Mar-08-21

CYBER WEEKLY AWARENESS REPORT

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

netSecurity®

INFORMATION WARFARE CENTER

Si LINUX

ARGOS APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

March 8, 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

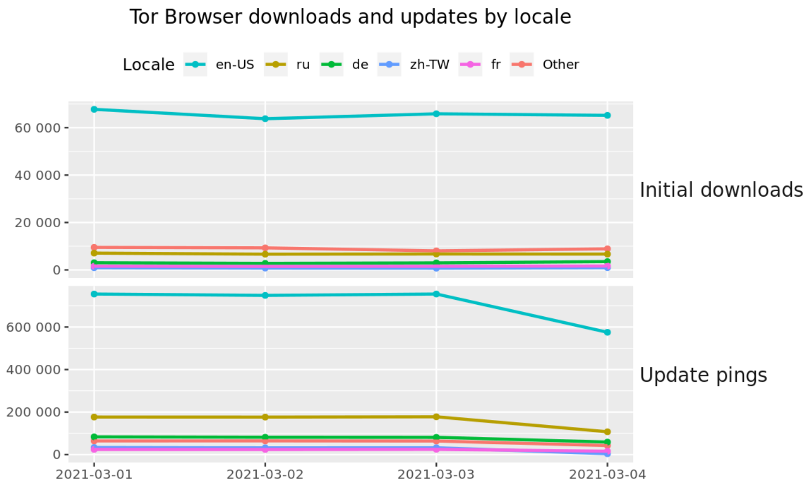
Internet Storm Center Infocon Status

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.



The Tor Project - https://metrics.torproject.org/

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.

* CSI Linux has a tools update. You can update the tools in a terminal by typing
wget csilinux.com/downloads/csitoolsupdate.sh -O - | sh

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

Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* Supernova Malware Links Chinese Group To SolarWinds Hack
* Ten Of Thousands Of Orgs Hit In Ongoing Exchange Hack
* Intel, DoD Start Sprint To Make Homomorphic Encryption Ready For Real
* European Banking Authority Hit By Microsoft Exchange Hack
* FTC Joins 38 States Taking Down Massive Charity Robocall Operation
* Malicious Code Bombs Target Amazon, Lyft, Slack, Zillow
* Biden Administration Labels China Top Tech Threat, Promises Proportionate Responses To Cyberattacks
* NSA, CISA, Issue Guidance On Protective DNS Services
* Accellion Zero Day Claims A New Victim In Qualys
* Microsoft Exchange Zero-Day Attackers Spy On U.S. Targets
* Researcher Finds 5 Privilege Escalation Vulns In Linux Kernel
* Maza Russian Cybercriminal Forum Suffers Data Breach
* Ursnif Trojan Has Targeted Over 100 Italian Banks
* Google Says They Won't Use Other Web Tracking Tools After Phasing Out Cookies
* Microsoft Accuses China Over Email Cyber-Attacks
* MS Account Hijacking Vuln Earns Bug Bounty Hunter $50,000
* Malaysia Airlines Security Incident Spanned 9 Years
* Trump's Is One Of 15,000 Gab Accounts That Just Got Hacked
* Flaws Fixed Incorrectly, As Secure Coding Education Lags
* Oxfam Australia Supporters Embroiled In New Data Breach
* Hackers Improve SEO Before Deploying Malware
* Spyware Fan MBS Accused By US Intel Of Khashoggi Death
* Clubhouse's Security And Privacy Lag Behind Its Quick Growth
* Judge Approves $650 Million Settlement Of Privacy Lawsuit Against Facebook
* Go Malware Is Now Common, Having Been Adopted By Both APT And E-Crime Groups

Krebs on Security

LATEST NEWS

Dark Reading

* Why Data Privacy Should Be on President Biden's Agenda for His First 100 Days
* Microsoft Exchange Server Exploits Hit Retail, Government, Education
* Microsoft Adopted an 'Aggressive' Strategy for Sharing SolarWinds Attack Intel
* 5 Ways Social Engineers Crack Into Human Beings
* Realistic Patch Management Tips, Post-SolarWinds
* On International Women's Day 2021, Does the 'Rule of Steve' Still Apply? Yes.
* Encrypted Traffic Strategies
* Make Sure That Stimulus Check Lands in the Right Bank Account
* Business Apps Spoofed in 45% of Impersonation Attacks
* Healthcare Still Seeing High Level of Attacker Activity
* Microsoft, FireEye Uncover More Malware Used in the SolarWinds Campaign
* John McAfee Charged in 'Pump & Dump' Cryptocurrency Scheme
* Secure Laptops & the Enterprise of the Future
* New Social Security Scam Spoofs Government Badges
* Qualys Is the Latest Victim of Accellion Data Breach
* Why We Need More Blue Team Voices at the Table
* Intel: More Than 90% of Our Vulnerabilities Found via Research
* More Details Emerge on the Microsoft Exchange Server Attacks
* Okta to Buy Rival Auth0
* CISA to Federal Agencies: Immediately Patch or 'Disconnect' Microsoft Exchange Servers

The Hacker News

* Iranian Hackers Using Remote Utilities Software to Spy On Its Targets
* Malware Can Exploit New Flaw in Intel CPUs to Launch Side-Channel Attacks
* Microsoft Exchange Cyber Attack - What Do We Know So Far?
* Bug in Apple's Find My Feature Could've Exposed Users' Location Histories
* Google Cloud Certifications - Get Prep Courses and Practice Tests at 95% Discount
* Mazafaka - Elite Hacking and Cybercrime Forum - Got Hacked!
* Researchers Find 3 New Malware Strains Used by SolarWinds Hackers
* Google Will Use 'FLoC' for Ad Targeting Once 3rd-Party Cookies Are Dead
* Extortion Gang Breaches Cybersecurity Firm Qualys Using Accellion Exploit
* CISA Issues Emergency Directive on In-the-Wild Microsoft Exchange Flaws
* Hackers Now Hiding ObliqueRAT Payload in Images to Evade Detection
* Replacing EDR/NGAV with Autonomous XDR Makes a Big Difference for Small Security Teams
* A $50,000 Bug Could've Allowed Hackers Access Any Microsoft Account
* URGENT - 4 Actively Exploited 0-Day Flaws Found in Microsoft Exchange
* New Chrome 0-day Bug Under Active Attacks - Update Your Browser ASAP!

LATEST NEWS

Security Week

* FINRA Warns of Ongoing Phishing Attacks Targeting Brokerage Firms
* Idaho Man Charged With Hacking Into Computers in Georgia
* Disruptions at Pan-American Life Likely Caused by Ransomware Attack
* Ukrainians Extradited to U.S. for Providing Money Laundering Services to Cybercriminals
* EU Banking Regulator Hit by Microsoft Email Hack
* Cybersecurity M&A Roundup for Week of Mar. 1, 2021
* Casting a Wide Intrusion Net: Dozens Burned With Single Hack
* F1 Team Williams Unveils New Car After Hackers Foil Launch
* Microsoft Shares Additional Mitigations for Exchange Server Vulnerabilities Under Attack
* Software Icon McAfee Charged in Cryptocurrency Scam
* Thousands of Mobile Apps Expose Data via Misconfigured Cloud Containers
* Ransomware Takedowns Underscore Need for Private-Public Cybersecurity Collaboration
* Multiple Airlines Impacted by Data Breach at Aviation IT Firm SITA
* NSA, DHS Issue Guidance on Protective DNS
* Report: Russian Hackers Exploit Lithuanian Infrastructure
* Supermicro, Pulse Secure Respond to Trickbot's Ability to Target Firmware
* Three New Malware Strains Linked to SolarWinds Hackers
* South Africa Opposes WhatsApp-Facebook Data Sharing
* Someone Is Hacking Cybercrime Forums and Leaking User Data
* Privilege Escalation Bugs Patched in Linux Kernel

Infosecurity Magazine

* McAfee Agrees Deal to Sell Enterprise Business for $4bn
* McAfee Faces Decades Behind Bars After Fraud Indictment
* FTC Busts $110m Charity Fraud Operation
* #IWD2021: Pandemic Fails to Shatter Glass Ceiling for Women in Cyber
* Hackers Target Russian Cybercrime Forums
* US Warns of Fake Unemployment Benefit Websites
* Failure to Report Breach Costs Mortgage Lender $1.5m
* Docker Hub and Bitbucket Resources Hijacked for Crypto-Mining
* Fraudsters Circumvent 3D Secure with Social Engineering
* SITA Supply Chain Breach Hits Multiple Airlines
* Cryptocurrency Fraudster Steals $16m
* Two-Thirds of Irish Women Harassed Online

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* CyberheistNews Vol 11 #10 [Heads Up] The Bad Guys Now Likely Own Your Exchange OWA Server
* The Different Scenarios How Backups are Vulnerable to Ransomware Attacks
* WSJ: Russian Disinformation Campaign Aims to Undermine Confidence in Covid-19 Vaccines
* [Heads Up] The Chinese Have Likely Hacked Your Exchange Email Server
* Think Your Cyber Insurance is Going to Cover that $6 Million in Cyber Fraud? Think Again.
* 1 in 4 Business Email Compromise Attacks Use Lookalike Domains to Trick Victims
* Phishing Attacks Continue to Impersonate Trusted Brands to Deceive Potential Victims
* Vendor Email Compromise is Officially A Big (Seven-Figure) Problem
* Phishing Scammers Send a Fake "Private Shared Document" as the Initial Attack Vector for Stealing Lin
* Someone Hacked The Four Top Russian Cybercrime Forums In One Month

ISC2.org Blog

* Celebrating Women in Cybersecurity and Committing to Diversity, Equity and Inclusion
* CISSPs from Around the Globe: An Interview with Chris Clinton
* What Are the Best Free Cybersecurity Webinars?
* What Are the Phases of an Incident Response Plan?
* THE HEALTHCARE INTERNET OF THINGS - FOR BETTER OR WORSE

HackRead

* John McAfee Charged with Fraud in Cryptocurrency Scam
* U.S. DOJ warns of fake unemployment benefit websites stealing data
* Microsoft, FireEye report 3 new malware linked to SolarWinds hackers
* Threat actors hijacking Bitbucket and Docker Hub for Monero mining
* Top Russian hacker forums Maza, Verified hacked; data leaked online
* IT Security firm Qualys extorted by Clop gang after data breach
* Marketing firm CallX exposed customers data including call recordings

Koddos

* John McAfee Charged with Fraud in Cryptocurrency Scam
* U.S. DOJ warns of fake unemployment benefit websites stealing data
* Microsoft, FireEye report 3 new malware linked to SolarWinds hackers
* Threat actors hijacking Bitbucket and Docker Hub for Monero mining
* Top Russian hacker forums Maza, Verified hacked; data leaked online
* IT Security firm Qualys extorted by Clop gang after data breach
* Marketing firm CallX exposed customers data including call recordings

LATEST NEWS

Naked Security

* Naked Security Live - ICU: How much do your home-working photos give away?
* Poison packages - "Supply Chain Risks" user hits Python community with 4000 fake modules
* Using TikTok? Check out these six security tips
* S3 Ep22: Cryptographic escapes and social media scams [Podcast]
* Another Chrome zero-day exploit - so get that update done!
* How (NOT?!) to jailbreak your iPhone
* I see you: your home-working photos reveal more than you think!
* Search crimes - how the Gootkit gang poisons Google searches
* Naked Security Live - Beware copyright scams
* S3 Ep21: Cryptomining clampdown, the 100-ton man, and ScamClub ads [Podcast]

Threat Post

* U.S. DoD Weapons Programs Lack 'Key' Cybersecurity Measures
* WordPress Injection Anchors Widespread Malware Campaign
* Massive Supply-Chain Cyberattack Breaches Several Airlines
* Critics Blast Google's Aim to Replace Browser Cookie with 'FLoC'
* D-Link, IoT Devices Under Attack By Tor-Based Gafgyt Variant
* Microsoft, FireEye Unmask More Malware Linked to SolarWinds Attackers
* Cyberattackers Target Top Russian Cybercrime Forums
* National Surveillance Camera Rollout Roils Privacy Activists
* CISA Orders Federal Agencies to Patch Exchange Servers
* COVID-19 Vaccine Spear-Phishing Attacks Jump 26 Percent

Null-Byte

* Master the Internet of Things with This Certification Bundle
* There Are Hidden Wi-Fi Networks All Around You - These Attacks Will Find Them
* Rank Up in Google Searches with This SEO Couse Bundle
* How to Generate Crackable Wi-Fi Handshakes with an ESP8266-Based Test Network
* This Master Course Bundle on Coding Is Just $34.99
* How to Automate Remote SSH Control of Computers with Expect Scripts
* 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)

LATEST NEWS

IBM Security Intelligence

* Innovation Through Diverse Thinking: Amplifying Gender Diversity and Shrinking the Skills Gap
* Cloud Native Tools Series Part 2: Understand Your Responsibilities
* Cloud Clarity: Adding Security and Control to the AWS Shared Responsibility Model
* How Enterprise Design Thinking Can Improve Data Security Solutions
* The Shift to E-Commerce: How Retail Cybersecurity is Changing
* Don't Speed Past Better Cloud App Security
* A More Effective Approach to Combating Software Supply Chain Attacks
* Cybersecurity Trends and Emerging Threats in 2021
* 'Clear and Present Danger': Why Cybersecurity Risk Management Needs to Keep Evolving
* Cybersecurity Gaps and Opportunities in the Logistics Industry

InfoWorld

* Devops salaries continued to rise during the pandemic
* Career roadmap: Database Administrator
* You can't escape Pulumi and other IaC tools
* Visual Studio Code 1.54 runs on Apple Silicon
* How to work with read-only collections in C#
* 6 security risks in software development and how to address them
* Cybersecurity in 2021: Stopping the madness
* Visual Studio 2019 16.9 brings memory error detection, C++ capabilities
* Multicloud architecture decomposition simplified
* What is an internal developer platform? PaaS done your way

C4ISRNET - Media for the Intelligence Age Military

* Mind meld: Synthetic training brought to life
* More work needed to integrate cyber and information ops, former official says
* A 'splinternet' won't solve global cyber defense problems
* Exclusive: Navy transfers network authorities to Project Overmatch office
* Pentagon struggles to add cybersecurity to weapon contracts, watchdog finds
* Space Force launches experimental research payload
* Webcast: What's Next for Army PNT
* Space Force chief says he's working on a declassification strategy, but offers scant details
* Defense Intelligence Agency awards IT services contract worth up to $12.6 billion
* 8 ideas for successful technology convergence

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

* D&eacute;j&agrave; 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.

* White-Hats Break the Syntax CTF
* DaVinciCTF 2021
* NahamCon CTF 2021
* UTCTF 2021
* vishwaCTF 2021
* BCA CTF 2021
* BlueHens CTF 2021
* LINE CTF 2021
* PoseidonCTF 2nd Edition **cancelled**
* SPRUSH CTF Quals 2021

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

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

Tools & Techniques

Packet Storm Security Tools Links

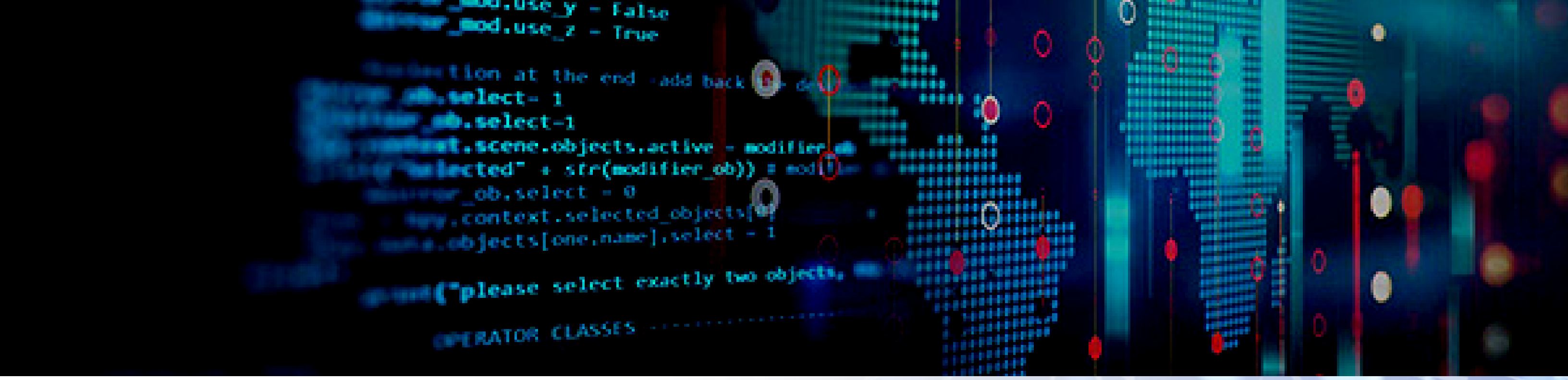
* Raptor WAF 0.62
* SQLMAP - Automatic SQL Injection Tool 1.5.3
* OpenSSH 8.5p1
* Zeek 4.0.0
* Suricata IDPE 6.0.2
* American Fuzzy Lop plus plus 3.10c
* Faraday 3.14.2
* Global Socket 1.4.25
* jSQL Injection 0.84
* Zeek 3.2.4

Kali Linux Tutorials

* Teatime : A Blockchain RPC Attack Framework
* Fake SMS : Skip Phone Verification By Using A Proxy
* WdToggle : Direct System Calls To Enable WDigest Credential Caching
* Gatekeeper : First Open-Source DDoS Protection System
* Horusec : An Open Source Tool That Improves Identification Of Vulnerabilities
* OpenWifiPass : An Open Source Implementation Of Apple's Wi-Fi Password
* GitLab Watchman : Monitoring GitLab For Sensitive Data Shared Publicly
* Understanding the Desktop as a Service Model
* OSV : Open Source Vulnerabilities
* UDdup : Urls De-Duplication Tool For Better Recon

GBHackers Analysis

* Linux Kernel Vulnerability that Allows Local Attackers to Escalate Privileges
* Microsoft Issues Emergency Patch as Chinese Hackers Exploiting Exchange Server Flaws
* Researchers Find a Way to Learn What Users Type in Video Calling
* New PDF Vulnerability Let Attackers Bypass the Signature Validation in PDF and Replace Content
* Unpatched SHAREit Flaw Let Attackers Execute Remote Code


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
"Selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Weekly Cyber Security Video and Podcasts

SANS DFIR

* [Episode 181: When Forensicators Screw Up - Part 1]
* [Cyber-Espionage: Out of the shadows. Into the digital crosshairs | John Grim | SANS CTI Summit 2021]
* [xStart When You're Ready | John Southworth | SANS CTI Summit 2021]
* [Episode 180: Introducing FOR498A Forensic Data Acquisition]

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

* [LastPass Tracks Android Users - ThreatWire]
* [Apple M1 Malware Found, Brave Browser Leaked DNS Queries - ThreatWire]
* [Phishing Using Morse Code, Signal Responds to Iran Ban, Chrome Zero Day News - ThreatWire]

The PC Security Channel [TPSC]

* [Cyberpunk's Company Hacked by HelloKitty Ransomware: Live Demo]
* [Windows Defender vs Ransomware in 2021]

Eli the Computer Guy

* [LINKEDIN ADMITS IDFA TRACKING ISN'T VALUABLE]
* [GOOGLE KILLS THIRD PARTY TRACKING]
* [BEST BUY LAYOFFS - 5000 Jobs Cut as Business IMPROVES]
* [MS EXCHANGE SERVERS HACKED by Nation States]

Security Now

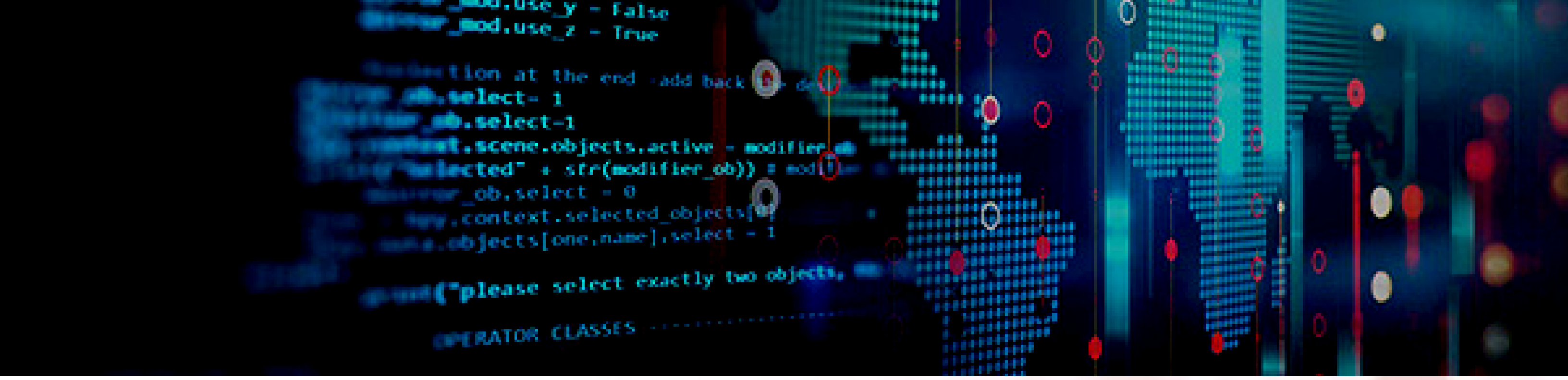
* [CNAME Collusion - Seven Exchange 0-Days, Firefox Enhanced Tracking Protection, SolarWinds Password]
* [Dependency Confusion - SHAREit's Security Update, Solorigate, Brave's "Private Window With Tor"]

Troy Hunt

* [Weekly Update 233]

Intel Techniques: The Privacy, Security, & OSINT Show

* [209-New OSINT Tactics]
* [208-Amazon Privacy & VOIP Updates]



Trend Micro Anti-Malware Blog

* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

RiskIQ

* Turkey Dog Continues to Target Turkish Speakers with RAT Trojans via COVID Lures
* Threat Hunting in a Post-WHOIS World
* The Business of LogoKit: The Actors and Marketing Behind a Popular Phishing Tool
* 2020 Mobile App Threat Landscape: New Threats Arise, But the Ecosystem Got Safer
* LogoKit: Simple, Effective, and Deceptive
* 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

FireEye

* Metasploit Wrap-Up
* Mass Exploitation of Exchange Server Zero-Day CVEs: What You Need to Know
* IAM Never Gonna Give You Up, Never Gonna Breach Your Cloud
* Rapid7's InsightIDR Enables Detection And Response to Microsoft Exchange Zero-Day
* How to Achieve and Maintain Continuous Cloud Compliance
* Metasploit Wrap-Up
* Celebrating Black History Today and Every Day
* Building a Holistic VRM Strategy That Includes the Web Application Layer
* Multiple Unauthenticated Remote Code Control and Execution Vulnerabilities in Multiple Cisco Products
* VMware vCenter Server CVE-2021-21972 Remote Code Execution Vulnerability: What You Need to Know

Proof of Concept (PoC) & Exploits

Packet Storm Security

* VMware vCenter Server File Upload / Remote Code Execution
* WordPress SuperStoreFinder / SuperInteractiveMaps 6.3 SQL Injection
* Hotel And Lodge Management System 1.0 Shell Upload
* Backdoor.Win32.Agent.bjev Insecure Permissions
* Joomla JCK Editor 6.4.4 SQL Injection
* Joomla Matukio Events 7.0.5 Cross Site Scripting
* GLPI 9.5.3 Unsafe Reflection
* Backdoor.Win32.GTbot.c Insecure Permissions
* Backdoor.Win32.Antilam.14.o Code Execution
* Print Job Accounting 4.4.10 Unquoted Service Path
* Configuration Tool 1.6.53 Unquoted Service Path
* Pingzapper 2.3.1 Unquoted Service Path
* Microsoft Windows RRAS Service MIBEntryGet Overflow
* Fluig 1.7.0 Path Traversal
* CatDV 9.2 Authentication Bypass
* Doctor Appointment System 1.0 Cross Site Scripting
* Textpattern CMS 4.8.3 Remote Code Execution
* Textpattern CMS 4.9.0-dev Cross Site Scripting
* Textpattern CMS 4.8.4 Cross Site Scripting
* Online Ordering System 1.0 SQL Injection
* Online Ordering System 1.0 Shell Upload
* Web Based Quiz System 1.0 SQL Injection
* e107 CMS 2.3.0 Cross Site Request Forgery
* Doctor Appointment System 1.0 Blind SQL Injection
* Doctor Appointment System 1.0 SQL Injection

CXSecurity

* AnyDesk 5.5.2 Remote Code Execution
* TinyTinyRSS Remote Code Execution
* Zen Cart 1.5.7b Remote Code Execution (Authenticated)
* Covid-19 Contact Tracing System 1.0 Code Execution
* VMware vCenter Server 7.0 Unauthenticated File Upload
* Unified Remote 3.9.0.2463 Remote Code Execution
* SLMail 5.1.0.4420 Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

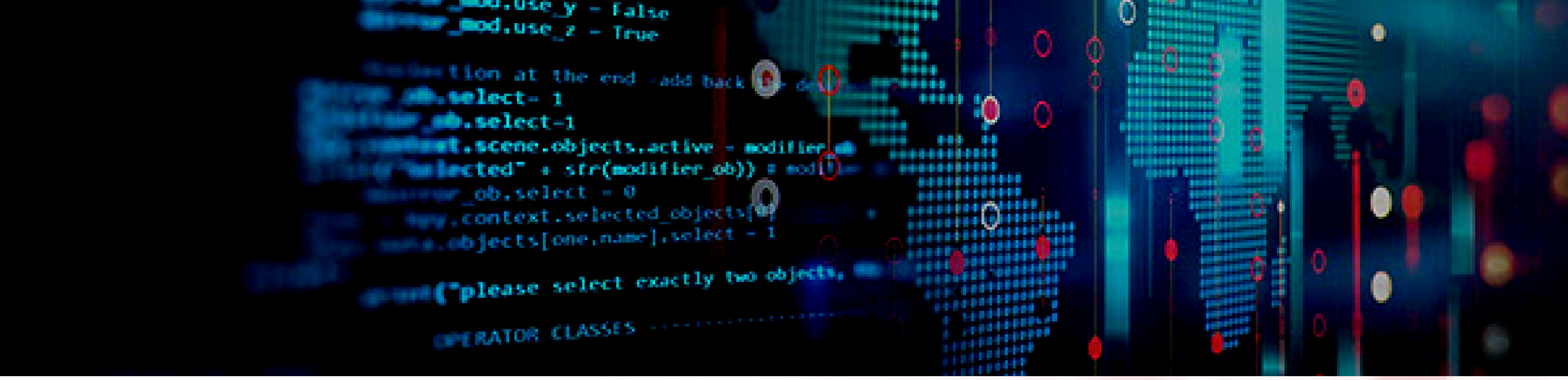
* [webapps] GLPI 9.5.3 - 'fromtype' Unsafe Reflection
* [webapps] Joomla JCK Editor 6.4.4 - 'parent' SQL Injection (2)
* [local] Pingzapper 2.3.1 - 'PingzapperSvc' Unquoted Service Path
* [webapps] Hotel and Lodge Management System 1.0 - Remote Code Execution (Unauthenticated)
* [local] Configuration Tool 1.6.53 - 'OpLclSrv' Unquoted Service Path
* [local] Print Job Accounting 4.4.10 - 'OkiJaSvc' Unquoted Service Path
* [webapps] Fluig 1.7.0 - Path Traversal
* [remote] CatDV 9.2 - RMI Authentication Bypass
* [webapps] Textpattern 4.8.3 - Remote code execution (Authenticated) (2)
* [webapps] Web Based Quiz System 1.0 - 'eid' Union Based Sql Injection (Authenticated)
* [webapps] Online Ordering System 1.0 - Blind SQL Injection (Unauthenticated)
* [webapps] Textpattern CMS 4.9.0-dev - 'Excerpt' Persistent Cross-Site Scripting (XSS)
* [webapps] Textpattern CMS 4.8.4 - 'Comments' Persistent Cross-Site Scripting (XSS)
* [webapps] Online Ordering System 1.0 - Arbitrary File Upload to Remote Code Execution
* [webapps] e107 CMS 2.3.0 - CSRF
* [remote] AnyDesk 5.5.2 - Remote Code Execution
* [webapps] Local Services Search Engine Management System (LSSMES) 1.0 - Blind & Error based SQL injec
* [webapps] Local Services Search Engine Management System (LSSMES) 1.0 - 'name' Persistent Cross-Site
* [webapps] Zen Cart 1.5.7b - Remote Code Execution (Authenticated)
* [webapps] Web Based Quiz System 1.0 - 'name' Persistent/Stored Cross-Site Scripting
* [webapps] Tiny Tiny RSS - Remote Code Execution
* [webapps] Web Based Quiz System 1.0 - 'MCQ options' Persistent/Stored Cross-Site Scripting
* [webapps] Covid-19 Contact Tracing System 1.0 - Remote Code Execution (Unauthenticated)
* [webapps] Online Catering Reservation System 1.0 - Remote Code Execution (Unauthenticated)

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
```

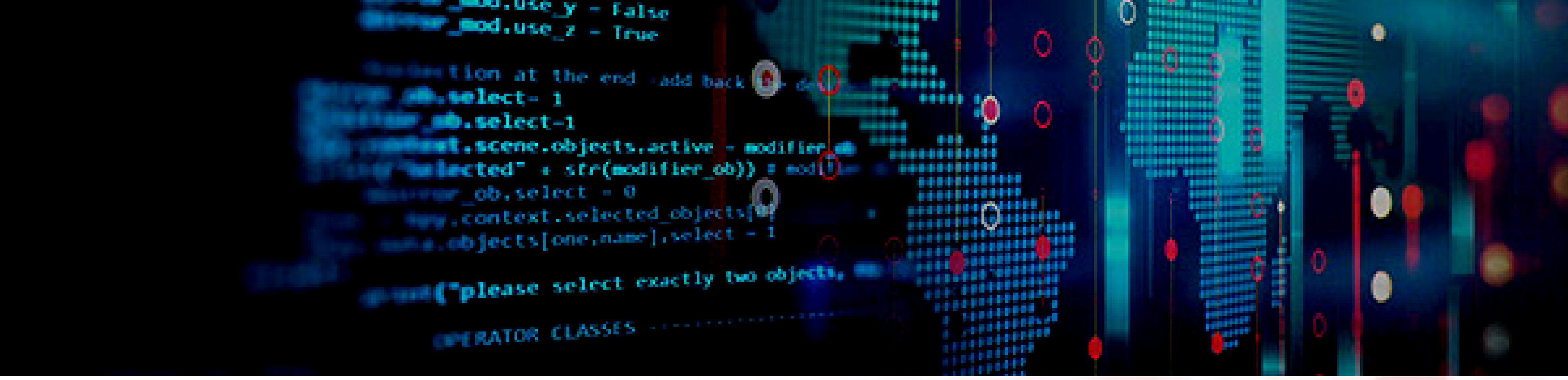
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://thanhthieunhi.thuathienhue.gov.vn/ma.html
http://thanhthieunhi.thuathienhue.gov.vn/ma.html notified by M3sicth
http://trungtamvhtt.thuathienhue.gov.vn/ma.html
http://trungtamvhtt.thuathienhue.gov.vn/ma.html notified by M3sicth
http://congdoan.thuathienhue.gov.vn/ma.html
http://congdoan.thuathienhue.gov.vn/ma.html notified by M3sicth
http://thanhnien.thuathienhue.gov.vn/ma.html
http://thanhnien.thuathienhue.gov.vn/ma.html notified by M3sicth
http://hoinongdan.thuathienhue.gov.vn/ma.html
http://hoinongdan.thuathienhue.gov.vn/ma.html notified by M3sicth
http://hoiphunu.thuathienhue.gov.vn/ma.html
http://hoiphunu.thuathienhue.gov.vn/ma.html notified by M3sicth
http://suhochue.thuathienhue.gov.vn/ma.html
http://suhochue.thuathienhue.gov.vn/ma.html notified by M3sicth
http://edic.thuathienhue.gov.vn/ma.html
http://edic.thuathienhue.gov.vn/ma.html notified by M3sicth
http://quybtte.thuathienhue.gov.vn/ma.html
http://quybtte.thuathienhue.gov.vn/ma.html notified by M3sicth
http://mattran.thuathienhue.gov.vn/ma.html
http://mattran.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://dulichphuloc.thuathienhue.gov.vn/ma.html
http://dulichphuloc.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://hueasean.thuathienhue.gov.vn/ma.html
http://hueasean.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://congtacxahoi.thuathienhue.gov.vn/ma.html
http://congtacxahoi.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://cpxd.thuathienhue.gov.vn/ma.html
http://cpxd.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://doanccq.thuathienhue.gov.vn/ma.html
http://doanccq.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://pccc.thuathienhue.gov.vn/ma.html
http://pccc.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution
http://hoinguoimu.thuathienhue.gov.vn/ma.html
http://hoinguoimu.thuathienhue.gov.vn/ma.html notified by Moroccan Revolution


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

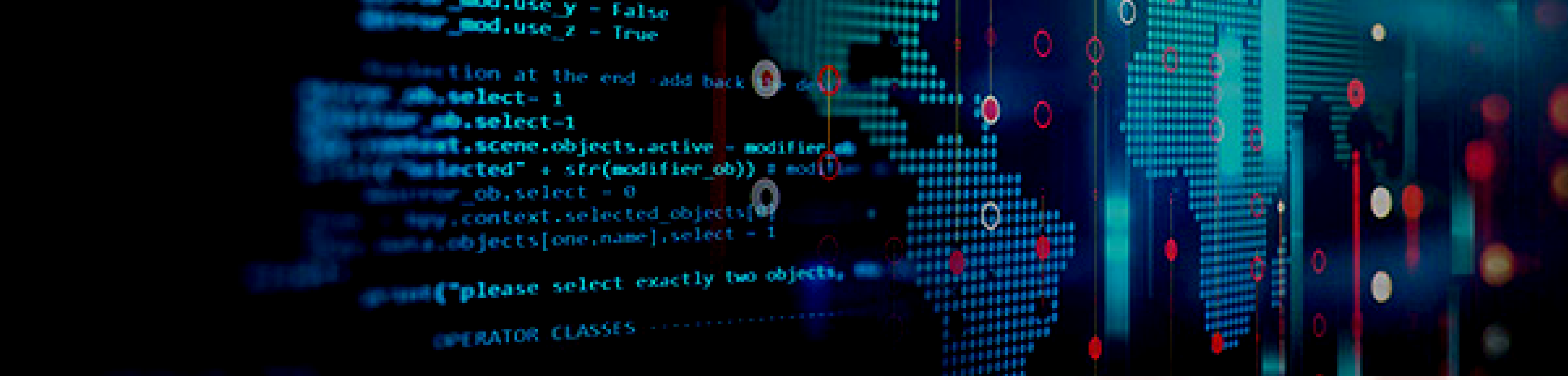
Dark Web News

Darknet Live

[UK Man Admits Ordering Drugs on the Darkweb](#)
A man from Swindon pleaded guilty to importing a variety of drugs he had purchased on the darkweb. (via darknetlive.com)
[German Man Avoids Prison in Attempted Drug Possession Case](#)
A German man who admitted purchasing ecstasy and amphetamine on the darkweb avoided prison by telling the judge he had "changed his ways.&rdquo; (via darknetlive.com)
[Three Arrested for Selling Opioids on Darkweb Markets](#)
The FBI relied on a Bitcoin trader during an investigation into the suspected operators of two darkweb vendor accounts. (via darknetlive.com)
[Four Arrested in Germany for Selling Drugs on the Darkweb](#)
German Customs arrested four men suspected of selling prescription medication and other drugs on the darkweb. (via darknetlive.com)

Dark Web Link

[Dark Web Forums: Cyberattack Compromises Renowned Cybercrime Platforms](#)
A series of cyberattacks have almost crippled four of the widely used hacking-based dark web forums. The unknown attackers had successfully seized the personal data of the forum members and siphoned away cash. In the past couple of weeks, the attackers had stolen user databases from these dark web forums. The databases contained hashed passwords [...] The post [Dark Web Forums: Cyberattack Compromises Renowned Cybercrime Platforms](#) appeared first on [Dark Web Link | Deep web Onion Links | Darknet News](#).
[CryptoPhone: A New Way To Keep Your Cryptocurrency Safe](#)
Cryptocurrencies or digital currencies seem to be the new currency that the majority of people rely on. Being digital assets, it is vulnerable to getting hacked, and people owing them can get so-called "wallet-rupt&rdquo; if they do not care about its security. This thought has given rise to what we will discuss here, Cryptophone. Additionally, [...] The post [CryptoPhone: A New Way To Keep Your Cryptocurrency Safe](#) appeared first on [Dark Web Link | Deep web Onion Links | Darknet News](#).
[How To Secure Your Bitcoin Wallet?](#)
Bitcoin (BTC), the most talked about and used cryptocurrencies, has attracted an enormous mass of people since it gained popularity. This is probably the first-ever digital currency or cryptocurrency and can be bought, sold and traded. Since it is a digital currency, one would need a digital wallet (not physical ones) to buy and sell [...] The post [How To Secure Your Bitcoin Wallet?](#) appeared first on [Dark Web Link | Deep web Onion Links | Darknet News](#).



Advisories

US-Cert Alerts & bulletins

* Microsoft IOC Detection Tool for Exchange Server Vulnerabilities
* Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities
* Update to Alert on Mitigating Microsoft Exchange Server Vulnerabilities
* Joint NSA and CISA Guidance on Strengthening Cyber Defense Through Protective DNS
* Cisco Releases Security Updates
* VMware Releases Security Update
* CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities
* Google Releases Security Updates for Chrome
* AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities
* AA21-055A: Exploitation of Accellion File Transfer Appliance
* Vulnerability Summary for the Week of February 22, 2021
* Vulnerability Summary for the Week of February 15, 2021

Zero Day Initiative Advisories

ZDI-CAN-12977: Delta Industrial Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2021-03-05, 3 days ago. The vendor is given until 2021-07-03 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-13097: Microsoft
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-03-05, 3 days ago. The vendor is given until 2021-07-03 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-12819: 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 'Francis Provencher {PRL}' was reported to the affected vendor on: 2021-03-05, 3 days ago. The vendor is given until 2021-07-03 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-12820: 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 'Francis Provencher {PRL}' was reported to the affected vendor on: 2021-03-05, 3 days ago. The vendor is given until 2021-07-03 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-12720: 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: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13304: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13309: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13307: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13306: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13305: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13311: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-11883: Advantech

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Selim Enes Karaduman (@Enesdex)' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13319: Trend Micro

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'HexKitchen' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13170: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13169: 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 'Michael

DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13162: 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 'Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13092: 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 'Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13095: 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 'Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13091: 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 'Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13068: VMware

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 'Zeeshan Shaikh (@bugzzzhunter) from NotSoSecure' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13147: 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: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13150: 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: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13102: 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: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 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-13100: 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 'Yongil Lee(@intellee) and Wonyoung Jung(@nonetype) of Diffense' was reported to the affected vendor on: 2021-03-03, 5 days ago. The vendor is given until 2021-07-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Red Hat Security Advisory 2021-0744-01

Red Hat Security Advisory 2021-0744-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0740-01

Red Hat Security Advisory 2021-0740-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0738-01

Red Hat Security Advisory 2021-0738-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0741-01

Red Hat Security Advisory 2021-0741-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0739-01

Red Hat Security Advisory 2021-0739-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0743-01

Red Hat Security Advisory 2021-0743-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products.

Asterisk Project Security Advisory - AST-2021-006

When Asterisk sends a re-invite initiating T.38 faxing and the endpoint responds with a m=image line and zero port, a crash will occur in Asterisk. This is a re-occurrence of AST-2019-004.

Ubuntu Security Notice USN-4757-2

Ubuntu Security Notice 4757-2 - USN-4757-1 fixed a vulnerability in wpa_supplicant and hostapd. This update provides the corresponding update for Ubuntu 14.04 ESM. It was discovered that wpa_supplicant did not properly handle P2P provision discovery requests in some situations. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-0736-01

Red Hat Security Advisory 2021-0736-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR6-FP25. Issues addressed include buffer overflow and bypass vulnerabilities.

Red Hat Security Advisory 2021-0735-01

Red Hat Security Advisory 2021-0735-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0734-01

Red Hat Security Advisory 2021-0734-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2021-0733-01

Red Hat Security Advisory 2021-0733-01 - IBM Java SE version 7 Release 1 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 7 to version 7R1 SR4-FP80. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0717-01

Red Hat Security Advisory 2021-0717-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR6-FP25. Issues addressed include buffer overflow and bypass vulnerabilities.

Red Hat Security Advisory 2021-0719-01

Red Hat Security Advisory 2021-0719-01 - Red Hat Advanced Cluster Management for Kubernetes 2.0.8 images. Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console&mdash;with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which resolve some security issues and bugs.

Red Hat Security Advisory 2021-0727-01

Red Hat Security Advisory 2021-0727-01 - The Berkeley Internet Name Domain is an implementation of the Domain Name System protocols. BIND includes a DNS server ; a resolver library ; and tools for verifying that the DNS server is operating correctly. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0711-01

Red Hat Security Advisory 2021-0711-01 - Kernel-based Virtual Machine offers a full virtualization solution for Linux on numerous hardware platforms. The virt:rhel module contains packages which provide user-space components used to run virtual machines using KVM. The packages also provide APIs for managing and interacting with the virtualized systems.

Ubuntu Security Notice USN-4757-1

Ubuntu Security Notice 4757-1 - It was discovered that wpa_supplicant did not properly handle P2P provision discovery requests in some situations. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2021-0637-01

Red Hat Security Advisory 2021-0637-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include XML injection and information leakage vulnerabilities.

Red Hat Security Advisory 2021-0710-01

Red Hat Security Advisory 2021-0710-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc.

Red Hat Security Advisory 2021-0428-01

Red Hat Security Advisory 2021-0428-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2021-0429-01

Red Hat Security Advisory 2021-0429-01 - 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 4.5.33. Issues addressed include cross site scripting, denial of service, deserialization, and traversal vulnerabilities.

Red Hat Security Advisory 2021-0701-01

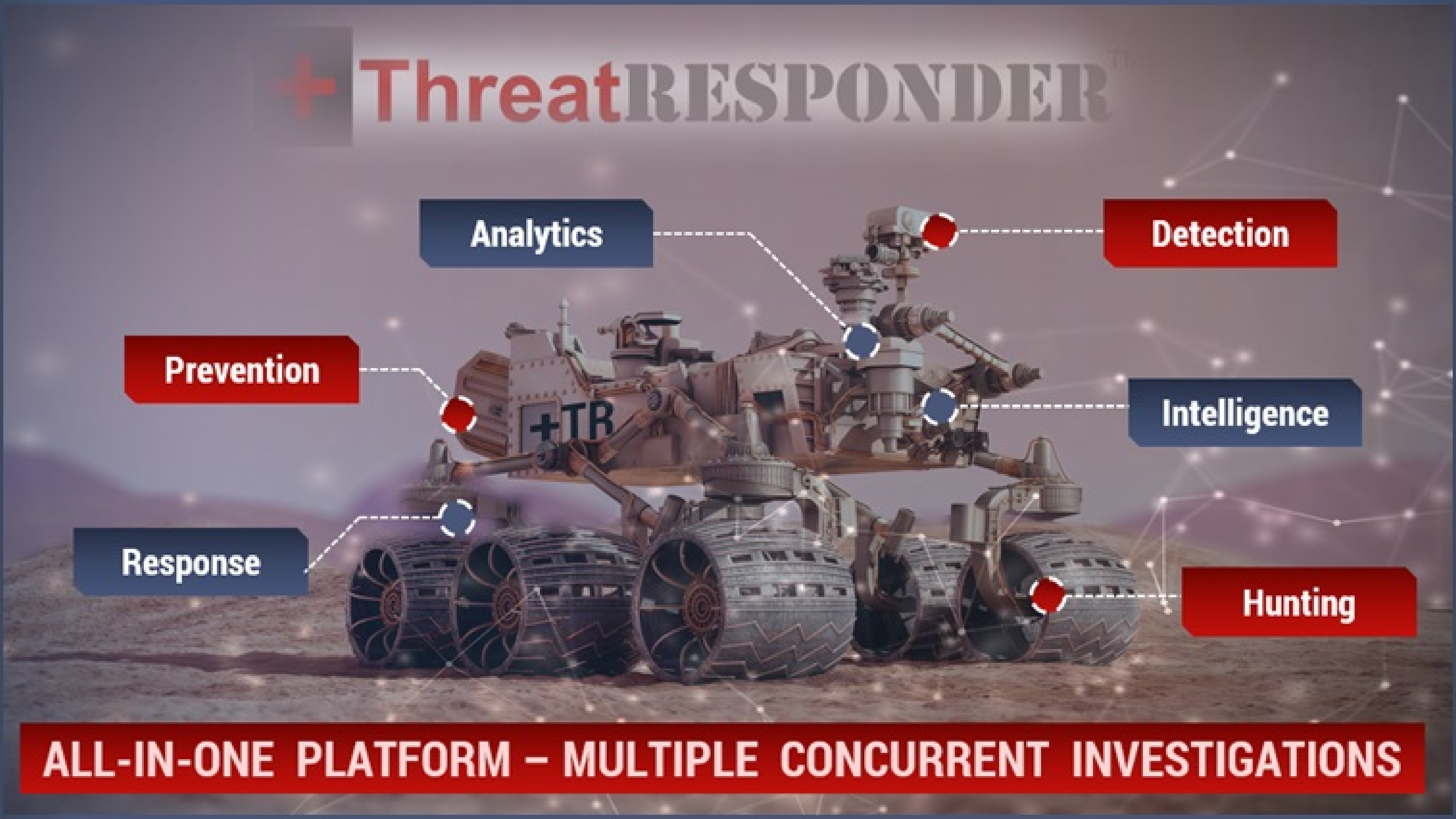
Red Hat Security Advisory 2021-0701-01 - The grub2 packages provide version 2 of the Grand Unified Boot Loader, a highly configurable and customizable boot loader with modular architecture. The packages support a variety of kernel formats, file systems, computer architectures, and hardware devices. Issues addressed include buffer overflow, out of bounds write, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-4754-4

Ubuntu Security Notice 4754-4 - USN-4754-1 fixed vulnerabilities in Python. Because of a regression, a subsequent update removed the fix for CVE-2021-3177. This update reinstates the security fix for CVE-2021-3177. It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-0700-01

Red Hat Security Advisory 2021-0700-01 - The grub2 packages provide version 2 of the Grand Unified Boot Loader, a highly configurable and customizable boot loader with modular architecture. The packages support a variety of kernel formats, file systems, computer architectures, and hardware devices. Issues addressed include buffer overflow, out of bounds write, and use-after-free vulnerabilities.


ThreatRESPONDER
Analytics
Detection
Prevention
+TR
Intelligence
Response
Hunting
ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

Sponsored Products

CSI Linux: Current Version: 2021.1

Download here.

CSI Linux 2021.1 is an investigation platform focusing on OSINT, SOCMINT, SIGINT, Cyberstalking, Darknet, Cryptocurrency, (Online-Network-Disk) Forensics, Incident Response, & Reverse Engineering/Malware Analysis.

CSI Linux 2021.1 has been rebuilt from the ground up on Ubuntu 20.04 LTS to provide long term support for the backend OS and has become a powerful Investigation environment that comes in both the traditional Virtual Machine option and a bootable image that you can install onto an external drive or USB to use as your daily driver or DFIR triage drive. The SIEM has been given an evolution boost with capability while being encapsulated into a Docker container

CSI Linux Tutorials for 2021.1:

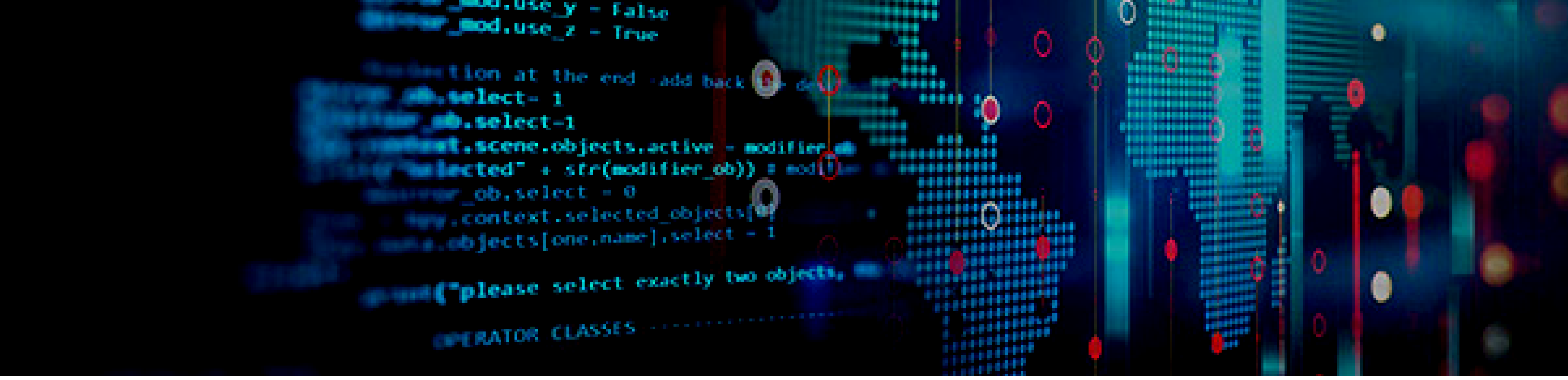
PDF: Installation Document (CSI Linux 2021.1 Virtual Appliance)
PDF: Installation Document (CSI Linux 2021.1 Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:
* Amazon FireTV App - amzn.to/30oiUpE
* YouTube - youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg

Printed / Kindle Publications:
* Cyber Secrets on Amazon - amzn.to/2UuIG9B



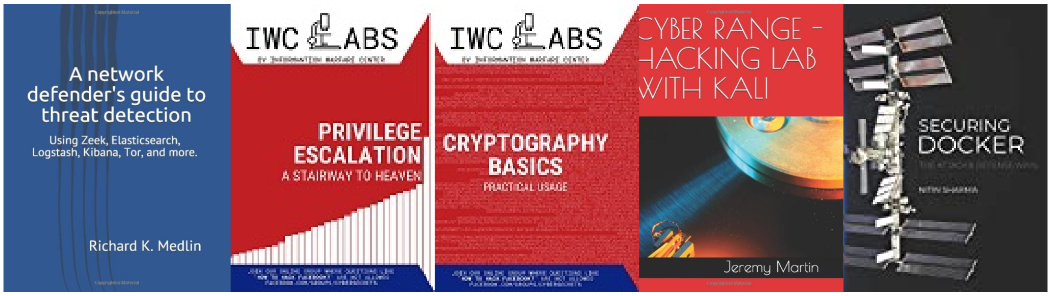
The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

CYBER Secrets
What's Inside?
Threat Intelligence & Training
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION

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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP