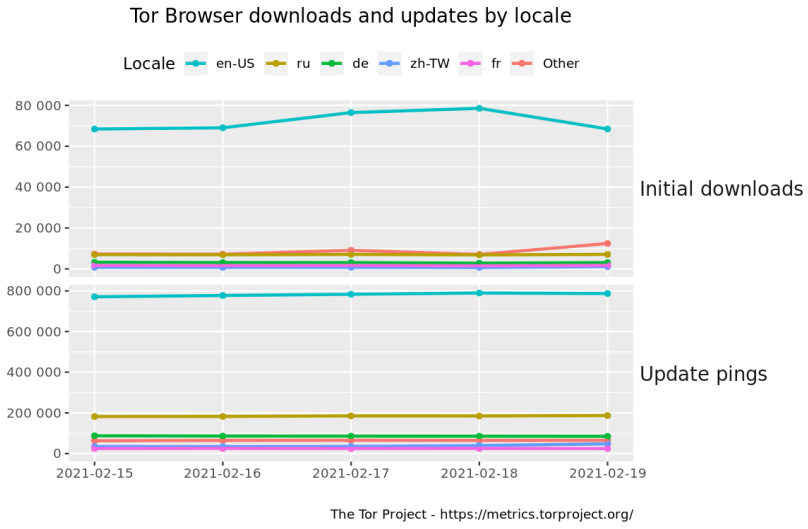
Internet Storm Center Infocon Status

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 in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

* The newest issue in the Cyber Secrets series (#6) - Incident Response: Evidence Preservation and Collection is now availible on Amazon!! This issue Incident Responce and Threat Hunting topics. Great for any security team.

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

Index of Sections

Packet Storm Security

* Browser Tracking Via Favicons Affects Multiple Browsers
* Microsoft Wraps SolarWinds Probe, Nudges Companies Towards Zero Trust
* Apple Outlines 2021 Security, Privacy Roadmap
* WhatsApp To Move Ahead With Privacy Update Despite Backlash
* Masslogger Swipes Outlook, Google Chrome Credentials
* ScamClub Cybergang Campaign Leveraged Safari Flaw
* SolarWinds Attack Hit 100 Companies And Took Months Of Planning, Says White House
* Three More North Korean Hackers Charged
* Spy Pixels In Emails Have Become Endemic
* Dutch Police Post Friendly Warnings On Hacking Forums
* France Ties Russia's Sandworm To A Multiyear Hacking Spree
* Trump's Election Fighting Law Firm Jones Day Gets Breached
* Hackers Are Starting To Code Malware For Apple's M1 Computers
* Unpatched Android App With 1 Billion Downloads Threatens Spying, Malware
* Cybercrooks Rake In $304M In Romance Scams
* Obvious Supply Chain Attack Hits Dozens Of Companies
* North Korea Accused Of Hacking Pfizer For Covid-19 Vaccine Data
* Singtel Suffers Zero-Day Cyberattack, Damage Unknown
* Egregor Ransomware Operators Arrested In Ukraine
* mHealth Apps Expose Millions To Cyberattacks
* A Windows Defender Vuln Lurked Undetected For 12 Years
* Brazil Probes Data Leak Of 102 Million Consumers
* Military, Nuclear Entities Under Target By Novel Android Malware
* Pre-Valentine's Day Malware Attack Mimics Flower, Lingerie Stores
* Microsoft Is Seeing A Big Spike In Web Shell Use

Krebs on Security

* Mexican Politician Removed Over Alleged Ties to Romanian ATM Skimmer Gang
* U.S. Indicts North Korean Hackers in Theft of $200 Million
* Bluetooth Overlay Skimmer That Blocks Chip
* What's most interesting about the Florida water system hack? That we heard about it at all.
* Microsoft Patch Tuesday, February 2021 Edition
* Arrest, Raids Tied to 'U-Admin' Phishing Kit
* Facebook, Instagram, TikTok and Twitter Target Resellers of Hacked Accounts
* 'ValidCC,' a Major Payment Card Bazaar and Looter of E-Commerce Sites, Shuttered
* U.K. Arrest in 'SMS Bandits' Phishing Service
* The Taxman Cometh for ID Theft Victims

Dark Reading

* Kia Denies Ransomware Attack as IT Outage Continues
* Attackers Already Targeting Apple's M1 Chip with Custom Malware
* Omdia's On-Demand Webinars
* How to Fine-Tune Vendor Risk Management in a Virtual World
* Microsoft Concludes Internal Investigation into Solorigate Breach
* CrowdStrike Buys Log Management Startup Humio for $400M
* Apple Offers Closer Look at Its Platform Security Technologies, Features
* Microsoft Azure Front Door Gets a Security Upgrade
* Hiding in Plain Sight: What the SolarWinds Attack Revealed About Efficacy
* Data Security Accountability in an Age of Regular Breaches
* How to Run a Successful Penetration Test
* Virginia Takes Different Tack Than California With Data Privacy Law
* The Edge Pro Tip: Say What You Know
* Egregor Arrests a Blow, but Ransomware Will Likely Bounce Back
* US Unseals Indictments Against North Korean Cyberattackers for Thefts Totaling $1.3B
* White House Says 100 Private Sector Orgs Hit in SolarWinds Campaign
* Kia Faces $20M DoppelPaymer Ransomware Attack
* Ransomware? Let's Call It What It Really Is: Extortionware
* Breach Etiquette: How to Mind Your Manners When It Matters
* Enterprise Windows Threats Drop as Mac Attacks Rise: Report

The Hacker News

* How to Fight Business Email Compromise (BEC) with Email Authentication?
* Chinese Hackers Had Access to a U.S. Hacking Tool Years Before It Was Leaked Online
* New 'Silver Sparrow' Malware Infected Nearly 30,000 Apple Macs
* Privacy Bug in Brave Browser Exposes Dark-Web Browsing History of Its Users
* New Hack Lets Attackers Bypass MasterCard PIN by Using Them As Visa Card
* Masslogger Trojan Upgraded to Steal All Your Outlook, Chrome Credentials
* SolarWinds Hackers Stole Some Source Code for Microsoft Azure, Exchange, Intune
* First Malware Designed for Apple M1 Chip Discovered in the Wild
* U.S. Charges 3 North Korean Hackers Over $1.3 Billion Cryptocurrency Heist
* Agora SDK Bug Left Several Video Calling Apps Vulnerable to Snooping
* Researchers Unmask Hackers Behind APOMacroSploit Malware Builder
* Malvertisers Exploited WebKit 0-Day to Redirect Browser Users to Scam Sites
* Learn How to Manage and Secure Active Directory Service Accounts
* Unpatched ShareIT Android App Flaw Could Let Hackers Inject Malware
* Managed Service Provider? Watch This Video to Learn about Autonomous XDR

Security Week

* Supermarket Chain Kroger Discloses Data Breach
* Cybersecurity M&A Roundup for Week of Feb. 15, 2021
* Privacy Faces Risks in Tech-Infused Post-Covid Workplace
* Mysterious Mac Malware Infected at Least 30,000 Devices Worldwide
* Suspected Russian Hack Fuels New US Action on Cybersecurity
* 1Kosmos Emerges from Stealth Mode With $15 Million in Funding
* Inside the Battle to Control Enterprise Security Data Lakes
* Brussels Okays EU-UK Personal Data Flows
* After IT Outage, Carmakers Kia and Hyundai Say No Evidence of Ransomware Attack
* Virginia Lawmakers Advance Consumer Data Protection Act
* Protecting Against Vaccine-Themed Attacks and Misinformation
* Microsoft: SolarWinds Hackers Attempted to Access Our Systems Until January 2021
* Access Governance Company SPHERE Raises $10 Million
* Apple Platform Security Guide Gets Biggest Update to Date
* France to Boost Cyberdefense After Hospital Malware Attacks
* Elevate the Value of Threat Intelligence in the SOC
* Stored XSS Vulnerability on iCloud.com Earned Researcher $5,000
* Hackers Target Myanmar Government Websites in Coup Protest
* Mac Malware Targeting Apple's M1 Chip Emerges
* US Still Unraveling 'Sophisticated' Hack of 9 Gov't Agencies

Infosecurity Magazine

* Kaspersky Appoints Christopher Hurst GM of UK and Ireland
* BBC Reports Theft of 105 Electrical Devices
* US Retailer Kroger Admits Accellion Breach
* Concern as Attacker "Breakout" Time Halves in 2020
* CIS Offers Free DNS Security Tool for US Hospitals
* US Arrests Six Alleged Cyber-Scam Money Launderers
* Kia Denies Ransomware Attack
* Healthcare Data Breaches Halved in January
* Draft Adequacy Decision Paves the Way for EU-UK Data Flows to Continue Freely
* Kaspersky: Decline in DDoS Attacks Linked to Surge in Cryptocurrency Value
* Shift to Remote Work Necessitating Greater Innovation in Cybersecurity
* CrowdStrike Snaps Up London Start-Up Humio

KnowBe4 Security Awareness Training Blog RSS Feed

* U.K. Phishing Attack Targets Those Seeking the COVID-19 Vaccine
* Be on the Watch for W-2 Phishing Scams!
* The Cybersecurity Book You Should Read
* Popular Car Company Becomes Next Target in $20 Million Dollar Ransomware Attack
* KnowBe4 Named a January 2021 Gartner Peer Insights Customers' Choice for Security Awareness Computer-
* KnowBe4 Adds New Language Localization Options to its Security Awareness Training and Simulated Phish
* The DOJ Charged Two Alleged Members of North Korea's Military Intelligence Services With a Scheme Tha
* Redirection to Zero Days
* Does Your Domain Have an Evil Twin? Find Out for a Chance to Win!
* Bogus Bug Reports as Phishbait, Scams

ISC2.org Blog

* Technology and the New Frontier of the Healthcare Industry (The Internet of Medical Things)
* How You Can Take The CISSP Exam From Home
* The Weeds and Flowers of Information Security
* Garfield Teaches Hawaii Students how to be Safe and Secure Online
* Responsibility and Accountability in the Cloud: Where Does the Buck Stop?

HackRead

* Brave browser Tor feature leaked .Onion queries to ISPs
* SolarWinds hackers accessed source code of Azure, Exchange, Intune
* New variant of MassLogger Trojan stealing Chrome, Outlook data
* The Most Commonly Hacked Smart Home Tech
* US charges 3 North Korean hackers for extorting $1.3+ billion
* Features to look for when choosing VoIP phone system
* Hackers Targeting Apple's M1 Chip with Mac Malware

Koddos

* Brave browser Tor feature leaked .Onion queries to ISPs
* SolarWinds hackers accessed source code of Azure, Exchange, Intune
* New variant of MassLogger Trojan stealing Chrome, Outlook data
* The Most Commonly Hacked Smart Home Tech
* US charges 3 North Korean hackers for extorting $1.3+ billion
* Features to look for when choosing VoIP phone system
* Hackers Targeting Apple's M1 Chip with Mac Malware

Naked Security

* Nvidia announces official "anti-cryptomining" software drivers
* The massive coronavirus IT blunder with a funny side
* S3 Ep20: Corporate megahacking, true love gone bad, and tax grabs [Podcast]
* US names three North Koreans in laundry list of cybercrime charges
* "ScamClub" gang outed for exploiting iPhone browser bug to spew ads
* Romance scams at all-time high: here's what you need to know
* How one man silently infiltrated dozens of high-tech networks
* Naked Security Live - When is a bug bounty not a bug bounty?
* Egregor ransomware criminals allegedly busted in Ukraine
* Fallen victim to online fraud? Here's what to do…

Threat Post

* Malformed URL Prefix Phishing Attacks Spike 6,000%
* Mysterious Silver Sparrow Malware Found Nesting on 30K Macs
* Credential-Stuffing Attack Targets Regional Internet Registry
* Microsoft: SolarWinds Attackers Downloaded Azure, Exchange Code
* Cybercriminal Enterprise 'Ringleaders' Stole $55M Via COVID-19 Fraud, Romance Scams
* Apple Outlines 2021 Security, Privacy Roadmap
* Kia Motors Hit With $20M Ransomware Attack - Report
* Exploit Details Emerge for Unpatched Microsoft Bug
* Mac Malware Targets Apple's In-House M1 Processor
* SDK Bug Lets Attackers Spy on User's Video Calls Across Dating, Healthcare Apps

Null-Byte

* This Master Course Bundle on Coding Is Just $34.99
* How to Automate Remote SSH Control of Computers with Expect Scripts
* This VPN Will Give You a Lifetime of Security for Just $18
* How to Write Your Own Bash Scripts to Automate Tasks on Linux
* Start Learning How to Code in Just a Week
* Create a USB Mouse Jiggler to Keep a Target Computer from Falling Asleep (& Prank Friends Too)
* Boost Your Security with a VPN & Private Email Service
* How to Use RedRabbit for Pen-Testing & Post-Exploitation of Windows Machines
* This Top-Rated Audio & Video Production Bundle Is on Sale for $40
* Null Byte's Hacker Guide to Buying an ESP32 Camera Module That's Right for Your Project

IBM Security Intelligence

* How a CISO's Executive Role Has Changed
* Manufacturing Cybersecurity Threats and How To Face Them
* Cyber Resilience Strategy Changes You Should Know in the EU's Digital Decade
* Braced for Impact: Fostering Good Cloud Security Posture Management
* The Uncertainty of Cybersecurity Hiring
* Firewall Services and More: What's Next for IT?
* Solving 5 Challenges of Contact Tracing Apps
* Unleash the Power of MITRE for a More Mature SOC
* Network Segmentation Series: What is It?
* Beyond Text Messages: How to Secure 2FA Against Phone Authentication Scams

InfoWorld

* IT Salary Survey 2021: Compensation holds steady despite pandemic
* The real value of open source in the cloud
* How to use LazyCache in ASP.NET Core MVC 5
* Why Microsoft Azure wins with enterprise customers
* The Linux Foundation adds 7 projects to combat racial injustice
* "Do More with R" video tutorials
* Microsoft unveils first .NET 6 preview
* Cloud overspending spotlights the need for cost governance
* Google introduces API for faster Kotlin builds
* 3 ways to get into reinforcement learning

C4ISRNET - Media for the Intelligence Age Military

* Geospatial intelligence could offer blueprint for protecting national security through technological
* GEOINT provider BlackSky to go public through merger with investment company
* Host of challenges await next Pentagon CIO
* Live-fire drill puts Europe's military cyber responders to the test
* Threats abound as defense agencies make long-term move to hybrid work patterns
* Special Forces to build 'influence artillery' for online campaigns
* Space Force says new anti-jamming upgrade coming in 2022
* Transforming Command and Control - A Strategic Imperative for the Warfighter
* With the submarine threat on the rise, the US Navy looks to autonomous water sensor drones
* Space Operations Command taps LinQuest for support

The Hacker Corner

Conferences

* 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!
* Best Web Application Conferences 2021 - 2022

Google Zero Day Project

* Déjà vu-lnerability
* A Look at iMessage in iOS 14

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.

* Ugra CTF Quals 2021
* Aero CTF 2021
* zer0pts CTF 2021
* NahamCon CTF 2021
* UTCTF 2021
* vishwaCTF 2021
* BCA CTF 2021
* LINE CTF 2021
* PoseidonCTF 2nd Edition
* SPRUSH CTF Quals 2021

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

* y0usef: 1
* BlueSky: 1
* Chill Hack: 1
* Jetty: 1
* DevGuru: 1

Tools & Techniques

Packet Storm Security Tools Links

* Faraday 3.14.1
* OpenSSL Toolkit 1.1.1j
* TOR Virtual Network Tunneling Tool 0.4.5.6
* Recon Informer 1.3
* AIDE 0.17.3
* AIDE 0.17.2
* TOR Virtual Network Tunneling Tool 0.4.4.7
* Clam AntiVirus Toolkit 0.103.1
* Mandos Encrypted File System Unattended Reboot Utility 1.8.14
* SQLMAP - Automatic SQL Injection Tool 1.5.2

Kali Linux Tutorials

* GitLab Watchman : Monitoring GitLab For Sensitive Data Shared Publicly
* OSV : Open Source Vulnerabilities
* UDdup : Urls De-Duplication Tool For Better Recon
* Damn Vulnerable GraphQL Application
* BaphoDashBoard : Dashboard For Manage & Generate The Baphomet Ransomware
* XSSTRON : Electron JS Browser To Find XSS Vulnerabilities
* What is DNS Filtering and How to Use It for Safe Browsing
* Pineapple MK7 REST Client : WiFi Hacking Workflow With Pineapple Mark 7 API
* K55 : Linux X86_64 Process Injection Utility
* RadareEye : A Tool Made For Specially Scanning Nearby devices

GBHackers Analysis

* Unpatched SHAREit Flaw Let Attackers Execute Remote Code
* Microsoft will Enable Domain Controller Enforcement Mode to Address Zerologon Flaw
* Hackers Using 4 Zero-day Vulnerabilities to Attack Windows and Android Devices Remotely
* Secret Backdoor found Installed in Zyxel Firewall and VPN
* Critical Dell Wyse Bugs Let Attackers to Execute Code and Access Files and Credentials

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Pivoting from Art to Science | SANS CTI Summit 2021
* Episode 174: Apple Security: System Integrity Protection
* The Joy of Threat Landscaping | SANS CTI Summit 2021
* Threat Intel for Everyone: Writing Like A Journalist To Produce Clear, Concise Reports | CTI Summit

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

* Phishing Using Morse Code, Signal Responds to Iran Ban, Chrome Zero Day News - ThreatWire
* Unlimited LTE Hotspot on PC via Phone or USB modem! -GlytchTips
* Emotet Botnet Sinkholed, Apple Adds App Tracking Opt-In - ThreatWire

The PC Security Channel [TPSC]

* Windows Defender vs Ransomware in 2021
* Best Browser Extensions for Security

Eli the Computer Guy

* Arduino - Raspberry Pi Web Fan Control with MySQL
* DELIVERY TRUCK ROBBED
* APPLE LEADS by REMOVING CHARGER - Xiaomi Follows
* REDDITORS BUY TIMES SQUARE BILLBOARD for GAMESTOP STOCK

Security Now

* C.O.M.B. - Florida Water Supply Hack Update, Major Patch Tuesday, Android SHAREit Vulnerability
* SCADA Scandal - Defender Thinks Chrome is Malware, Plex Media Servers in DDoS Attacks

Troy Hunt

* Weekly Update 231

Intel Techniques: The Privacy, Security, & OSINT Show

* 207-VPN Routers Revisited
* 206-Website Analytics Concerns & Solutions

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Firejail TOCTOU Race Condition
* dataSIMS Avionics ARINC 664-1 4.5.3 Buffer Overflow
* Online Exam System With Timer 1.0 SQL Injection
* Beauty Parlour Management System 1.0 Cross Site Scripting
* Beauty Parlour Management System 1.0 SQL Injection
* Backdoor.Win32.Bionet.10 Anonymous Login
* Comment System 1.0 Cross Site Scripting
* Backdoor.Win32.DarkKomet.apcc Insecure Permissions
* Backdoor.Win32.DarkKomet.bhfh Insecure Permissions
* OpenText Content Server 20.3 Cross Site Scripting
* Neo LMS / Matrix LMS Cross Site Scripting
* Backdoor.Win32.Agent.aak Buffer Overflow
* Batflat CMS 1.3.6 Remote Code Execution
* Apport 2.20 Privilege Escalation
* Backdoor.Win32.Agent.aak Code Execution / Cross Site Request Forgery
* Backdoor.Win32.Agent.aak Hardcoded Credentials
* Gitea 1.12.5 Remote Code Execution
* Billing Management System 2.0 SQL Injection
* Faulty Evaluation System 1.0 Cross Site Scripting
* Backdoor.Win32.Burbul.b Anonymous Login
* Backdoor.Win32.Indexer.a Denial Of Service
* BlackCat CMS 1.3.6 Cross Site Scripting
* Managed Switch Port Mapping Tool 2.85.2 Denial Of Service
* Backdoor.Win32.Indexer.a Hardcoded Credentials
* Nsauditor 3.2.2.0 Denial Of Service

CXSecurity

* Recon-Informer v1.3 - Intel for offensive systems anti-reconnaissance (nmap) tool
* dataSIMS Avionics ARINC 664-1 Local Buffer Overflow (PoC)
* Batflat CMS 1.3.6 Remote Code Execution
* TestLink 1.9.20 Shell Upload
* SEO Panel 4.6.0 Remote Code Execution (2)
* PhreeBooks 5.2.3 Remote Code Execution
* Solaris 10 1/13 (SPARC) dtprintinfo Local Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

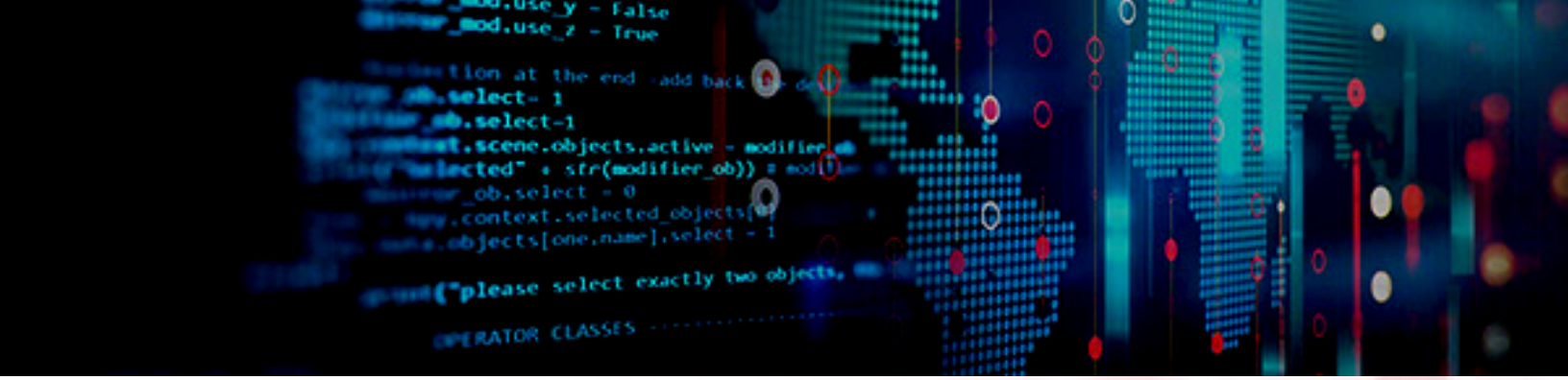
* [webapps] Beauty Parlour Management System 1.0 - 'sername' SQL Injection
* [webapps] OpenText Content Server 20.3 - 'multiple' Stored Cross-Site Scripting
* [local] dataSIMS Avionics ARINC 664-1 - Local Buffer Overflow (PoC)
* [webapps] Online Exam System With Timer 1.0 - 'email' SQL injection Auth Bypass
* [webapps] Comment System 1.0 - 'multiple' Stored Cross-Site Scripting
* [webapps] PEEL Shopping 9.3.0 - 'Comments/Special Instructions' Stored Cross-Site Scripting
* [webapps] Batflat CMS 1.3.6 - Remote Code Execution (Authenticated)
* [local] Apport 2.20 - Local Privilege Escalation
* [webapps] Gitea 1.12.5 - Remote Code Execution (Authenticated)
* [webapps] Billing Management System 2.0 - 'email' SQL injection Auth Bypass
* [webapps] Faulty Evaluation System 1.0 - 'multiple' Stored Cross-Site Scripting
* [dos] Nsauditor 3.2.2.0 - 'Event Description' Denial of Service (PoC)
* [dos] AgataSoft PingMaster Pro 2.1 - Denial of Service (PoC)
* [dos] Managed Switch Port Mapping Tool 2.85.2 - Denial of Service (PoC)
* [webapps] BlackCat CMS 1.3.6 - 'Display name' Cross Site Scripting (XSS)
* [webapps] Online Internship Management System 1.0 - 'email' SQL injection Auth Bypass
* [local] Tasks 9.7.3 - Insecure Permissions
* [webapps] Teachers Record Management System 1.0 - 'searchteacher' SQL Injection
* [webapps] TestLink 1.9.20 - Unrestricted File Upload (Authenticated)
* [webapps] School Event Attendance Monitoring System 1.0 - 'Item Name' Stored Cross-Site Scripting
* [webapps] School File Management System 1.0 - 'multiple' Stored Cross-Site Scripting
* [local] PDFCOMPLETE Corporate Edition 4.1.45 - 'pdfcDispatcher' Unquoted Service Path
* [webapps] Online Marriage Registration System (OMRS) 1.0 - Remote code execution (3)
* [webapps] Openlitespeed WebServer 1.7.8 - Command Injection (Authenticated) (2)
* [webapps] b2evolution 6.11.6 - 'tab3' Reflected XSS

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

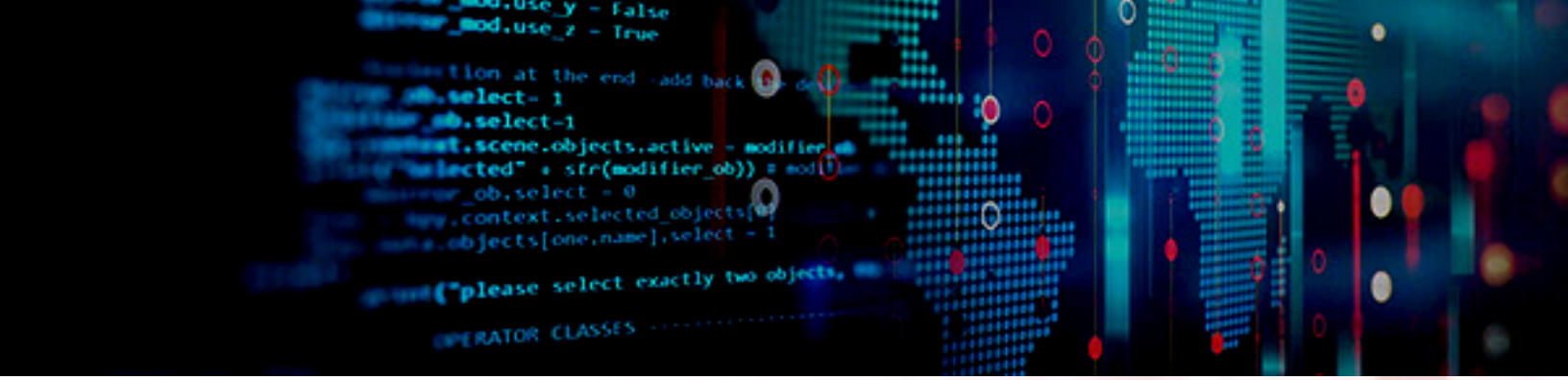
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://sgddt.dongnai.gov.vn/0x48.txt
http://sgddt.dongnai.gov.vn/0x48.txt notified by FRK48
https://intranet.pmo.gov.ps/0x48.txt
https://intranet.pmo.gov.ps/0x48.txt notified by FRK48
http://e-learning.rid.go.th/0x48.txt
http://e-learning.rid.go.th/0x48.txt notified by FRK48
http://www.pn-tilamuta.go.id/perpustakaan//repository/krz.txt
http://www.pn-tilamuta.go.id/perpustakaan//repository/krz.txt notified by Mr.Kro0oz.305
http://www.pn-semarapura.go.id/perpustakaan//repository/krz.txt
http://www.pn-semarapura.go.id/perpustakaan//repository/krz.txt notified by Mr.Kro0oz.305
http://www.pn-buntok.go.id/perpustakaan//repository/krz.txt
http://www.pn-buntok.go.id/perpustakaan//repository/krz.txt notified by Mr.Kro0oz.305
http://perpustakaan.pa-dompu.go.id//repository/krz.txt
http://perpustakaan.pa-dompu.go.id//repository/krz.txt notified by Mr.Kro0oz.305
http://pa-dompu.go.id/perpustakaan/repository/krz.txt
http://pa-dompu.go.id/perpustakaan/repository/krz.txt notified by Mr.Kro0oz.305
http://www.cs.moe.go.th/1.php
http://www.cs.moe.go.th/1.php notified by -1
http://yns.gov.my/r4s.html
http://yns.gov.my/r4s.html notified by Ren4Sploit
http://pkdkulai.gov.my/r4s.html
http://pkdkulai.gov.my/r4s.html notified by Ren4Sploit
http://pahanglibrary.gov.my/r4s.html
http://pahanglibrary.gov.my/r4s.html notified by Ren4Sploit
http://pkbf.gov.my/r4s.html
http://pkbf.gov.my/r4s.html notified by Ren4Sploit
http://mpkb-bri.gov.my/r4s.html
http://mpkb-bri.gov.my/r4s.html notified by Ren4Sploit
http://muftikelantan.gov.my/r4s.html
http://muftikelantan.gov.my/r4s.html notified by Ren4Sploit
http://nutrikl.gov.my/r4s.html
http://nutrikl.gov.my/r4s.html notified by Ren4Sploit
http://lpbm.gov.my/r4s.html
http://lpbm.gov.my/r4s.html notified by Ren4Sploit



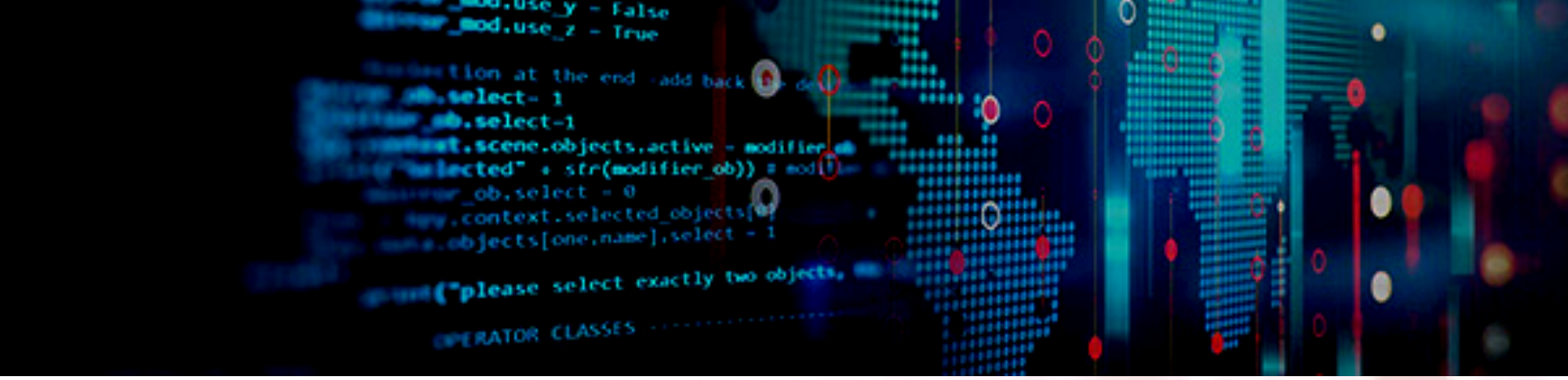
Dark Web News

Darknet Live

Australian Border Force Seizes Meth Inside a Stuffed Llama
An Australian man was charged for attempting to import meth inside a stuffed llama even though he burned the pack before the cops showed up. (via darknetlive.com)
New Change to German Postal Law Targets Internet Drug Trade
The German government passed a draft law that requires employees of private postal services to report packages of drugs to law enforcement. (via darknetlive.com)
Dream Market Vendor "Rackjaw2" Sentenced to Prison
A 52-year-old from Everett, Washington, was sentenced to four years in prison for selling methamphetamine and heroin on the darkweb. (via darknetlive.com)
Feds Traced Bitcoin Transactions to a Drug Dealer's Apartment
Feds identified a darkweb vendor by linking Bitcoin transactions to an apartment I.P. address. They also monitored his internet traffic. (via darknetlive.com)

Dark Web Link

What Are Phishing Attacks? How To Identify And Scam Prevention Tips
The advent of modernization in the digital landscape has brought with it different variations in digital threat landscape. Of all, undoubtedly phishing attacks of all types are the most prevalent ones. In the 2020 Data Breach Investigations Report, the Verizon Enterprise had uncovered that phishing had been the second top-most cyber threat in the security [...] The post What Are Phishing Attacks? How To Identify And Scam Prevention Tips appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
How Australian Cops Found Darknet Meth In A Stuffed Llama
An Australian man had been charged in the Perth Magistrates Court for trying to import methamphetamine, commonly known as Meth, hidden in a stuffed llama toy. In the darknet meth supply process, the Australian border cops guessed that there is something very suspicious about the children's stuff toy. In the bid to get past the Australian law [...] The post How Australian Cops Found Darknet Meth In A Stuffed Llama appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Cyber Attack Ransom: N.Carolina County Rejects BTC Having Value Of $2.4M
A cyber attack had been conducted on Chatham County, North Carolina back on the 28th of October last year. During that period, an investigation on the computer network revealed that personal information had been posted on the dark web. The hackers have claimed a cyber attack ransom following that. The computer network had been hit with DoppelPaymer [...] The post Cyber Attack Ransom: N.Carolina County Rejects BTC Having Value Of $2.4M appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

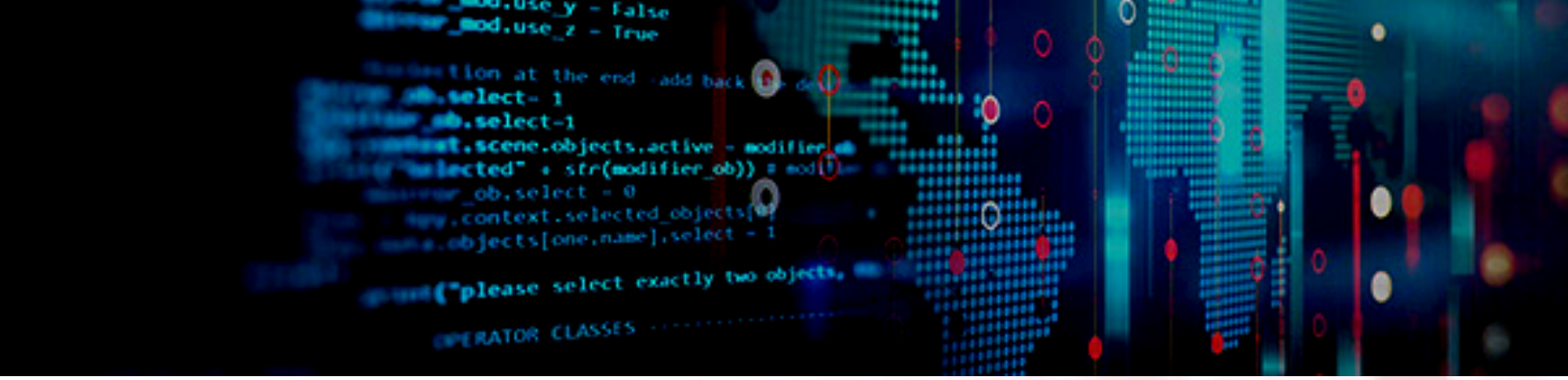
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing 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

Unfortunately, at the time of this report, the RiskIQ resource was not availible.

FireEye

* Metasploit Wrap-Up
* Take the Full-Stack Approach to Securing Your Modern Attack Surface
* Securing Your Web App, One Robot at a Time
* Why More Teams are Shifting Security Analytics to the Cloud This Year
* Monitor Google Cloud Platform (GCP) Data With InsightIDR
* Metasploit Wrap-Up
* Talkin' SMAC: Alert Labeling and Why It Matters
* New InsightVM Dashboard Helps You Discover Significant Changes in Your Environment from the Past 30 D
* CVE-2021-22652: Advantech iView Missing Authentication RCE (FIXED)
* SOAR Tools: What to Look for When Investing in Security Automation Tech



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for AnyConnect Secure Mobility Client
* Google Releases Security Updates for Chrome
* North Korean Malicious Cyber Activity: AppleJeus
* VMware Releases Security Update
* Compromise of U.S. Water Treatment Facility
* Verify Your Valentine
* Microsoft Launches Phase 2 Mitigation for Netlogon Remote Code Execution Vulnerability (CVE-2020-1472
* Microsoft Releases February 2021 Security Updates
* AA21-048A: AppleJeus: Analysis of North Korea's Cryptocurrency Malware
* AA21-042A: Compromise of U.S. Water Treatment Facility
* Vulnerability Summary for the Week of February 8, 2021
* Vulnerability Summary for the Week of February 1, 2021

Zero Day Initiative Advisories

ZDI-CAN-12814: GoPro
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 'garmin' was reported to the affected vendor on: 2021-02-15, 7 days ago. The vendor is given until 2021-06-15 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-13041: GoPro
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: 2021-02-15, 7 days ago. The vendor is given until 2021-06-15 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-12710: OpenText
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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12711: OpenText
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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12712: OpenText
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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12890: Arlo

A CVSS score 6.8 (AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Team FLASHBACK: Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) + Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12718: OpenText

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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12716: OpenText

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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12717: OpenText

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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12715: OpenText

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 'rgod' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-13039: Advantech

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-13038: Advantech

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12579: Apple

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'mipu94 of SEFCOM lab, ASU.' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-13244: 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: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-13245: 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: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-13131: Siemens

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 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-12, 10 days ago. The vendor is given until 2021-06-12 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-12986: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-12919: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-12984: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-13227: 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: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-12708: OpenText

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 'rgod' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-12987: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-13241: 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: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 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-13101: 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 'Xu Peng from UCAS and Wang Yanhao from QiAnXin Technology Research Institute ' was reported to the affected vendor on: 2021-02-10, 12 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-0611-01

Red Hat Security Advisory 2021-0611-01 - The xterm program is a terminal emulator for the X Window System. It provides DEC VT102 and Tektronix 4014 compatible terminals for programs that can't use the window system directly.

Asterisk Project Security Advisory - AST-2021-005

Given a scenario where an outgoing call is placed from Asterisk to a remote SIP server it is possible for a crash to occur. The code responsible for negotiating SDP in SIP responses incorrectly assumes that SDP negotiation will always be successful. If a SIP response containing an SDP that can not be negotiated is received a subsequent SDP negotiation on the same call can cause a crash.

Ubuntu Security Notice USN-4741-1

Ubuntu Security Notice 4741-1 - It was discovered that Jackson Databind incorrectly handled deserialization. An attacker could possibly use this issue to execute arbitrary code.

Asterisk Project Security Advisory - AST-2021-004

Due to a signedness comparison mismatch, an authenticated WebRTC client could cause a stack overflow and Asterisk crash by sending multiple hold/unhold requests in quick succession.

Asterisk Project Security Advisory - AST-2021-003

An unauthenticated remote attacker could replay SRTP packets which could cause an Asterisk instance configured without strict RTP validation to tear down calls prematurely.

Asterisk Project Security Advisory - AST-2021-002

When re-negotiating for T.38 if the initial remote response was delayed just enough Asterisk would send both audio and T.38 in the SDP. If this happened, and the remote responded with a declined T.38 stream then Asterisk would crash.

Asterisk Project Security Advisory - AST-2021-001

If a registered user is tricked into dialing a malicious number that sends lots of 181 responses to Asterisk, each one will cause a 181 to be sent back to the original caller with an increasing number of entries in the ???Supported??? header. Eventually the number of entries in the header exceeds the size of the entry array and causes a crash.

Ubuntu Security Notice USN-4739-1

Ubuntu Security Notice 4739-1 - 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.

Ubuntu Security Notice USN-4738-1

Ubuntu Security Notice 4738-1 - Paul Kehrer discovered that OpenSSL incorrectly handled certain input lengths in EVP functions. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer fields. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4737-1

Ubuntu Security Notice 4737-1 - It was discovered that Bind incorrectly handled GSSAPI security policy negotiation. A remote attacker could use this issue to cause Bind to crash, resulting in a denial of service, or possibly execute arbitrary code. In the default installation, attackers would be isolated by the Bind AppArmor profile.

Red Hat Security Advisory 2021-0423-01

Red Hat Security Advisory 2021-0423-01 - 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 4.6.17. Issues addressed include cross site scripting, denial of service, deserialization, and traversal vulnerabilities.

IrfanView 4.57 Denial Of Service / Code Execution

IrfanView version 4.57 with WPG.dll version 2.0.0.0 suffer from access violation and out-of-bounds write vulnerabilities that can lead to denial of service or code execution.

Red Hat Security Advisory 2021-0603-01

Red Hat Security Advisory 2021-0603-01 - Red Hat Decision Manager is an open source decision management platform that combines business rules management, complex event processing, Decision Model & Notation execution, and Business Optimizer for solving planning problems. It automates business decisions and makes that logic available to the entire business. This release of Red Hat Decision Manager 7.10.0 serves as an update to Red Hat Decision Manager 7.9.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a remote SQL injection vulnerability.

Red Hat Security Advisory 2021-0600-01

Red Hat Security Advisory 2021-0600-01 - 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 7.10.0 serves as an update to Red Hat Process Automation Manager 7.9.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a remote SQL injection vulnerability.

Ubuntu Security Notice USN-4734-2

Ubuntu Security Notice 4734-2 - USN-4734-1 fixed several vulnerabilities in wpa_supplicant. This update provides the corresponding update for Ubuntu 14.04 ESM. It was discovered that wpa_supplicant did not properly handle P2P group information in some situations, leading to a heap overflow. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that hostapd did not properly handle UPnP subscribe messages in some circumstances. An attacker could use this to cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-0599-01

Red Hat Security Advisory 2021-0599-01 - Red Hat Directory Server is an LDAPv3-compliant directory server. The suite of packages includes the Lightweight Directory Access Protocol server and command-line utilities for server administration, the Administration Server HTTP agent package, and the GUI console packages. Issues addressed include an information leakage vulnerability.

Ubuntu Security Notice USN-4736-1

Ubuntu Security Notice 4736-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, or execute arbitrary code. It was discovered that responses received during the plaintext phase of the STARTTLS connection setup were subsequently evaluated during the encrypted session. A person in the middle could potentially exploit this to perform a response injection attack. Various other issues were also addressed.

Red Hat Security Advisory 2021-0557-01

Red Hat Security Advisory 2021-0557-01 - Perl is a high-level programming language that is commonly used for system administration utilities and web programming. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0531-01

Red Hat Security Advisory 2021-0531-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Red Hat Security Advisory 2021-0549-01

Red Hat Security Advisory 2021-0549-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include HTTP request smuggling, denial of service, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0558-01

Red Hat Security Advisory 2021-0558-01 - 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 2021-0548-01

Red Hat Security Advisory 2021-0548-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include HTTP request smuggling, buffer overflow, denial of service, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0538-01

Red Hat Security Advisory 2021-0538-01 - Network Security Services is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2021-0551-01

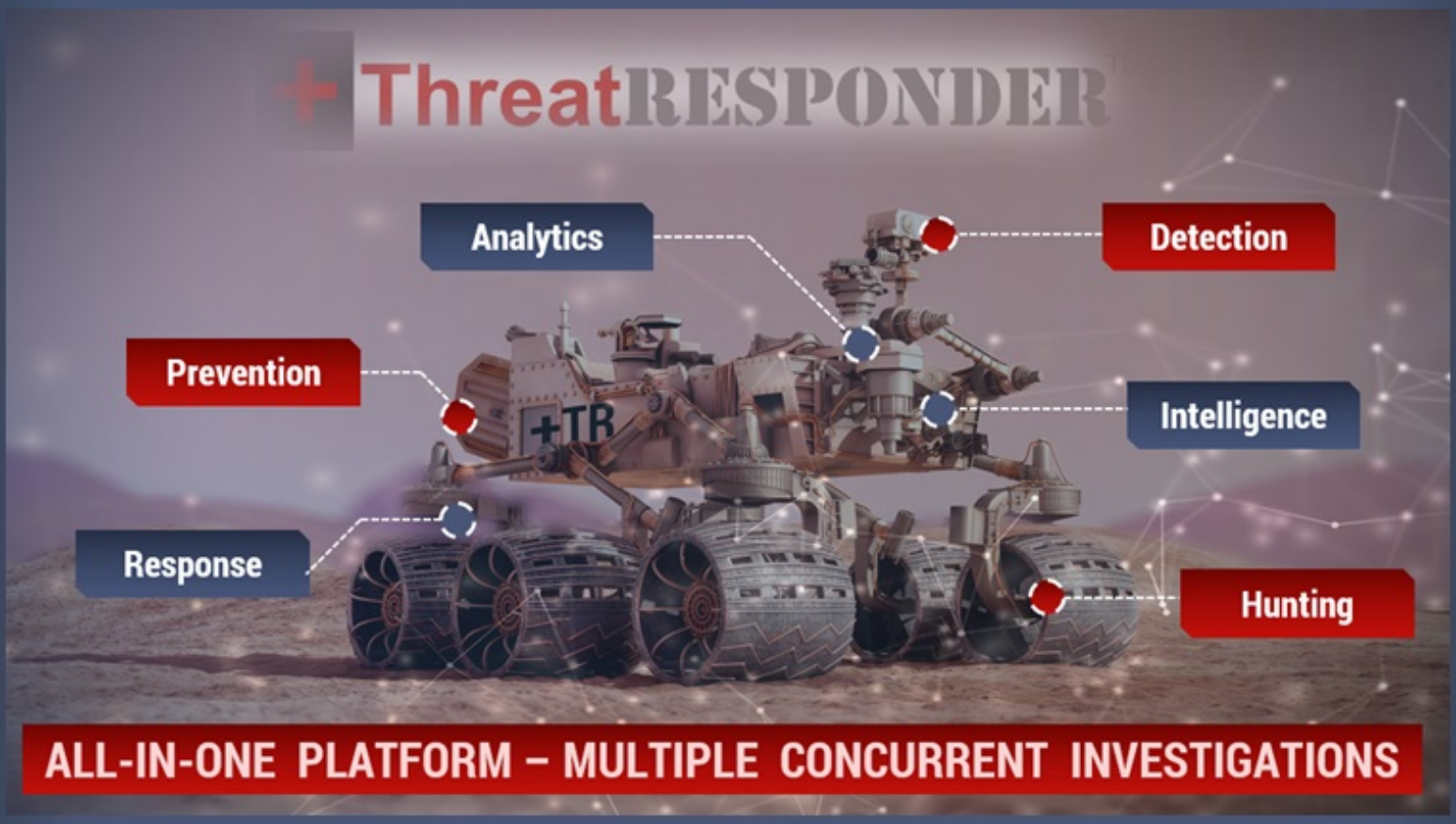
Red Hat Security Advisory 2021-0551-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include HTTP request smuggling, denial of service, and use-after-free vulnerabilities.

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



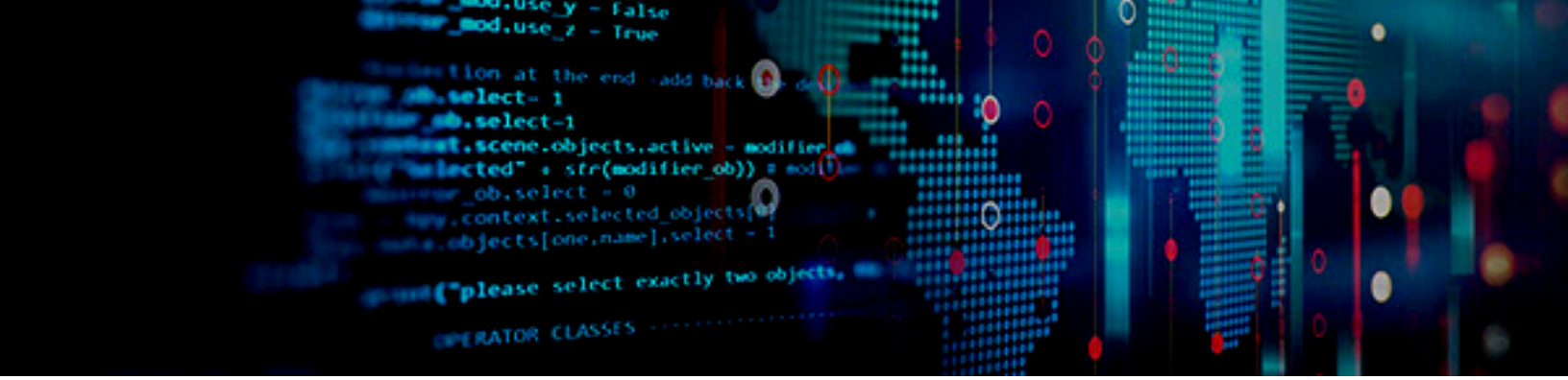
The Solution – ThreatResponder® Platform

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

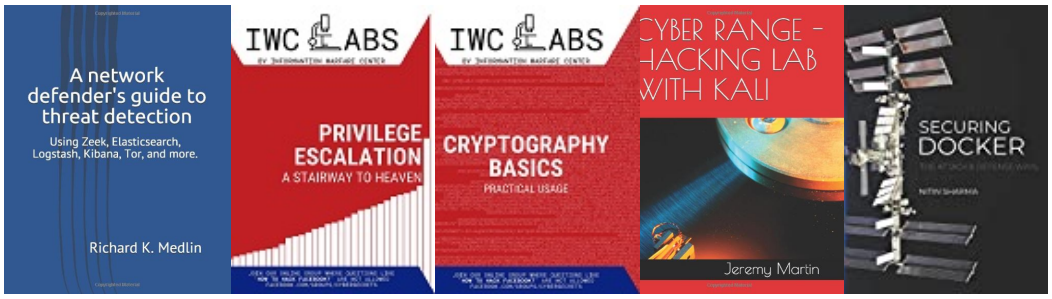


The Cyber Secrets publications on Amazon

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