Feb-01-21

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 1, 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

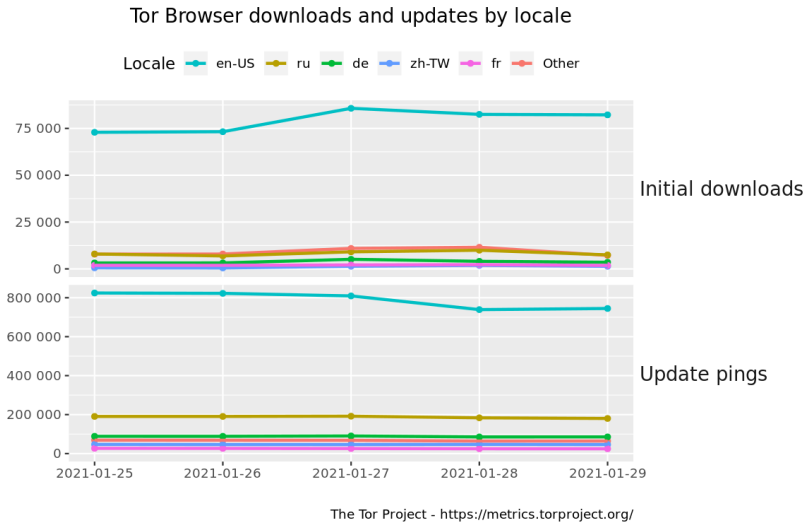
Internet Storm Center Infocon Status

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

* Rocke Group's Malware Now Has Worm Capabilities
* Bitcoin Soars 14% After Elon Musk Namecheck On Twitter
* Google Bans Another Misbehaving CA From Chrome
* Apple Comes Out Swinging Against Facebook Over Data Privacy
* $2.3 Million Settlement Reached With Citrix Over Data Breach
* TikTok Vulnerability Left Users' Private Information Exposed
* 2019 Stack Overflow Hack Guided By Advice On Stack Overflow
* New Social Media Site Pillowfort Is Riddled With Basic Bugs
* Insurers Defend Covering Ransomware Payments
* 23 Million Gamer Records Exposed In VIPGames Leak
* Apple Patches Three Actively Exploited Zero Days
* Emotet Botnet Disrupted By International Police Operation
* Former LulzSec Hacker Releases SonicWall VPN Zero-Day
* Dutch COVID-19 Patient Data Sold On The Criminal Underground
* The History Of The Connected Battlespace, Part One
* Google: North Korean Hackers Have Targeted Security Researchers Via Social Media
* DreamBus Botnet Targets Enterprise Apps Running On Linux Servers
* DDoSers Are Abusing Microsoft RDP To Make Attacks More Powerful
* ADT Tech Hacks Home Security Cameras To Spy On Women
* SonicWall Says It Was Hacked Using Zero-Days In Its Own Products
* Biden Beefs Up Cybersecurity Team Post SolarWinds Hack
* Bugs Allowed Hackers To Hijack Kindle Accounts With Malicious Ebooks
* Hackers Publish Thousands Of Files After Govt Refuses To Pay Ransom
* New Website Launched To Document Vulnerabilities In Malware Strains
* Google Searches Expose Stolen Corporate Credentials

Krebs on Security

* The Taxman Cometh for ID Theft Victims
* Arrest, Seizures Tied to Netwalker Ransomware
* International Action Targets Emotet Crimeware
* DDoS-Guard To Forfeit Internet Space Occupied by Parler
* New Charges Derail COVID Release for Hacker Who Aided ISIS
* Joker's Stash Carding Market to Call it Quits
* Microsoft Patch Tuesday, January 2021 Edition
* SolarWinds: What Hit Us Could Hit Others
* Ubiquiti: Change Your Password, Enable 2FA
* Sealed U.S. Court Records Exposed in SolarWinds Breach

Dark Reading

* 6 Cybersecurity Start-Up Trends to Track
* Cloud Security Startup Armo Emerges from Stealth with $4.5M
* FBI Encounters: Reporting an Insider Security Incident to the Feds
* Ransomware Payoffs Surge by 311% to Nearly $350 Million
* Is the Web Supply Chain Next in Line for State-Sponsored Attacks?
* 2020 Marked a Renaissance in DDoS Attacks
* Law Enforcement Aims to Take Down Netwalker Ransomware
* Breach Data Highlights a Pivot to Orgs Over Individuals
* Digital Identity Is the New Security Control Plane
* Building Your Personal Privacy Risk Tolerance Profile
* App Variety -- and Security Innovation -- Surged in 2020
* Data Privacy Day 2021: Pandemic Response Data Must Align with Data Privacy Rules
* Intl. Law Enforcement Operation Disrupts Emotet Botnet
* Critical Vulnerability Patched in 'sudo' Utility for Unix-Like OSes
* Microsoft Security Business Exceeds $10B in Revenue
* 4 Clues to Spot a Bot Network
* Many Cybersecurity Job Candidates Are Subpar, While On-the-Job Training Falls Short
* Apple Patches Three iOS Zero-Day Vulnerabilities
* Security's Inevitable Shift to the Edge
* LogoKit Group Aims for Simple Yet Effective Phishing

The Hacker News

* A New Software Supply‑Chain Attack Targeted Millions With Spyware
* LIVE Webinar: Major Lessons to be Learned from Top Cyber Attacks in 2020
* New Cryptojacking Malware Targeting Apache, Oracle, Redis Servers
* Google Discloses Severe Bug in Libgcrypt Encryption Library-Impacting Many Projects
* Google uncovers new iOS security feature Apple quietly added after zero-day attacks
* New CISOs Survey Reveals How Small Cybersecurity Teams Can Confront 2021
* Hezbollah Hacker Group Targeted Telecoms, Hosting, ISPs Worldwide
* Italy CERT Warns of a New Credential Stealing Android Malware
* Authorities Seize Dark-Web Site Linked to the Netwalker Ransomware
* European Authorities Disrupt Emotet - World's Most Dangerous Malware
* New Docker Container Escape Bug Affects Microsoft Azure Functions
* Warning Issued Over Hackable ADT's LifeShield Home Security Cameras
* New Attack Could Let Remote Hackers Target Devices On Internal Networks
* Top Cyber Attacks of 2020
* Using the Manager Attribute in Active Directory (AD) for Password Resets

Security Week

* OwnBackup Achieves 'Unicorn' Status With $167.5 Million Funding Round
* Root9B, Fidem in Cybersecurity M&A Round-Up for January 2021
* Hijacked Perl.com Domain Hosted on IP Address Linked to Malicious Activity
* OT Cybersecurity Firm Mission Secure Raises $5.6 Million in Series B Funding
* UScellular Breach Allowed Hackers to Port Customer Phone Numbers
* Unemployment Fraud - Preying on Those Most in Need
* Tanium Announces $150 Million Funding Investment From Ontario Teachers'
* Elusive Lebanese Threat Actor Compromised Hundreds of Servers
* Deep Analysis of More than 60,000 Breach Reports Over Three Years
* Attacks on Individuals Fall as Cybercrime Shifts Tactics
* Encrypted Services Providers Concerned About EU Proposal for Encryption Backdoors
* TPG Capital Acquires Majority Stake in PAM Solutions Provider Centrify
* Many WordPress Sites Affected by Vulnerabilities in 'Popup Builder' Plugin
* Apple CEO Escalates Battle With Facebook Over Online Privacy
* Apple Adds 'BlastDoor' to Secure iPhones From Zero-Click Attacks
* For Microsoft, Security is a $10 Billion Business
* Security Resolutions to Make in 2021
* Many European CISOs Shift Focus to Mobile Security: Survey
* Law Enforcement Planning Emotet Cleanup Operation Following Botnet Takedown
* Apple to Crack Down on Tracking iPhone Users in Early Spring

Infosecurity Magazine

* Facial Recognition Ethical Framework Launched by BSIA
* Researchers Spot SonicWall Exploit in the Wild
* Trickbot Trojan Back from the Dead in New Campaign
* Global Government Outsourcer Serco Hit by Ransomware
* Cyber-Cop Charged with Forgery and Bigamy
* Miss England Held to Ransom by Cyber-attackers
* Texas Tech Company Scoops Fourth Equality Title
* A Fifth of Sunburst Backdoor Victims from Manufacturing Industry
* #DataPrivacyDay: Organizations Must Increase Focus on Data Privacy in 2021
* 66% of Workers Risk Breaching GDPR by Printing Work-Related Docs at Home
* Apprenticeships Could Solve Cyber-Skills Crisis, Say Experts
* Delivery Biz Exposes 400 Million Records in Privacy Snafu

KnowBe4 Security Awareness Training Blog RSS Feed

* KnowBe4 graduates to become one of Okta's most popular apps by number of customers
* KnowBe4 Fresh Content Updates from January: Including 'The Inside Man' Season 3 Official Trailer
* [HEADS UP] New Phishing Kit Spotted on Over 700 Domains
* Beware the Long Con Phish
* Data Privacy and Fingerprints
* 2021 Begins a New Decade of Privacy
* NSA Warns Against Using Third-Party DNS and Encourages DNS Over HTTPS
* Australians Experienced over 200K Scams in 2020 Costing Over A$176 Million
* UK Insurer Defends the Coverage of Ransomware Payments
* A UK Case Study: Recognizing COVID-19 Phishing

ISC2.org Blog

* Looking for Resources on Privacy? You've Come to the Right Place
* Biden Administration Seeks $9 Billion for Emergency Cybersecurity Improvements
* Evolution vs. Extinction
* (ISC)² Cybersecurity Webinars Available On-Demand on BrightTalk
* How Access Control and Network Segmentation Can Protect Your Assets

HackRead

* Microsoft patent reveals chatbot to talk to dead people
* Popular Shopify app exposes private data of thousands of shoppers
* Windows finger command abused to download MineBridge backdoor
* 5 cases when ethical hackers saved companies from devastating hacks
* Hezbollah linked hackers hit companies in global malware attack
* BYKEA data breach: Pakistani ride-hailing app exposed 400m records
* This malware hides behind free VPN, pirated security software keys

Koddos

* Microsoft patent reveals chatbot to talk to dead people
* Popular Shopify app exposes private data of thousands of shoppers
* Windows finger command abused to download MineBridge backdoor
* 5 cases when ethical hackers saved companies from devastating hacks
* Hezbollah linked hackers hit companies in global malware attack
* BYKEA data breach: Pakistani ride-hailing app exposed 400m records
* This malware hides behind free VPN, pirated security software keys

Naked Security

* Emotet takedown - Europol attacks "world's most dangerous malware"
* GnuPG crypto library can be pwned during decryption - patch now!
* The mystery of the missing Perl website
* Cybersecurity tips for university students
* S3 Ep17: Facemasks, hidden ads and paranormal hacking [Podcast]
* Apple critical patches fix in-the-wild iPhone exploits - update now!
* Ghost hack - criminals use deceased employee's account to wreak havoc
* Ready to take the red pill? Catch up with Keren Elazari at Sophos Evolve
* Naked Security Live - Don't let digital jokes turn into digital disasters
* US administration adds "subliminal" ad to White House website

Threat Post

* WordPress Pop-Up Builder Plugin Flaw Plagues 200K Sites
* Microsoft 365 Becomes Haven for BEC Innovation
* Industrial Gear at Risk from Fuji Code-Execution Bugs
* Apple iOS 14 Thwarts iMessage Attacks With BlastDoor System
* Lazarus Affiliate 'ZINC' Blamed for Campaign Against Security Researcher
* Rocke Group's Malware Now Has Worm Capabilities
* Utah Ponders Making Online 'Catfishing' a Crime
* LogoKit Simplifies Office 365, SharePoint 'Login' Phishing Pages
* Mimecast Confirms SolarWinds Hack as List of Security Vendor Victims Snowball
* TeamTNT Cloaks Malware With Open-Source Tool

Null-Byte

* Start Learning How to Code in Just a Week
* Create a Mouse Jiggler with a Digispark & Arduino to Keep a Target Computer from Falling Asleep
* 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
* This HD Infographic Design Software Is on Sale for $45
* How to Perform Keystroke Injection Attacks Over Wi-Fi with Your Smartphone
* Stay Fully in Sync with Your Remote Team Using TimeSync Pro
* How to Get an Internet Connection in the Middle of Nowhere to Hack Remotely

IBM Security Intelligence

* The Importance of Mobile Technology in State Electronic Visit Verification (EVV) Programs
* Triage Attacks More Efficiently With AI for Cybersecurity
* Space Cybersecurity: How Lessons Learned on Earth Apply in Orbit
* What You Need to Know About Scam Text Messages in 2021
* How is Enterprise Security Like Writing a Novel?
* TrickBot's Survival Instinct Prevails - What's Different About the TrickBoot Version?
* Credential Stuffing: AI's Role in Slaying a Hydra
* For Attackers, Home is Where the Hideout Is
* QR Code Security: What You Need to Know Today
* Managing Cybersecurity Costs: Bake These Ingredients Into Your Annual Budget

InfoWorld

* How to create PDF documents in ASP.NET Core 5
* The shifting market for PostgreSQL
* 6 ways to bring your spiraling cloud costs under control
* Angular adds error codes, debugging guides
* Patrick J. McGovern Foundation invests in AI for public good
* JFrog devops users freed from Docker Hub image-pull limits
* The new normal needs new cloud security
* Welcome to the client-serverless revolution
* How to handle errors in ReactJS
* Sentry for JavaScript monitors release health

C4ISRNET - Media for the Intelligence Age Military

* Solorigate attack - the challenge to cyber deterrence
* Pentagon could reassess future of JEDI cloud, depending on court action
* Hand-to-hand combat on computer networks: How cyber threat hunters work
* Army labs to host testing to connect joint war-fighting systems
* Latest version of cyber training to roll out in coming months
* The Space Force wants a more resilient architecture
* Getting away from 'anything goes': Military leaders set data standards for joint war fighting
* Elbit Systems UK to supply British Armed Forces target acquisition solution
* Air Force chief: Electromagnetic spectrum could be cheaper option to defeat enemies
* This is my Marine Corps robot, there are many like it but this one is mine

The Hacker Corner

Conferences

* 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
* Best Security Transport Conferences 2021 - 2022
* Best Social Engineering Conferences 2021 - 2022

Google Zero Day Project

* A Look at iMessage in iOS 14
* Windows Exploitation Tricks: Trapping Virtual Memory Access

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.

* DiceCTF 2021
* TrollCAT CTF 2021
* GunnHacks 7.0
* SecureBug CTF
* Tenable CTF 2021
* Union CTF 2021
* darkCON CTF
* Aero CTF 2021
* zer0pts CTF 2021
* UTCTF 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

* Sifter 11.5
* AIDE 0.17
* Logwatch 7.5.5
* OATH Toolkit 2.6.6
* Falco 0.27.0
* OpenStego Free Steganography Solution 0.8.0
* WhatWeb Scanner 0.5.5
* GNU Privacy Guard 2.2.27
* Flawfinder 2.0.15
* jSQL Injection 0.83

Kali Linux Tutorials

* 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
* ProtOSINT : Script Helps To Investigate Protonmail Accounts & ProtonVPN IP Addresses
* Sigurls : A Reconnaissance Tool & It Fetches URLs From AlienVault's OTX
* PongoOS : A Pre-Boot Execution Environment For Apple Boards
* Wprecon : A Vulnerability Recognition Tool In CMS WordPress
* Mud-Visualizer : A Tool To Visualize MUD Files
* Pidrila : Python Interactive Deepweb-Oriented Rapid Intelligent Link Analyzer

GBHackers Analysis

* 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
* WordPress Easy WP SMTP zero-day Vulnerability Exposes Hundreds of Thousands of Sites to Hack

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Episode 165: Collecting Machine Info on Mac - Part 2
* Ask Us (Almost) Anything About Threat Hunting & Incident Response | SANS THIR Summit 2020
* Episode 164: Collecting Machine Info on Mac - Part 1
* Herramientas rapidas DFIR para respuesta a incidentes y caza de amenazas Parte Deux

Defcon Conference

* 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
* Hacker History Project - The Dark Tangent Interviewed at DEF CON 5 - courtesy of ZDnet

Hak5

* Kindle E-Book Hack Discovered, DIA Collects Location Data (Without a Warrant!) - ThreatWire
* Touring Glytch's Hacker Van
* Ring Adds E2EE, Ubiquiti Suffers a Data Breach - ThreatWire

The PC Security Channel [TPSC]

* Best Browser Extensions for Security
* Bitdefender 2021 Review: Test vs Malware

Eli the Computer Guy

* APPLE BANS PROTEST APP - Vybe Together
* COVID RIOTS in the NETHERLANDS
* GIULIANI DEMONETIZED on YOUTUBE for WRONG SPEAK
* DOJ PROSECUTING ELECTION FRAUD on SOCIAL MEDIA ... from 2016

Security Now

* Comparative Smartphone Security - Browser Password Managers, Adobe Flash Repercussions, SolarWinds
* Where the Plaintext Is - 2021s First Patch Tuesday, Titan Security Key Side-Channel Attack, WhatsApp

Troy Hunt

* Weekly Update 228

Intel Techniques: The Privacy, Security, & OSINT Show

* 204-Radio Frequency Monitoring
* 203-Lessons in Redundancy

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Metasploit Framework 6.0.11 Command Injection
* Packed.Win32.Katusha.o Insecure Permissions
* Backdoor.Win32.MiniBlackLash Denial Of Service
* Online Voting System 1.0 Authorization Bypass
* BloofoxCMS 0.5.2.1 Cross Site Scripting
* Online Grading System 1.0 SQL Injection
* Backdoor.Win32.Mhtserv.b Missing Authentication
* Quick.CMS 6.7 Remote Code Execution
* Home Assistant Community Store 1.10.0 Path Traversal
* Backdoor.Win32.Zhangpo Denial Of Service
* Backdoor.Win32.Zetronic Denial Of Service
* MyBB Hide Thread Content 1.0 Information Disclosure
* PRTG Network Monitor Remote Code Execution
* Micro Focus UCMDB Remote Code Execution
* Chamilo LMS 1.11.14 Cross Site Scripting
* WordPress SuperForms 4.9 Shell Upload
* jQuery UI 1.12.1 Denial Of Service
* CMSUno 1.6.2 Remote Code Execution
* EgavilanMedia PHPCRUD 1.0 Cross Site Scripting
* Sudo Heap-Based Buffer Overflow
* STVS ProVision 5.9.10 Cross Site Request Forgery
* STVS ProVision 5.9.10 Cross Site Scripting
* STVS ProVision 5.9.10 File Disclosure
* Revive Adserver 5.1.0 Cross Site Scripting
* Constructor.Win32.SpyNet.a Remote Password Leak

CXSecurity

* PEAR Archive_Tar Arbitrary File Write
* Quick.CMS 6.7 Remote Code Execution
* Metasploit Framework 6.0.11 Command Injection
* PRTG Network Monitor Remote Code Execution
* SonicWall SSL-VPN 8.0.0.0 shellshock/visualdoor Remote Code Execution (Unauthenticated)
* Oracle WebLogic Server 14.1.1.0 Remote Code Execution
* ERPNext 12.14.0 SQL Injection (Authenticated)

Proof of Concept (PoC) & Exploits

Exploit Database

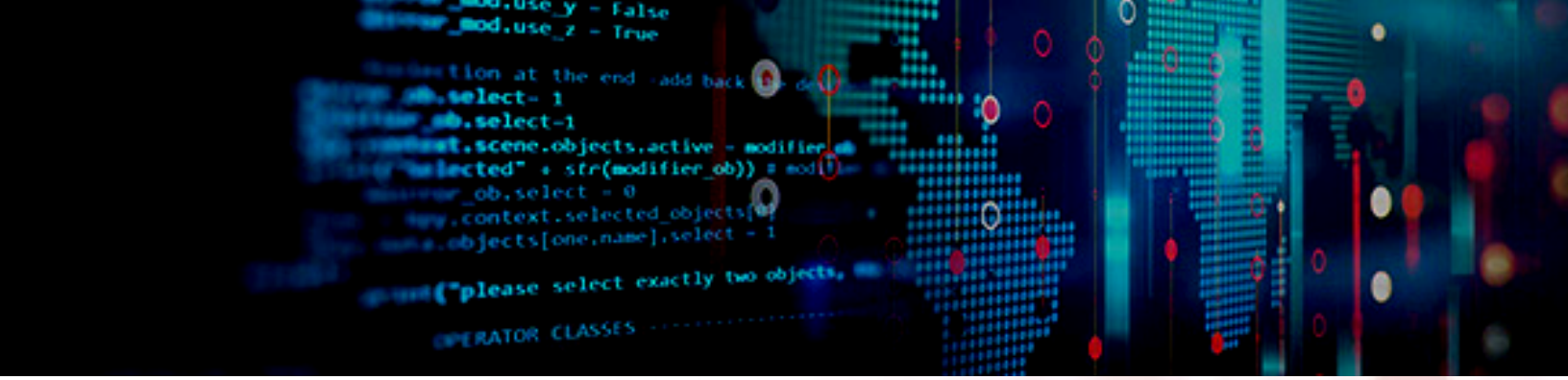
* [webapps] WordPress 5.0.0 - Image Remote Code Execution
* [webapps] Klog Server 2.4.1 - Command Injection (Authenticated)
* [webapps] Roundcube Webmail 1.2 - File Disclosure
* [webapps] Vehicle Parking Tracker System 1.0 - 'Owner Name' Stored Cross-Site Scripting
* [webapps] H8 SSRMS - 'id' IDOR
* [webapps] bloofoxCMS 0.5.2.1 - CSRF (Add user)
* [webapps] MyBB Thread Redirect Plugin 0.2.1 - Cross-Site Scripting
* [webapps] MyBB Trending Widget Plugin 1.2 - Cross-Site Scripting
* [webapps] Park Ticketing Management System 1.0 - 'viewid' SQL Injection
* [webapps] User Management System 1.0 - 'uid' SQL Injection
* [webapps] Zoo Management System 1.0 - 'anid' SQL Injection
* [webapps] MyBB Delete Account Plugin 1.4 - Cross-Site Scripting
* [webapps] SonicWall SSL-VPN 8.0.0.0 - 'shellshock/visualdoor' Remote Code Execution (Unauthenticated)
* [webapps] Simple Public Chat Room 1.0 - 'msg' Stored Cross-Site Scripting
* [webapps] Simple Public Chat Room 1.0 - Authentication Bypass SQLi
* [webapps] MyBB Hide Thread Content Plugin 1.0 - Information Disclosure
* [webapps] Home Assistant Community Store (HACS) 1.10.0 - Path Traversal to Account Takeover
* [webapps] Quick.CMS 6.7 - Remote Code Execution (Authenticated)
* [webapps] Online Grading System 1.0 - 'uname' SQL Injection
* [webapps] BloofoxCMS 0.5.2.1 - 'text' Stored Cross Site Scripting
* [local] Metasploit Framework 6.0.11 - msfvenom APK template command injection
* [webapps] WordPress Plugin SuperForms 4.9 - Arbitrary File Upload to Remote Code Execution
* [dos] jQuery UI 1.12.1 - Denial of Service (DoS)
* [webapps] Umbraco CMS 7.12.4 - Remote Code Execution (Authenticated)
* [webapps] Fuel CMS 1.4.1 - Remote Code Execution (2)

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*

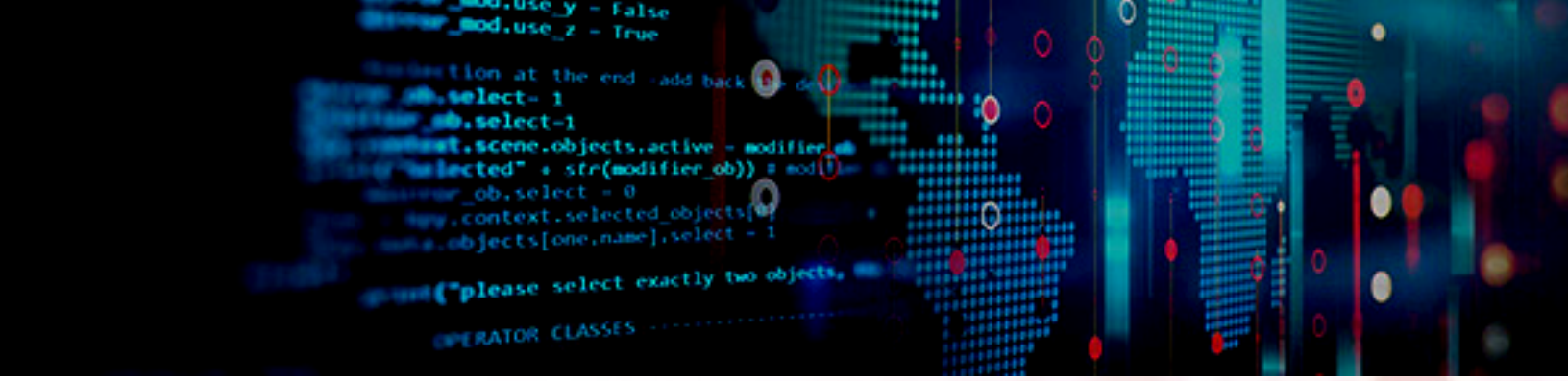
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://revistaciencias.inacipe.gob.mx/public/site/images/adminj/kingskrupellos.jpg
http://revistaciencias.inacipe.gob.mx/public/site/images/adminj/kingskrupellos.jpg notified by KingSkrupellos
https://static.investindia.gov.in/s3fs-public/2020-12/kingskrupellos.jpg
https://static.investindia.gov.in/s3fs-public/2020-12/kingskrupellos.jpg notified by KingSkrupellos
http://ogunstatejudiciary.gov.ng/images/fuck.txt
http://ogunstatejudiciary.gov.ng/images/fuck.txt notified by Imam
http://www.suwaree.go.th/hack3d.txt
http://www.suwaree.go.th/hack3d.txt notified by Imkey7
http://comunaaltodelosquebrachos.gob.ar/galau.htm
http://comunaaltodelosquebrachos.gob.ar/galau.htm notified by PYS404
http://municipalidaddesinsacate.gob.ar/galau.htm
http://municipalidaddesinsacate.gob.ar/galau.htm notified by PYS404
http://sinsacate.gob.ar/galau.htm
http://sinsacate.gob.ar/galau.htm notified by PYS404
http://municipalidadelbrete.gob.ar/galau.htm
http://municipalidadelbrete.gob.ar/galau.htm notified by PYS404
http://comunaguanacomuerto.gob.ar/galau.htm
http://comunaguanacomuerto.gob.ar/galau.htm notified by PYS404
https://dittop-tniad.mil.id
https://dittop-tniad.mil.id notified by ./Tikus_HaXoR
http://almafuerte.gov.ar
http://almafuerte.gov.ar notified by Cyb3r-3rr0r
http://pn-nganjuk.go.id/notFound.html
http://pn-nganjuk.go.id/notFound.html notified by 1K4lL_*
http://www.prachuap.go.th/vin.txt
http://www.prachuap.go.th/vin.txt notified by Imkey7
http://sorongkab.go.id/root.php
http://sorongkab.go.id/root.php notified by Black_X12
http://sipatola.padanglawasutarakab.go.id
http://sipatola.padanglawasutarakab.go.id notified by ONE HAT CYBER TEAM
https://www.cscu.go.ug/read.html
https://www.cscu.go.ug/read.html notified by Mr.Z
https://cedes.gob.mx/party.php
https://cedes.gob.mx/party.php notified by MR.Donut's



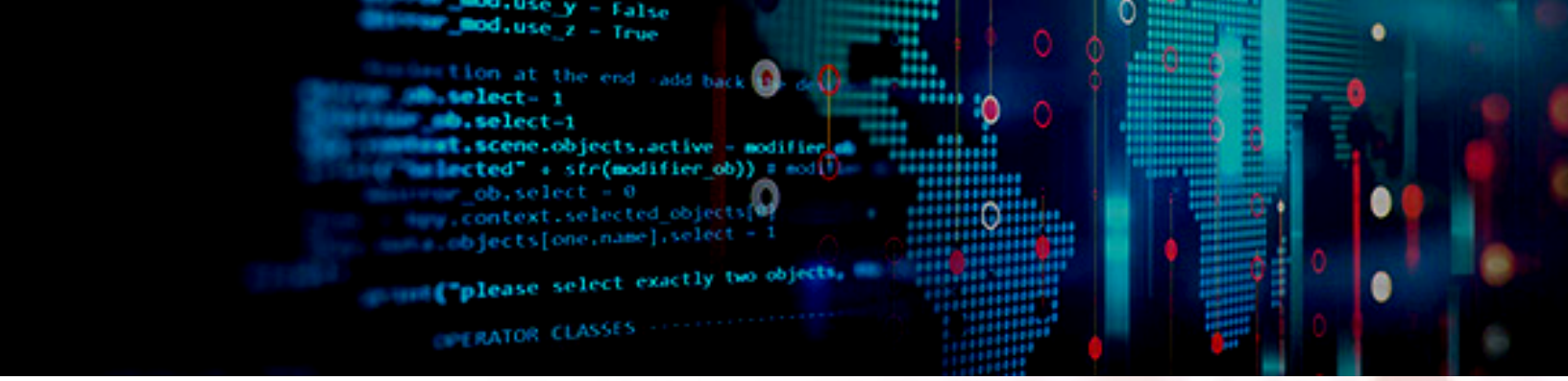
Dark Web News

Darknet Live

Here is How Easily the Feds Identified a Darkweb Opioid Dealer
Darkweb markets provide drug dealers with an anonymous platform to peddle their wares but that did not help the Empire Market vendor "chlnsaint." (via darknetlive.com)
Kentucky Man Sentenced for Selling Meth on the Darkweb
A counterfeit Adderall vendor from Kentucky was sentenced to 11 years in prison for drug trafficking and money laundering. (via darknetlive.com)
Netherlands Police Make Six Arrests in Dutchmasters Case
Law enforcement in the Netherlands arrested the alleged operators of the DutchMasters profile on the darkweb. (via darknetlive.com)
Prolific Marijuana Vendor Indicted in Germany
German authorities filed charges against the suspected operators of the vendor account "Lena'sBioLaden." (via darknetlive.com)

Dark Web Link

Darknet Fake ID Vendor "FakeIDDobby" Has Been Arrested In Germany
The German Federal Police has arrested a suspected trio for operating on various dark web marketplaces under the Fake ID vendor name "FakeIDDobby”. The Federal Police Inspection for Combating Crime in Halle (Saale) had stated in a press release that the suspects had sold German Fake ID documents and Fake ID cards for Italy, Austria, Poland, the Czech Republic and [...] The post Darknet Fake ID Vendor "FakeIDDobby” Has Been Arrested In Germany appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Hurtcore: Man Receives 15 Years Imprisonment Seeking Child Rape Photos
A man had posted an online picture of a male child being raped on a dark web hurtcore site and asked the viewers to send more pictures. In this child pornography case, the indicted man has been sentenced to mandatory 15 years behind bars followed by five years on the supervised release. He has also [...] The post Hurtcore: Man Receives 15 Years Imprisonment Seeking Child Rape Photos appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
NetWalker: Law Enforcement Shuts Down The Dark Web Website
The darknet leaks websites associated with the operations conducted by the NetWalker ransomware group have been taken down by the law enforcement agencies from Bulgaria and the USA. The agencies were successful in the global dismantlement of hundreds of servers and one million Emotet infections. They have also charged a suspect. NetWalker (Emotet) is a [...] The post NetWalker: Law Enforcement Shuts Down The Dark Web Website appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

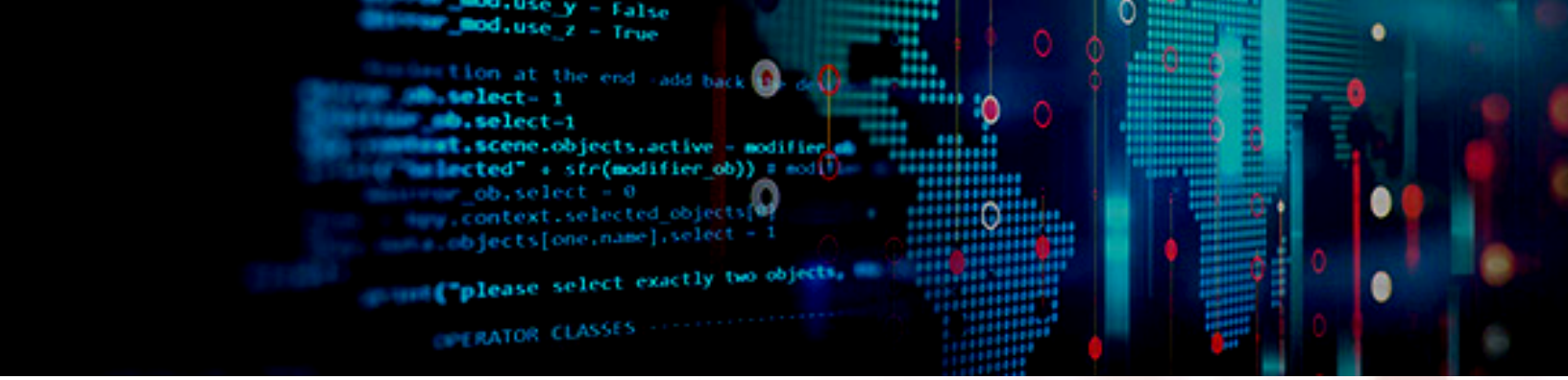
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing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

* LogoKit: Simple, Effective, and Deceptive
* Attacks on the Capitol Showed the Pitfalls of Having a Narrow View of the Internet
* New Analysis Puts Magecart Interconnectivity into Focus
* RiskIQ's New JARM Feature Supercharges Incident Response
* Skimming a Little Off the Top: 'Meyhod' Skimmer Hits Hair Loss Specialists
* SolarWinds Orion Hack: Know if You're Affected and Defend Your Attack Surface
* Implement FireEye's List of CVEs and Detections with RiskIQ Attack Surface Intelligence
* 'Shadow Academy' Targets 20 Universities Worldwide
* How Do Consumers View Spending and Safety for Online Shopping this Holiday Season? We Took a Look.
* A New Grelos Skimmer Reflects the Depth and Murkiness of the Magecart Ecosystem

FireEye

* Metasploit Wrap-Up
* NICER Protocol Deep Dive: Internet Exposure of HTTP and HTTPS
* Upcoming Rapid7 Webcast: How Far Does Your VRM Strategy Go?
* State-Sponsored Threat Actors Target Security Researchers
* Finding Results at the Intersection of Security and Engineering
* Metasploit Wrap-Up
* NICER Protocol Deep Dive: Internet Exposure of NTP
* Principles for personal information security legislation
* You Can Now Buy (And Renew) Five More Rapid7 Products Through AWS Marketplace
* InsightIDR: 2020 Highlights and What's Ahead in 2021



Advisories

US-Cert Alerts & bulletins

* Data Privacy Day
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* Apple Releases Security Updates
* CISA Malware Analysis on Supernova
* FTC Reports Scammers Impersonating FTC
* Cisco Releases Advisories for Multiple Products
* Drupal Releases Security Updates
* CERT/CC and CISA Report Multiple Vulnerabilities in Dnsmasq
* AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
* AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and
* Vulnerability Summary for the Week of January 18, 2021
* Vulnerability Summary for the Week of January 11, 2021

Zero Day Initiative Advisories

ZDI-CAN-12703: 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 'AIOFuzzer' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12792: Microsoft
A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'JeongOh Kyea (@kkokkokye) of THEORI' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12795: 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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12740: 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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12954: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is

given until 2021-05-29 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-12878: 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 ' Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12952: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12928: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12886: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12884: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12927: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12930: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12880: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12926: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12887: 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 'Mat Powell of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12879: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12932: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12885: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-11832: 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 'Selim Enes Karaduman (@Enesdex)' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12889: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12951: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12864: 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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12953: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-12931: Autodesk

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: 2021-01-29, 3 days ago. The vendor is given until 2021-05-29 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-4714-1

Ubuntu Security Notice 4714-1 - Zhihong Tian and Hui Lu found that XStream was vulnerable to remote code execution. A remote attacker could run arbitrary shell commands by manipulating the processed input stream. It was discovered that XStream was vulnerable to server-side forgery attacks. A remote attacker could request data from internal resources that are not publicly available only by manipulating the processed input stream. Various other issues were also addressed.

Red Hat Security Advisory 2021-0299-01

Red Hat Security Advisory 2021-0299-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.7.0. Issues addressed include an information leakage vulnerability.

Gentoo Linux Security Advisory 202101-37

Gentoo Linux Security Advisory 202101-37 - A buffer overflow in VLC might allow remote attacker(s) to execute arbitrary code. Versions less than 3.0.12.1 are affected.

Gentoo Linux Security Advisory 202101-36

Gentoo Linux Security Advisory 202101-36 - A vulnerability in ImageMagick's handling of PDF was discovered possibly allowing code execution. Versions less than 6.9.11.41-r1 are affected.

Red Hat Security Advisory 2021-0298-01

Red Hat Security Advisory 2021-0298-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.7.0. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-0297-01

Red Hat Security Advisory 2021-0297-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.7.0. Issues addressed include an information leakage vulnerability.

Glibc Character Conversion Assertion

If an application uses iconv() with an attacker specified character set, there's an assertion in the gconv buffer management code that can be triggered, crashing the application. The crash only occurs with ISO-2022-JP-3 encoding.

Ubuntu Security Notice USN-4706-1

Ubuntu Security Notice 4706-1 - Olle Segerdahl found that ceph-mon and ceph-mgr daemons did not properly restrict access, resulting in gaining access to unauthorized resources. An authenticated user could use this vulnerability to modify the configuration and possibly conduct further attacks. Adam Mohammed found that Ceph Object Gateway was vulnerable to HTTP header injection via a CORS ExposeHeader tag. An attacker could use this to gain access or cause a crash. Various other issues were also addressed.

Ubuntu Security Notice USN-4707-1

Ubuntu Security Notice 4707-1 - It was discovered that TCMU lacked a check for transport-layer restrictions, allowing remote attackers to read or write files via directory traversal in an XCOPY request.

Ubuntu Security Notice USN-4712-1

Ubuntu Security Notice 4712-1 - USN-4576-1 fixed a vulnerability in the overlay file system implementation in the Linux kernel. Unfortunately, that fix introduced a regression that could incorrectly deny access to overlay files in some situations. This update fixes the problem.

Ubuntu Security Notice USN-4713-1

Ubuntu Security Notice 4713-1 - It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

Ubuntu Security Notice USN-4711-1

Ubuntu Security Notice 4711-1 - It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data. Kiyin discovered that the perf subsystem in the Linux kernel did not properly deallocate memory in some situations. A privileged attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4710-1

Ubuntu Security Notice 4710-1 - Kiyin discovered that the perf subsystem in the Linux kernel did not properly deallocate memory in some situations. A privileged attacker could use this to cause a denial of service.

Red Hat Security Advisory 2021-0290-01

Red Hat Security Advisory 2021-0290-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.7.0 ESR. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-0289-01

Red Hat Security Advisory 2021-0289-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.7.0 ESR. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-0288-01

Red Hat Security Advisory 2021-0288-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.7.0 ESR. Issues addressed include an information leakage vulnerability.

Gentoo Linux Security Advisory 202101-35

Gentoo Linux Security Advisory 202101-35 - Multiple vulnerabilities have been found in phpMyAdmin, allowing remote attackers to conduct XSS. Versions less than 4.9.6:4.9.6 are affected.

Gentoo Linux Security Advisory 202101-34

Gentoo Linux Security Advisory 202101-34 - Multiple vulnerabilities have been found in Telegram, the worst of which could result in information disclosure. Versions less than 2.4.4 are affected.

Ubuntu Security Notice USN-4709-1

Ubuntu Security Notice 4709-1 - It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data. Wen Xu discovered that the XFS filesystem implementation in the Linux kernel did not properly track inode validations. An attacker could use this to construct a malicious XFS image that, when mounted, could cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4708-1

Ubuntu Security Notice 4708-1 - Wen Xu discovered that the XFS filesystem implementation in the Linux kernel did not properly track inode validations. An attacker could use this to construct a malicious XFS image that, when mounted, could cause a denial of service. It was discovered that the btrfs file system implementation in the Linux kernel did not properly validate file system metadata in some situations. An attacker could use this to construct a malicious btrfs image that, when mounted, could cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-0285-01

Red Hat Security Advisory 2021-0285-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 78.7.0 ESR. Issues addressed include an information leakage vulnerability.

Ubuntu Security Notice USN-4705-2

Ubuntu Security Notice 4705-2 - USN-4705-1 fixed a vulnerability in Sudo. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. It was discovered that Sudo incorrectly handled memory when parsing command lines. A local attacker could possibly use this issue to obtain unintended access to the administrator account. Various other issues were also addressed.

Gentoo Linux Security Advisory 202101-33

Gentoo Linux Security Advisory 202101-33 - Multiple vulnerabilities have been found in sudo, the worst of which could result in privilege escalation. Versions less than 1.9.5_p2 are affected.

Gentoo Linux Security Advisory 202101-32

Gentoo Linux Security Advisory 202101-32 - A weakness was discovered in Mutt and NeoMutt's TLS

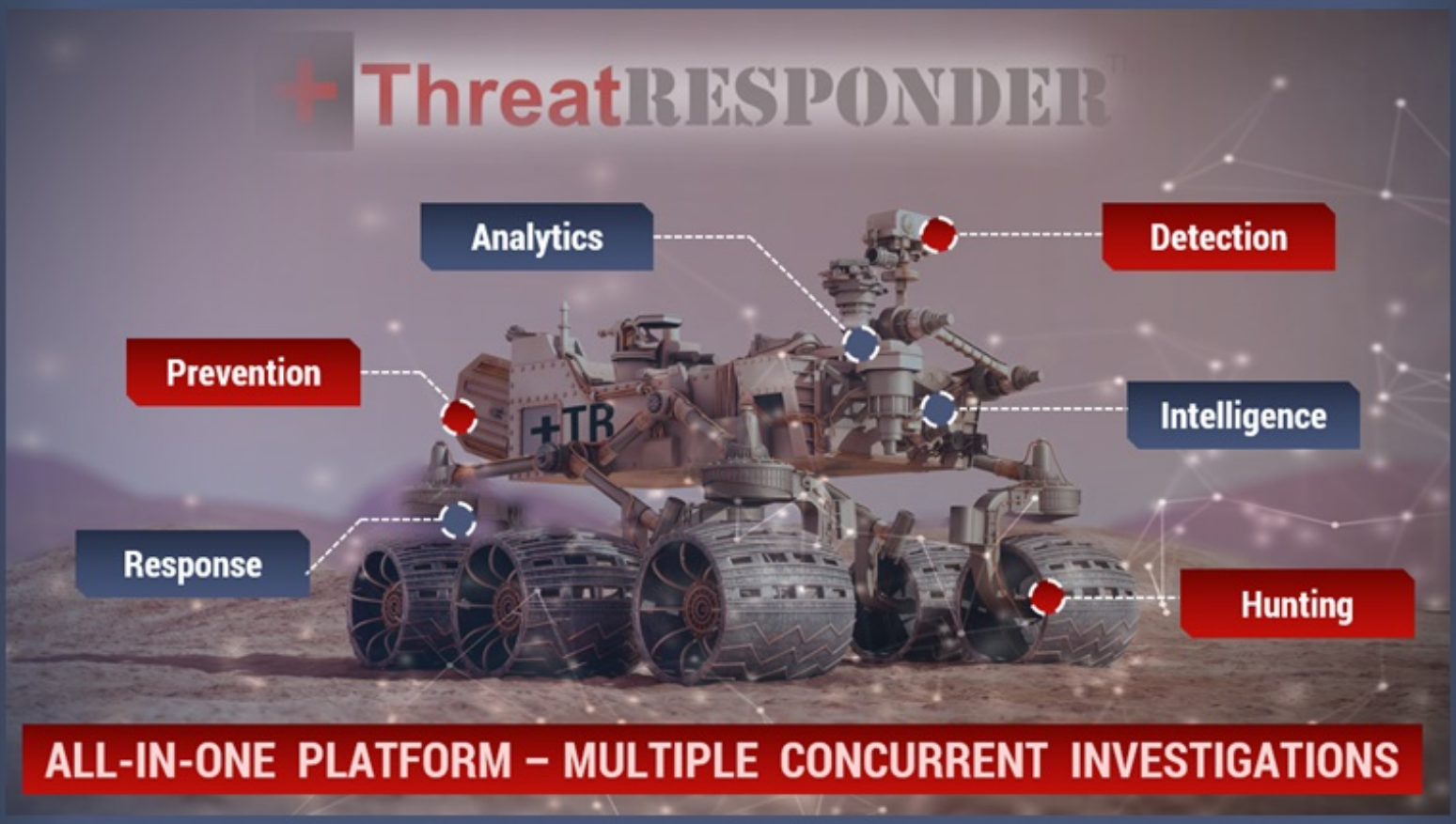
handshake handling. Versions less than 2.0.2 are affected.

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



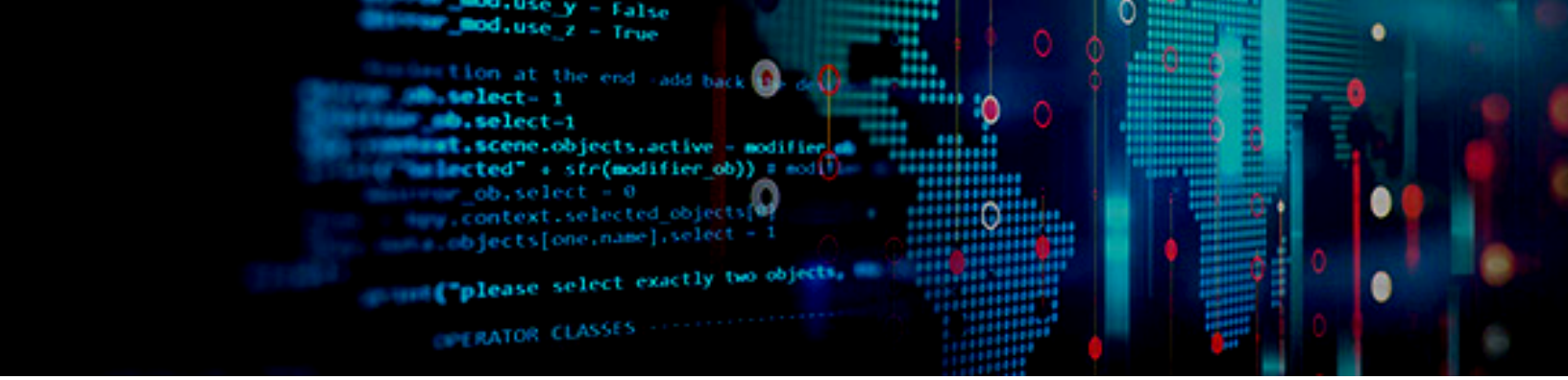
The Solution – ThreatResponder® Platform

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

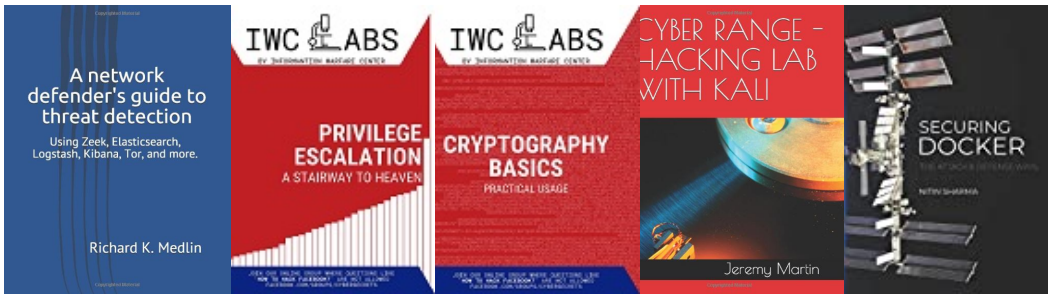


The Cyber Secrets publications on Amazon

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