Jul-12-21

CYBER WEEKLY AWARENESS REPORT

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

netSecurity®

INFORMATION WARFARE CENTER

LINUX

ARGOS APPLIED INTELLIGENCE

CYBER WEEKLY AWARENESS REPORT

July 12, 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

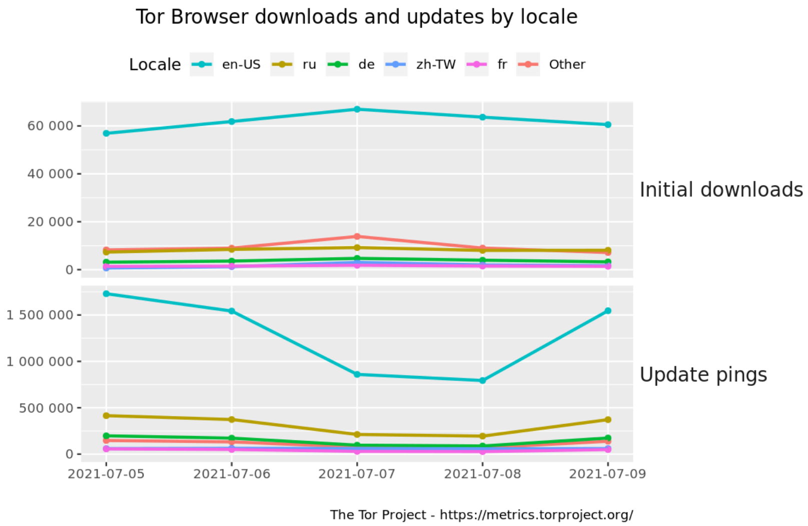
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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.

Just released!!! Web App Hacking: Carnage & Pwnage



Interesting News

* Subscribe to this OSINT resource to recieve it in your inbox. The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

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

*** CSI Linux 2021.2 has just been released! Download today! csilinux.com

Index of Sections

LATEST NEWS

Packet Storm Security

Krebs on Security

* Spike in "Chain Gang" Destructive Attacks on ATMs
* Kaseya Left Customer Portal Vulnerable to 2015 Flaw in its Own Software
* Microsoft Issues Emergency Patch for Windows Flaw
* Another 0-Day Looms for Many Western Digital Users
* Intuit to Share Payroll Data from 1.4M Small Businesses With Equifax
* We Infiltrated a Counterfeit Check Ring! Now What?
* MyBook Users Urged to Unplug Devices from Internet
* How Cyber Sleuths Cracked an ATM Shimmer Gang
* How Cyber Safe is Your Drinking Water Supply?
* First American Financial Pays Farcical $500K Fine

LATEST NEWS

Dark Reading

* Microsoft Confirms Acquisition of RiskIQ
* Kaseya Releases Security Patch as Companies Continue to Recover
* AI and Cybersecurity: Making Sense of the Confusion
* Navigating Active Directory Security: Dangers and Defenses
* How Dangerous Is Malware? New Report Finds It's Tough to Tell
* CISA Analysis Reveals Successful Attack Techniques of FY 2020
* New Framework Aims to Describe & Address Complex Social Engineering Attacks
* I Smell a RAT! New Cybersecurity Threats for the Crypto Industry
* It's in the Game (but It Shouldn't Be)
* Cartoon Caption Winner: Sight Unseen
* Morgan Stanley Discloses Data Breach
* New WildPressure Malware Capable of Targeting Windows and MacOS
* Kaseya Hacked via Authentication Bypass
* The NSA's 'New' Mission: Get More Public With the Private Sector
* What Colonial Pipeline Means for Commercial Building Cybersecurity
* Attacks on Kaseya Servers Led to Ransomware in Less Than 2 Hours
* Fake Android Apps Promise Cryptomining Services to Steal Funds
* Sophos Acquires Capsule8 for Linux Server & Container Security
* Are Security Attestations a Necessity for SaaS Businesses?
* Microsoft Releases Emergency Patch for 'PrintNightmare' Vuln

The Hacker News

* Crafting a Custom Dictionary for Your Password Policy
* Hackers Spread BIOPASS Malware via Chinese Online Gambling Sites
* Kaseya Releases Patches for Flaws Exploited in Widespread Ransomware Attack
* Magecart Hackers Hide Stolen Credit Card Data Into Images for Evasive Exfiltration
* New SaaS Security Report Dives into the Concerns and Plans of CISOs in 2021
* Critical Flaws Reported in Philips Vue PACS Medical Imaging Systems
* Hackers Use New Trick to Disable Macro Security Warnings in Malicious Office Files
* Critical Flaws Reported in Sage X3 Enterprise Management Software
* Experts Uncover Malware Attacks Targeting Corporate Networks in Latin America
* Security Awareness Training is Broken. Human Risk Management (HRM) is the Fix
* How to Mitigate Microsoft Print Spooler Vulnerability - PrintNightmare
* SideCopy Hackers Target Indian Government Officials With New Malware
* Microsoft's Emergency Patch Fails to Fully Fix PrintNightmare RCE Vulnerability
* WildPressure APT Emerges With New Malware Targeting Windows and macOS
* Dozens of Vulnerable NuGet Packages Allow Attackers to Target .NET Platform

LATEST NEWS

Security Week

* Microsoft to Acquire Threat Intelligence Vendor RiskIQ
* SolarWinds Confirms New Zero-Day Flaw Under Attack
* CISA Releases Analysis of 2020 Risk and Vulnerability Assessments
* Mitsubishi Electric Patches Vulnerabilities in Air Conditioning Systems
* Seizing Cryptocurrency: How is Law Enforcement Tracing and Recovering Bitcoin Payments?
* Kaseya Releases Patches for Vulnerabilities Exploited in Ransomware Attack
* Netskope Raises $300 Million at $7.5 Billion Valuation
* Consumer Group Lodges EU Complaint Against WhatsApp
* "Cyber Disruption" Stops Websites of Iranian Ministry
* Biden Tells Putin Russia Must Crack Down on Cybercriminals
* Insurer CNA Discloses Ransomware Attack
* ZLoader Adopts New Macro-Related Delivery Technique in Recent Attacks
* Cybersecurity M&A Roundup: 14 Deals Announced July 1-8, 2021
* Did Microsoft Botch the PrintNightmare Patch?
* Microsoft Paid Out $13.6 Million in Bug Bounties in Past Year
* Sage X3 Vulnerabilities Can Pose Serious Risk to Organizations
* Restart After Hacks Delayed Again by Software Firm
* Morgan Stanley Hit by Accellion Hack Through Third-Party Vendor
* Israel Says It's Targeting Hamas' Cryptocurrency Accounts
* Cisco Patches High Severity Vulnerabilities in BPA, WSA
* Use of Common Malware in Operation Targeting Energy Sector Makes Attribution Difficult
* IoT/OT Device Security Firm NanoLock Raises $11 Million
* Mac Malware Used in Attacks Targeting Industrial Organizations in Middle East
* Biden Pressured to Act on 'Russian' Ransomware, Hacking

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Ransomware Attacks Put Singapore Organizations at Risk of Violation of the Personal Data Protection A
* Counterterrorism Strategies Could Be the Key to Stopping Ransomware
* Phishbait Follows Current Events
* The Pandemic's Paradigm Shift with Cybersecurity
* How to Defeat REvil Ransomware
* KnowBe4 Fresh Content Updates from June
* Implement DMARC the Right Way to Keep Phishing Attacks Out of Your Inbox
* Ransomware Attacks from Within Russia So Impactful, U.S. Government Says They Will Take Action If Rus
* How REvil Works: A Look Inside the World's Most Famous Ransomware-as-a-Service
* Social Engineering and Organizational Culture

ISC2.org Blog

* Security Evangelist or Zealot - Where to Draw the Line
* CISSPs from Around The Globe: An Interview with Theresa Grafenstine
* Igniting Passion for Diversity, Equity and Inclusion (DEI): Cybersecurity Professionals Address Chall
* DoD Adds Two More (ISC)&sup2; Certifications to Requirements for Cybersecurity Staff
* NIST Has Come Out With Its Own Ransomware Guidance | #RansomwareWeek

HackRead

* Kaseya issues patches for vulnerabilities exploited in ransomware attack
* How data collected in gaming can be used to breach user privacy
* How can you protect your personal, sensitive data online?
* SEC charges dark web user of insider trading, money laundering
* Hackers disabling Macro security warnings in new malspam campaign
* Malware hits Hive OS cryptomining users; steals funds from wallets
* 5 Reasons Every Small Business Needs An Employee App

Koddos

* Kaseya issues patches for vulnerabilities exploited in ransomware attack
* How data collected in gaming can be used to breach user privacy
* How can you protect your personal, sensitive data online?
* SEC charges dark web user of insider trading, money laundering
* Hackers disabling Macro security warnings in new malspam campaign
* Malware hits Hive OS cryptomining users; steals funds from wallets
* 5 Reasons Every Small Business Needs An Employee App

LATEST NEWS

Naked Security

* Don't get tricked by this crashtastic iPhone Wi-Fi hack!
* Where do all those cybercrime payments go?
* S3 Ep40: Kaseya breach, PrintNightmare 0-day, and hacking versus the law [Podcast]
* PrintNightmare official patch is out - update now!
* Kaseya ransomware attackers say: "Pay $70 million and we'll set everyone free"
* S3 Ep39.5: A conversation with Eva Galperin [Podcast]
* US email hacker gets his "computer trespass" conviction reversed
* S3 Ep39: Paying the date, #SocialMediaDay tips, and a special splintersode [Podcast]
* PrintNightmare, the zero-day hole in Windows - here's what to do
* Colombian police arrest Gozi malware suspect after 8 years at large

Threat Post

* Critical RCE Vulnerability in ForgeRock OpenAM Under Active Attack
* Kaseya Patches Zero-Days Used in REvil Attacks
* Cyber Polygon 2021: Towards Secure Development of Digital Ecosystems
* Microsoft Office Users Warned on New Malware-Protection Bypass
* Cisco BPA, WSA Bugs Allow Remote Cyberattacks
* Lazarus Targets Job-Seeking Engineers with Malicious Documents
* Oil & Gas Targeted in Year-Long Cyber-Espionage Campaign
* Coursera Flunks API Security Test in Researchers' Exam
* How Fake Accounts and Sneaker-Bots Took Over the Internet
* Critical Sage X3 RCE Bug Allows Full System Takeovers

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

LATEST NEWS

IBM Security Intelligence

* RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
* Don't Be Rude, Stay: Avoiding Fork&Run .NET Execution With InlineExecute-Assembly
* What's Next for SIEM? A View From the 2021 Gartner SIEM Magic Quadrant
* REvil Ransomware Gang Launches Major Supply Chain Attack Through Kaseya, Downstream Impact May Affect
* Attacks on Operational Technology From IBM X-Force and Dragos Data
* The OSI Model and You Part 7: Stopping Threats at the Application Layer
* Confessions of a Famous Fraudster: How and Why Social Engineering Scams Work
* Hunting for Windows "Features" with Frida: DLL Sideloading
* June 2021 Security Intelligence Roundup: Cybersecurity Certifications, The Problem With New Accounts
* A Fly on ShellBot's Wall: The Risk of Publicly Available Cryptocurrency Miners

InfoWorld

* The real successes of AI
* 5 AI startups out to change the world
* How service virtualization improves application testing
* "Do More with R" video tutorials
* Don't be a ransomware victim
* Developers react to GitHub Copilot
* Get a look at CodeSandbox
* How to use R with BigQuery
* Getting started with time series analysis
* AI gives software development tools a boost

C4ISRNET - Media for the Intelligence Age Military

* Air Force cyber squadron offers its malicious file detection software to private sector
* Can a nominee with tech industry background disrupt Pentagon acquisition shop's status quo?
* The German 'new space' industry is booming. So why isn't Berlin buying in?
* New Mexico space innovation hub launches with federal funding
* With JEDI cloud scuttled, Pentagon embraces critics' idea of multicloud for digital warfare
* US needs radical shifts and bipartisan cooperation to defend its position against China
* Space Force opens facility to improve war-fighting capabilities
* US Marines get new cyber boss
* Maneuver warfare in space: The strategic imperative for nuclear thermal propulsion
* US Army to test electronic warfare coders at the edge during upcoming exercise

The Hacker Corner

Conferences

* Marketing For Cybersecurity
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* An EPYC escape: Case-study of a KVM breakout
* Fuzzing iOS code on macOS at native speed

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.

* Lexington Informatics Tournament CTF 2021
* Google Capture The Flag 2021
* CyberSci Nationals 2021
* Securebug.se CTF Loki 2021
* HTB Business CTF 2021
* ImaginaryCTF 2021
* IJCTF 2021
* CyBRICS CTF 2021
* Crypto CTF 2021
* UIUCTF 2021

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

* HackathonCTF: 2
* Hackable: II
* VulnCMS: 1
* hacksudo: ProximaCentauri
* Tech_Supp0rt: 1

Tools & Techniques

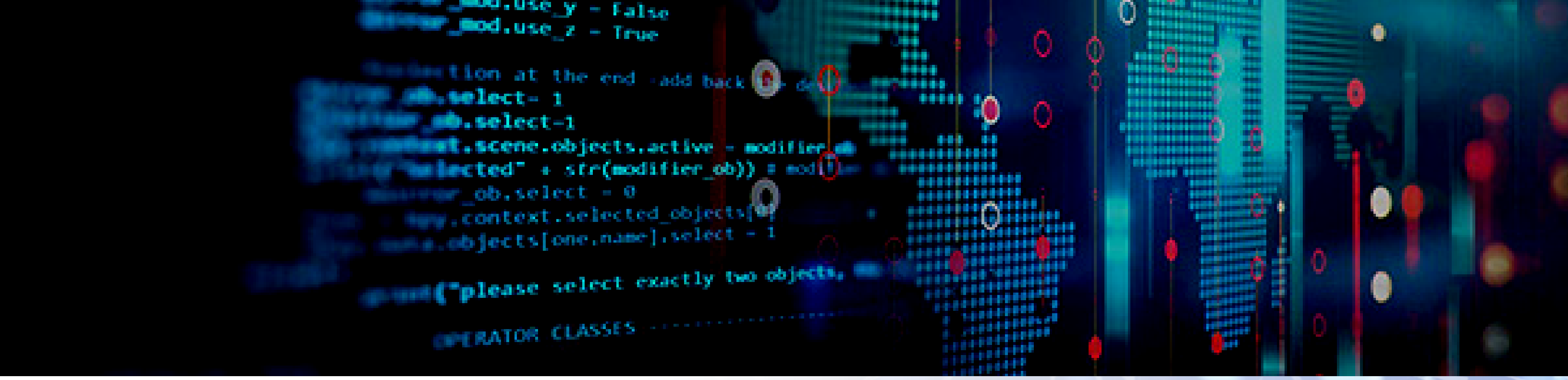
Packet Storm Security Tools Links

Kali Linux Tutorials

* TiEtwAgent : PoC Memory Injection Detection Agent Based On ETW, For Offensive And Defensive Research
* OpenAttack : An Open-Source Package For Textual Adversarial Attack
* Lazyrecon : Tool To Automate Your Reconnaissance Process In An Organized Fashion
* GDir-Thief : Red Team Tool For Exfiltrating The Target Organization'S Google People Directory That Yo
* MacHound : An extension to audit Bloodhound collecting and ingesting of Active Directory relationship
* FRIDA-DEXDump : Fast Search And Dump Dex On Memory
* Scour : AWS Exploitation Framework
* Backstab : A Tool To Kill Antimalware Protected Processes
* Invoke-DNSteal : Simple And Customizable DNS Data Exfiltrator
* Gorsair : Hacks Its Way Into Remote Docker Containers That Expose Their APIs

GBHackers Analysis

* Russian APT Hackers Launched A Mass Global Brute Force Attack to Hack Enterprise & Cloud Networks
* Hackers Use Western Digital My Book Zero-day Vulnerability to Mass-wipe Live Devices
* 5 Key Phases of Ethical Hacking
* Researcher Managed to Hack ATMs Using His Phone's NFC & Android App
* 10 Best WiFi Hacking Apps for Android - 2021 Edition



Weekly Cyber Security Video and Podcasts

SANS DFIR

* DFIR Summit 2021
* STAR Webcast: Dissecting BadBlood: an Iranian APT Campaign
* FOR585: Smartphone Forensic Analysis In-Depth
* Why take FOR585: Smartphone Forensic Analysis In-Depth OnDemand

Defcon Conference

* DEF CON China Party 2021 - Keynote Interview Excerpt - Steve Wozniak, The Dark Tangent
* DEF CON China Party 2021 - Whispers Among the Stars - James Pavur
* DEF CON China Party 2021- Wall of Sheep: Hilarious Fails and the Sheep Behind Them - Riverside
* DEF CON China Party - Cooper Quintin- Detecting Fake 4G Base Stations in Real Time

Hak5

* Touring Glytch's Hacker Van (It shrank!)
* Print Nightmare payload by @PanicAcid for the Bash Bunny -- Payload Hero!
* HakByte: Catch Hackers in Your Wi-Fi With a $3 FTP Honeypot

The PC Security Channel [TPSC]

* Windows 11: Better Security?
* F Secure Total: Test vs Malware and ID Protection

Eli the Computer Guy

* How to Become a YouTuber
* How to Become a Tech Professional
* "Easy" SMS with Twilio (Add SMS to Your Coding Projects)
* "Easy" Computer Vision with Azure and AWS

Security Now

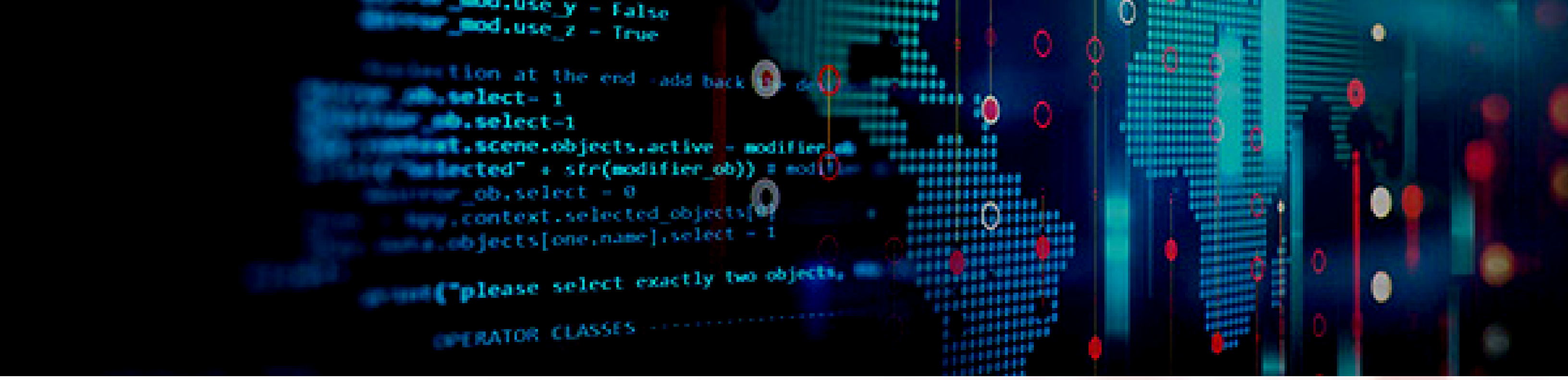
* The Kaseya Saga - Microsoft PrintNightmare, WD's MyCloud OS3 Troubles, SpinRite in a BMW
* Halfway Through 2021 - Google's FLoC, $600M Ransomware Attack, Where Will Windows 11 Run?

Troy Hunt

* Weekly Update 251

Intel Techniques: The Privacy, Security, & OSINT Show

* 224-Employment Privacy & Security
* 223-Secure Messaging Woes (and Solutions)



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

* Joining Microsoft is the Next Stage of the RiskIQ Journey
* Here's How Much Threat Activity is in Each Internet Minute
* Media Land: Bulletproof Hosting Provider is a Playground for Threat Actors
* Bit2check: Stolen Card Validation Service Illuminates A New Corner of the Skimming Ecosystem
* Microsoft Exchange is a Global Vulnerability. Patching Efforts Reveal Regional Inconsistencies
* The Sysrv-hello Cryptojacking Botnet: Here's What's New
* This is How Your Attack Surface May Be Larger and More Exposed Than You Think
* MobileInter: A Popular Magecart Skimmer Redesigned For Your Phone
* DarkSide is Standing Down, But Its Affiliates Live On
* Next-Gen Threat Intelligence: Adding Profound Value to Security and Risk Functions

FireEye

* Managed Service Providers Used in Coordinated, Mass Ransomware Attack Impacting Hundreds of Companies
* Securing the Supply Chain: Lessons Learned from the Codecov Compromise
* Metasploit Wrap-up
* Apple Silicon Support on Insight Agent
* What's New in InsightIDR: Q2 2021 in Review
* Introducing the Manual Regex Editor in IDR's Parsing Tool: Part 2
* [Security Nation] Jonathan Cran on demystifying startup funding for security companies
* Introducing InsightCloudSec
* CVE-2020-7387..7390: Multiple Sage X3 Vulnerabilities
* Introducing the Manual Regex Editor in IDR's Parsing Tool: Part 1

Proof of Concept (PoC) & Exploits

Packet Storm Security

CXSecurity

* GravCMS 1.10.7 Arbitrary YAML Write / Update
* Pallets Werkzeug 0.15.4 Path Traversal
* Netgear DGN2200v1 Remote Command Execution
* Docker Dashboard Remote Command Execution
* Ricon Industrial Cellular Router S9922XL Remote Command Execution (RCE)
* GLPI 9.4.5 Remote Code Execution
* EasyFTP Server 1.7.0.11 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

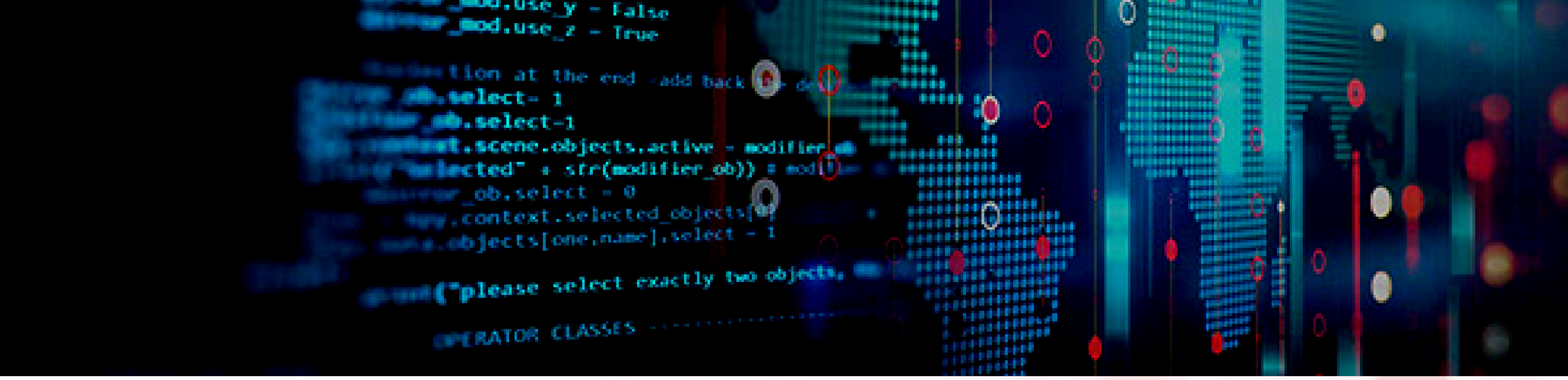
* [webapps] Zoo Management System 1.0 - 'Multiple' Stored Cross-Site-Scripting (XSS)
* [webapps] Church Management System 1.0 - SQL Injection (Authentication Bypass) + Arbitrary File Uploa
* [webapps] Wordpress Plugin SP Project & Document Manager 4.21 - Remote Code Execution (RCE) (Authenti
* [webapps] Online Covid Vaccination Scheduler System 1.0 - Arbitrary File Upload to Remote Code Execut
* [webapps] Wyomind Help Desk 1.3.6 - Remote Code Execution (RCE)
* [webapps] Employee Record Management System 1.2 - Stored Cross-Site Scripting (XSS)
* [webapps] Exam Hall Management System 1.0 - Unrestricted File Upload + RCE (Unauthenticated)
* [webapps] WordPress Plugin Plainview Activity Monitor 20161228 - Remote Code Execution (RCE) (Authent
* [webapps] Online Covid Vaccination Scheduler System 1.0 - 'username' time-based blind SQL Injection
* [webapps] Rocket.Chat 3.12.1 - NoSQL Injection to RCE (Unauthenticated) (2)
* [webapps] WordPress Plugin Anti-Malware Security and Bruteforce Firewall 4.20.59 - Directory Traversa
* [webapps] Phone Shop Sales Managements System 1.0 - 'Multiple' Arbitrary File Upload to Remote Code E
* [webapps] Phone Shop Sales Managements System 1.0 - Authentication Bypass (SQLi)
* [webapps] Visual Tools DVR VX16 4.2.28 - Local Privilege Escalation
* [webapps] Exam Hall Management System 1.0 - Unrestricted File Upload (Unauthenticated)
* [webapps] Billing System Project 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Pallets Werkzeug 0.15.4 - Path Traversal
* [webapps] Black Box Kvm Extender 3.4.31307 - Local File Inclusion
* [webapps] Netgear DGN2200v1 - Remote Command Execution (RCE) (Unauthenticated)
* [webapps] Visual Tools DVR VX16 4.2.28.0 - OS Command Injection (Unauthenticated)
* [webapps] perfexcrm 1.10 - 'State' Stored Cross-site scripting (XSS)
* [webapps] Ricon Industrial Cellular Router S9922XL - Remote Command Execution (RCE)
* [webapps] TextPattern CMS 4.9.0-dev - Remote Command Execution (RCE) (Authenticated)
* [webapps] Simple Client Management System 1.0 - Remote Code Execution (RCE)

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
```

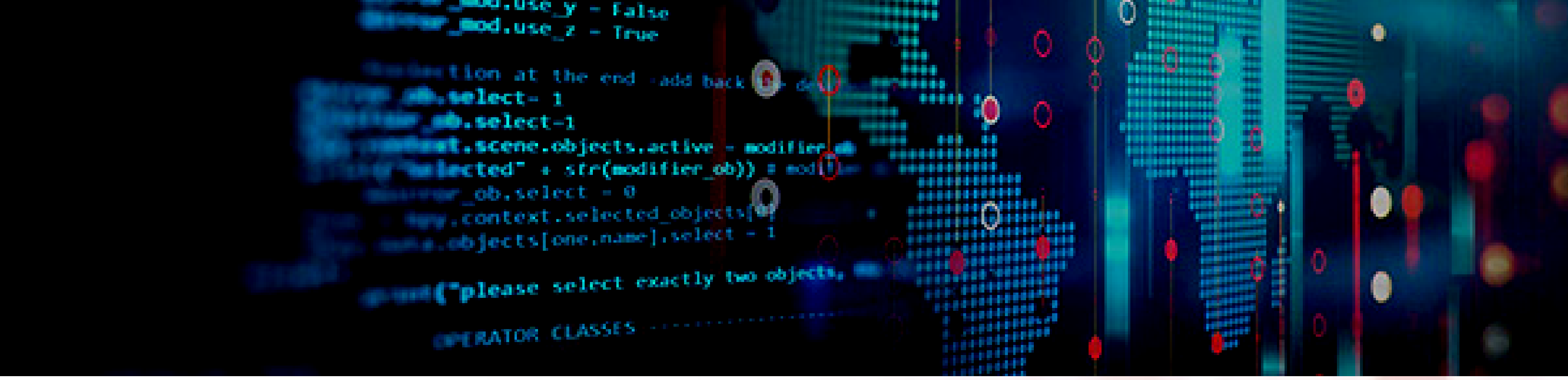
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

Unfortunately, at the time of this report, the Zone-H.org last hacked feed was not availible.


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

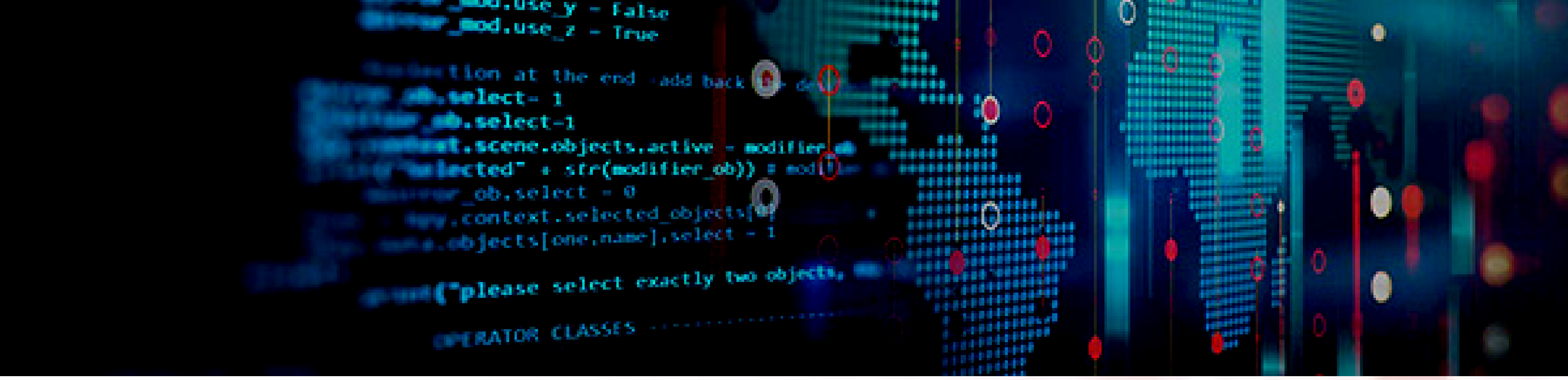
Dark Web News

Darknet Live

Operation DisrupTor: Cocaine Vendor Sentenced to Prison
A darkweb vendor has been sentenced to 6.5 years in federal prison for selling more than 4,000 grams of cocaine to customers throughout the United States. (via darknetlive.com)
Reminder: Tor is Ending Support for v2 Onion Services
Tor is depreciating v2 onion services. Soon they will become unreachable and you will feel bad. (via darknetlive.com)
The Majority of Market Admins Don't Get Caught
Although many high-profile cases involving darkweb market admins make the news, the majority of market creators retire in peace. (via darknetlive.com)
German Woman Tried to Hire a Hitman on the Darkweb
A German woman allegedly tried to hire a hitman on the darkweb to murder her ex-husband's girlfriend. (via darknetlive.com)

Dark Web Link

Uyghurs Were Oppressed In China Not Just In Xinjiang, But Also In 28 Other Countries: Details Of The Report Uyghur Muslims Are Being Persecuted Across China
The Oxus Society for Central Asian Affairs as well as the Uyghur Human Rights Project (UHRP) the have published a significant research paper revealing the scale of the People's Republic of China's transnational repression of Uyghurs for over three decades, as well as how many countries around the world have been complicit in the persecution [...] The post Uyghurs Were Oppressed In China Not Just In Xinjiang, But Also In 28 Other Countries: Details Of The Report Uyghur Muslims Are Being Persecuted Across China appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Beating Bitcoin: Why Some Traders Are Less Worried About Usd Prices
Each altcoin's price is always made up of two parts. The coin's own features include, among other things, fundamentals, investor sentiment toward the asset, liquidity, and trading volume. Bitcoin's performance is another powerful feature that frequently renders any altcoin-specific dynamics useless. Whether you like it or not, when the king of cryptocurrencies climbs, there's opportunity [...] The post Beating Bitcoin: Why Some Traders Are Less Worried About Usd Prices appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
$300 Million Investment In Blockchain Capital
Cryptocurrency is a digital currency that is used virtually as a medium of exchange between individuals. A cryptocurrency is designed through a strong computerized database that works as a medium of exchange between individuals. It exists in the virtual form and works as an asset. When particularly said it takes the form of virtual asset. [...] The post $300 Million Investment In Blockchain Capital appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


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

Advisories

US-Cert Alerts & bulletins

* Kaseya Provides Security Updates for VSA On-Premises Software Vulnerabilities
* Critical ForgeRock Access Management Vulnerability
* CISA Releases Analysis of FY20 Risk and Vulnerability Assessments
* Cisco Releases Security Updates for Multiple Products
* CISA Publishes Malware Analysis Report and Updates Alert on DarkSide Ransomware
* Microsoft Releases Out-of-Band Security Updates for PrintNightmare
* CISA Releases Security Advisory for Philips Vue PAC Products
* CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Att
* AA21-148A: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs
* AA21-131A: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Att
* Vulnerability Summary for the Week of July 5, 2021
* Vulnerability Summary for the Week of June 28, 2021

Zero Day Initiative Advisories

ZDI-CAN-14531: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-13801: Bitdefender

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by '@Kharosx0' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-14532: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-14529: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-13946: Jenkins

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Adith Sudhakar' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-13932: Parallels

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 'say2' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-13918: 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 'kdot' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-14586: Microsoft

A CVSS score 5.3 (AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-13830: 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 'Xavier DANEST - Decathlon' was reported to the affected vendor on: 2021-07-09, 3 days ago. The vendor is given until 2021-11-06 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-14533: Microsoft

A CVSS score 5.3 (AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14118: 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 'kdot' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14534: Microsoft

A CVSS score 5.3 (AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14528: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14120: 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 'ZhangJiaxing(@r0fm1a) from Codesafe Team of Legendsec at Qi'anxin Group' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14270: 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 'Anonymous' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14194: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until

2021-11-04 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-14056: Hewlett Packard Enterprise

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 'Erik de Jong' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14515: Apple

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 'Mickey Jin (@patch1t) of Trend Micro' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14110: NETGEAR

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'her0ysback' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14313: Open Design Alliance (ODA)

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: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14304: Open Design Alliance (ODA)

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: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14306: Open Design Alliance (ODA)

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: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14282: Open Design Alliance (ODA)

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' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 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-14297: Open Design Alliance (ODA)

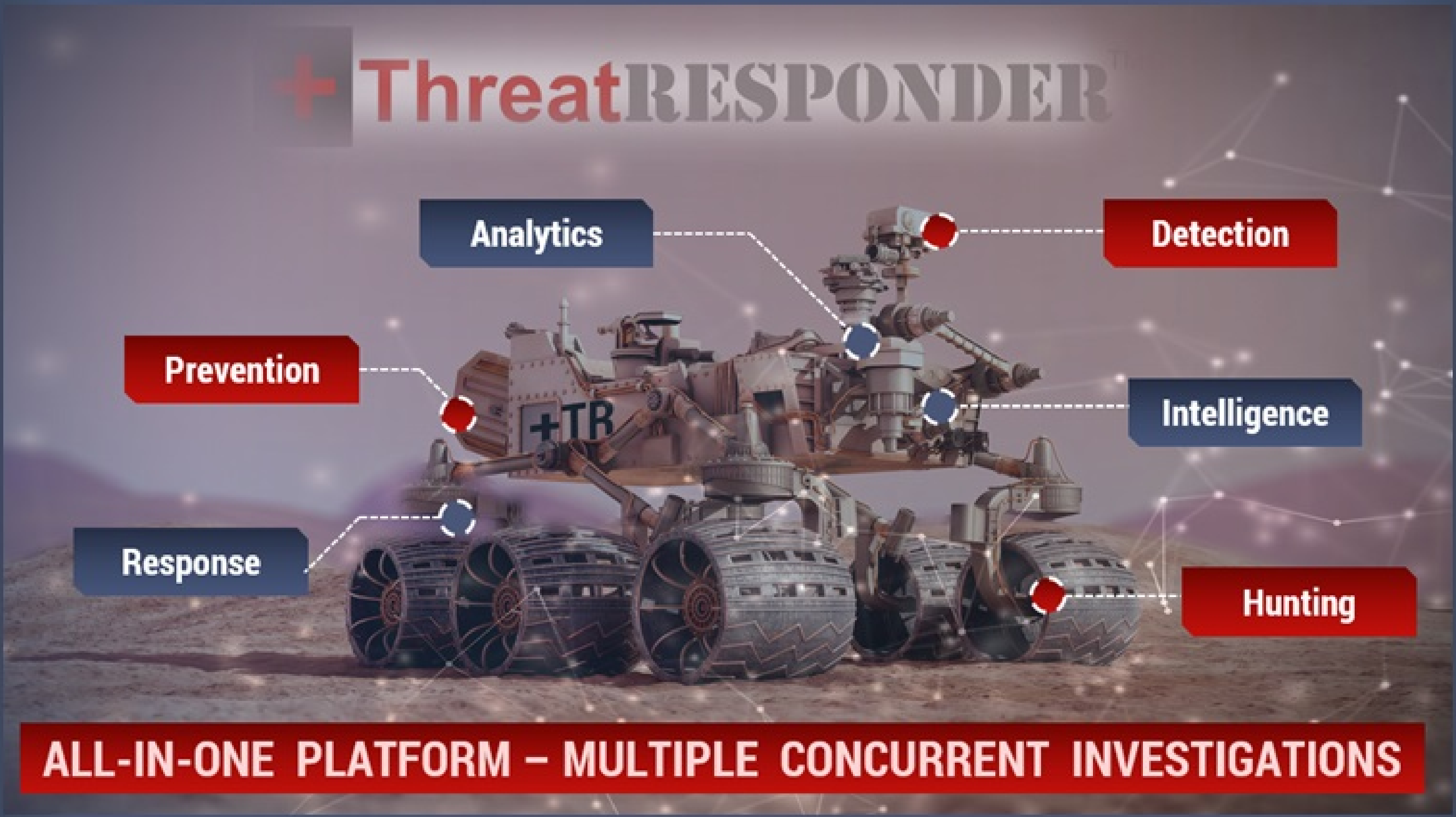
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-07-07, 5 days ago. The vendor is given until 2021-11-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Are You…

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

Sponsored Products

CSI Linux: Current Version: 2021.2

Download here.

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

CSI Linux 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:

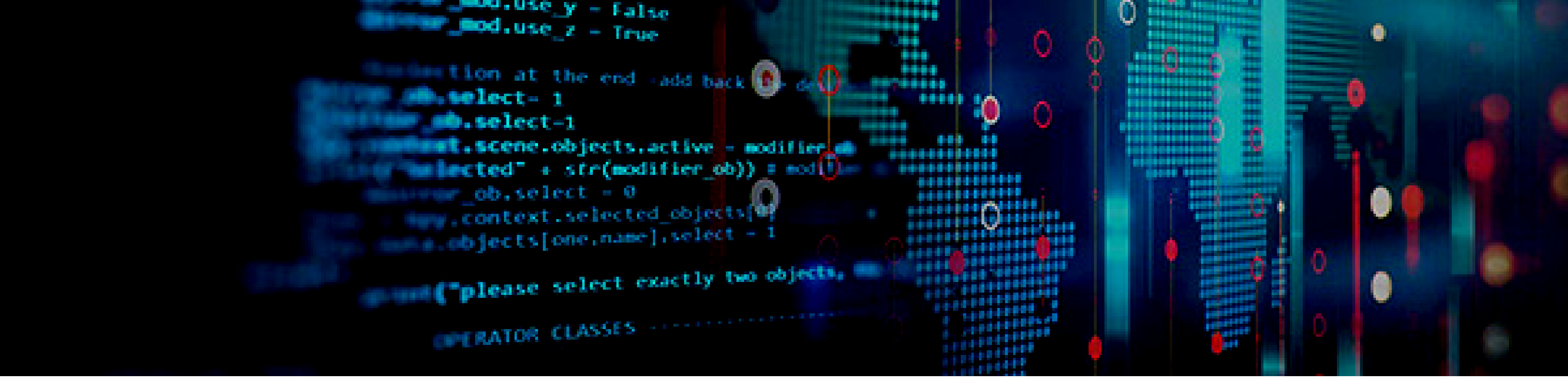
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

Cyber Secrets

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

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

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

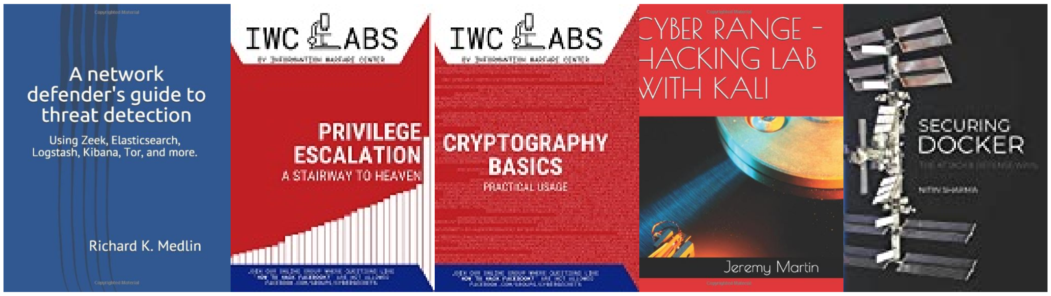


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP