Jun-21-21

# 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

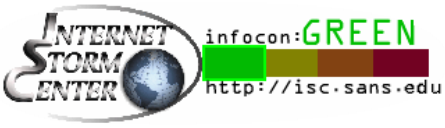
ARGOS
APPLIED INTELLIGENCE


## June 21, 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*

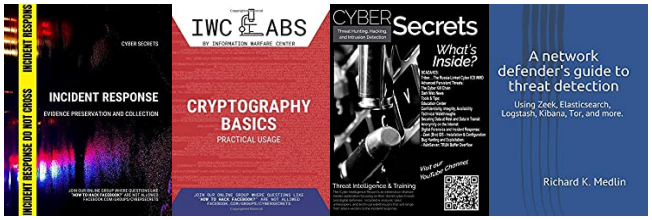


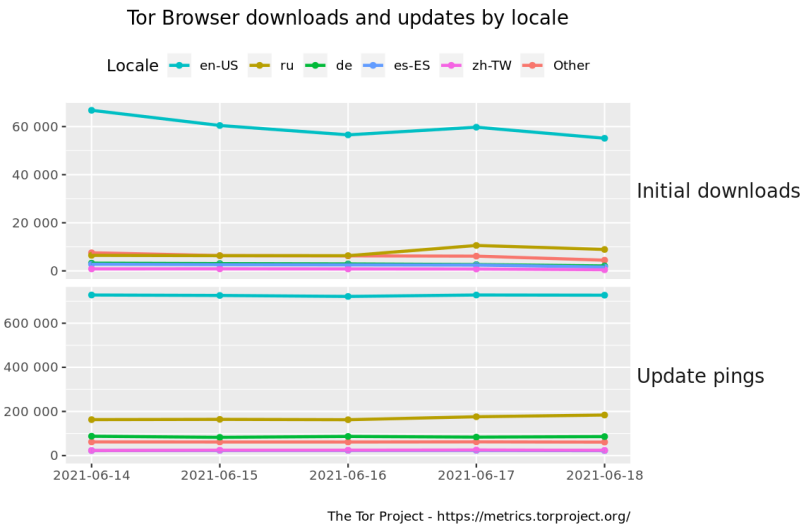

The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

## Other IWC Publications

*Cyber Secrets books and ebook series can be found on Amazon.com at.* [amzn.to/2UuIG9B](amzn.to/2UuIG9B)

Cyber Secrets was originally a video series and is on both [YouTube](YouTube).




## Interesting News

* [Subscribe to this OSINT resource to recieve it in your inbox.](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](Cyber Secrets Facebook group here).

*** CSI Linux 2021.2 has just been released!  Download today! [csilinux.com](csilinux.com)

# Index of Sections


**Packet Storm Security**

* Ten-Year Hacktivisit Fugitive Commander X Arrested In Mexico
* Sideloading Apps Would Destroy iOS Security And Privacy
* Why Cyber Gangs Won't Worry About US-Russia Talks
* Millions Of Connected Cameras Open To Eavesdropping
* Digital Ad Industry Accused Of Huge Data Breach
* Peloton Bike+ Was Vulnerable To Remote Hacking, Researchers Find
* Police Bust Major Ransomware Gang Cl0p
* Nasty Linux systemd Root Level Security Bug Revealed And Patched
* Facebook Awards $30,000 Bounty For Exploit Exposing Private Instagram Content
* Digital Artists Targeted In RedLine Infostealer Campaign
* Utilities Concerningly At Risk From Active Exploits
* Apple Hurries Patches For Safari Bugs Under Active Attack
* Critical Remote Code Execution Flaw In Thousands Of VMWare vCenter Servers Remains Unpatched
* TimeCache Aims To Block Side-Channel Cache Attacks
* Volkswagen, Audi Disclose Data Breach Impacting Over 3.3 Million Customers, Interested Buyers
* WhatsApp Boss Decries Attacks On Encryption As Orwellian
* Irish Police To Be Given Powers Over Passwords
* Russia Told To Tackle Cyber Criminals Operating From Within
* How Hackers Used Slack To Break Into EA Games
* STEM Audio Table Rife With Business Threatening Bugs
* McDonald's Operations In South Korea And Taiwan Hit By Data Breach
* US Retailer Carter Leaks PII With URL Shortener
* Hackers Force Iowa College To Cancel Classes For Four Days
* Cops Are Using Facebook To Target Pipeline Protest Leaders
* Intel Plugs 29 Holes In CPUs, Bluetooth, Security

**Krebs on Security**


**Dark Reading**

* Did Companies Fail to Disclose Being Affected by SolarWinds Breach?
* Software-Container Supply Chain Sees Spike in Attacks
* Data Leaked in Fertility Clinic Ransomware Attack
* Baltimore County Public Schools' Ransomware Recovery Tops $8M
* Fintech at SaaS Speed
* Are Ransomware Attacks the New Pandemic?
* Attackers Find New Way to Exploit Google Docs for Phishing
* This Week in Database Leaks: Cognyte, CVS, Wegmans
* Accidental Insider Leaks Prove Major Source of Risk
* 11 Security Certifications to Seek Out This Summer
* 4 Habits of Highly Effective Security Operators
* Data Breaches Surge in Food & Beverage, Other Industries
* One in Five Manufacturing Firms Targeted by Cyberattacks
* Carnival Cruise Line Reports Security Breach
* Google Launches SLSA, a New Framework for Supply Chain Integrity
* Cyberattacks Are Tailored to Employees ... Why Isn't Security Training?
* Mission Critical: What Really Matters in a Cybersecurity Incident
* Ukraine Police Disrupt Cl0p Ransomware Operation
* Ransomware Operators' Strategies Evolve as Attacks Rise
* Biden Tells Putin Critical Infrastructure Sectors 'Off Limits' to Russian Hacking

**The Hacker News**

* 5 Critical Steps to Recover From a Ransomware Attack
* DroidMorph Shows Popular Android Antivirus Fail to Detect Cloned Malicious Apps
* Beware! Connecting to This Wireless Network Can Break Your iPhone's Wi-Fi Feature
* North Korea Exploited VPN Flaw to Hack South's Nuclear Research Institute
* Cyber espionage by Chinese hackers in neighbouring nations is on the rise
* Russia bans VyprVPN, Opera VPN services for not complying with blacklist request
* Google Releases New Framework to Prevent Software Supply Chain Attacks
* [eBook] 7 Signs You Might Need a New Detection and Response Tool
* Update‌ ‌Your Chrome Browser to Patch Yet Another 0-Day Exploit‌ed ‌in‌-the&
* Molerats Hackers Return With New Attacks Targeting Middle Eastern Governments
* A New Spyware is Targeting Telegram and Psiphon VPN Users in Iran
* Strengthen Your Password Policy With GDPR Compliance
* Researchers Uncover 'Process Ghosting' - A New Malware Evasion Technique
* Ukraine Police Arrest Cyber Criminals Behind Clop Ransomware Attacks
* Malware Attack on South Korean Entities Was Work of Andariel Group


**Security Week**

* Ransomware Gangs Get Paid Off as Officials Struggle for Fix
* Attacks Against Container Infrastructures Increasing, Including Supply Chain Attacks
* Cybersecurity M&A Roundup for June 14-20, 2021
* Vermont Hospital Still Calculating Cost of Ransomware Attack
* South Korean Atomic Energy Research Institute Confirms Cyberattack
* Water Sector Security Report Released Just as Another Water Plant Hack Comes to Light
* Hit by a Ransomware Attack? Your Payment May be Deductible
* Major Cyberattack on Poland Came from Russian Territory: Kaczynski
* Vulnerabilities in Open Design Alliance SDK Impact Siemens, Other Vendors
* Researcher Finds Several Vulnerabilities in Cisco Small Business Switches
* NSA Releases Guidance for Securing Enterprise Communication Systems
* Cruise Giant Carnival Says Customers Affected by Breach
* Akamai Blames Outage on DDoS Protection Service
* Google Confirms Sixth Zero-Day Chrome Attack in 2021
* Google Intros SLSA Framework to Enforce Supply Chain Integrity
* UK Law Firm Gateley Discloses Data Breach
* Biden Sets Red Line for Putin Over Ransomware Attacks
* Russian Accused of Helping Kelihos Malware Evade Detection Convicted in U.S.
* How to Plan Your M&A Security Strategy
* Industrial Cybersecurity Firm Claroty Raises $140 Million in Series D Funding
* Security Flaw Found in 2G Mobile Data Encryption Standard
* Ukraine Police Seize Cash in Raids on Major Ransomware Gang
* Kaspersky Details Iranian Domestic Cyber-Surveillance Operation
* Apple Warns EU Law 'Risks Destroying iPhone Security'

**Infosecurity Magazine**

* California Cops Launch ALPR Transparency Portal
* Ohio Medicaid Provider Suffers Data Breach
* Finger Scanning Costs Six Flags $36m
* UK Parliamentary Staffers Lost 96 Devices in Past Two Years
* Amazon Prime Day - Beware of Phishing Deluge, Experts Warn
* Over 30,000 Fertility Clinic Patients Hit by Ransomware Data Breach
* Nuclear Research Institute Breached by Suspected North Korean Hackers
* Texan Admits Data Center Bomb Plot
* New Jersey Councilor Charged with Cyber-harassment
* Colorado Passes New Privacy Act
* Google Spices Up Supply Chain Security with SLSA Framework
* Infosecurity Europe 2021 Postpones Live Event


**KnowBe4 Security Awareness Training Blog RSS Feed**

* KnowBe4 Makes eSecurity Planet's Best Security Awareness Training for Employees 2021 List
* Credential Stuffing in the Travel and Retail Sectors
* CyberheistNews Vol 11 #24 [Scam of the Week] If Your Users Are Amazon Shoppers, Heed This Prime Day P
* Understanding Ransomware's True Costs
* [Heads Up] If You're an Amazon Prime Shopper, Heed This Prime Day Phishing Alert
* Bad Security Habits During the Pandemic
* Ragnar Locker Ransomware Finds Its Next Victim in Taiwan Computer Memory Manufacturer ADATA
* The Number of Phishing Websites Hits an All-Time High Reaching Nearly 350% Growth
* Tax Organizations Need to Focus on Cybersecurity
* New BEC Phishing Attack Steals Office 365 Credentials and Bypasses MFA

**ISC2.org Blog**

* U.S. Government Equates Threat of Ransomware with Terrorism | #RansomwareWeek
* Business Continuity - The Light in a Time of Darkness
* CCSP: The Best Way to Achieve Cloud Security
* What's Your Fail-Safe Posture? Before You Learn How to Fly, Learn How to Fall
* Best Practices and Techniques for Pseudonymization

**HackRead**

* Prominent defibrillator management tool exposed to remote attacks
* Vulnerability exposed Peloton bike, treadmil to malware attacks
* Cybersecurity firm exposes 5 billion data breach records
* Baby clothing giant Carter's exposed trove of shoppers data
* Threat actors using Google Docs exploit to spread phishing links
* N Korean hackers used VPN flaws to breach S Korean atomic agency
* Watch out Android users as Joker malware is back on Play Store

**Koddos**

* Prominent defibrillator management tool exposed to remote attacks
* Vulnerability exposed Peloton bike, treadmil to malware attacks
* Cybersecurity firm exposes 5 billion data breach records
* Baby clothing giant Carter's exposed trove of shoppers data
* Threat actors using Google Docs exploit to spread phishing links
* N Korean hackers used VPN flaws to breach S Korean atomic agency
* Watch out Android users as Joker malware is back on Play Store


**Naked Security**

* Can *YOU* blow a PC speaker using only a Linux kernel driver?
* S3 Ep37: Quantum crypto, refunding Bitcoins, and Alpaca problems [Podcast]
* How to hack a bicycle - Peloton Bike+ rooting bug patched
* Clop ransomware suspects busted in Ukraine, money and motors seized
* "Face of Anonymous" suspect deported from Mexico to face US hacking charges
* ALPACA - the wacky TLS security vulnerability with a funky name
* S3 Ep36: Trickbot coder busted, passwords cracked, and breaches judged [Podcast]
* Chrome zero-day, hot on the heels of Microsoft's IE zero-day. Patch now!
* How could the FBI recover BTC from Colonial's ransomware payment?
* Latvian woman charged with writing malware for the Trickbot Group

**Threat Post**

* Wegmans Exposes Customer Data in Misconfigured Databases
* Bugs in NVIDIA's Jetson Chipset Opens Door to DoS Attacks, Data Theft
* Embryology Data Breach Follows Fertility Clinic Ransomware Hit
* Agent Tesla RAT Returns in COVID-19 Vax Phish
* iPhone Wi-Fi Crushed by Weird Network
* What's Making Your Company a Ransomware Sitting Duck
* Carnival Cruise Cyber-Torpedoed by Cyberattack
* Insider Versus Outsider: Navigating Top Data Loss Threats
* 'Oddball' Malware Blocks Access to Pirated Software
* Faux 'DarkSide' Gang Takes Aim at Global Energy, Food Sectors

**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


**IBM Security Intelligence**

* The OSI Model and You Part 5: Stopping Threats at the OSI Session Layer
* Data is Wealth: Data Security is Wealth Protection
* The Art and Strategy of Becoming More Cyber Resilient
* Why a Phishing Attack Is Still Profitable - And How To Stop One
* The Hottest Cybersecurity Must-Reads for the Busy Security Practitioner
* Learning the Building Blocks for Your CIAM Framework Part 3: Manage
* Surge of New Digital Accounts During the Pandemic Leads to Lingering Security Side Effects
* Cybersecurity Certifications: Take Your Career to the Next Level
* The OSI Model and You Part 4: Stopping Threats at the OSI Transport Layer
* Educating the Educators: Protecting Student Data

**InfoWorld**

* What's new in Microsoft .NET 6
* 5 AI startups leading MLops
* The wrong way to think about IT
* 3 signs of an overengineered enterprise cloud solution
* Eclipse launches group to shepherd popular Java IDE
* Why developers should use Apache Pulsar
* How to use Razor View Engine in ASP.NET Core MVC
* What is Azure Confidential Ledger?
* Get started with Anaconda Python
* Why you need a data integration platform

**C4ISRNET - Media for the Intelligence Age Military**

* FAA and Air Force sign agreement on commercial launches from Space Force bases
* Pentagon to reveal JEDI cloud computing contract's future in coming weeks
* NATO soliciting industry to beef up internal cyber defenses
* Space Force launches fifth GPS III satellite for more secure positioning
* Verizon wins $495 million contract for DoD research network
* You go to war with the data you have: next-generation AI for national security
* Even generals must learn new skills in tech-dominated special operations future
* US Air Force attempts to awaken spectrum ops after decades of waning electromagnetic warfare
* The Space Force wants to use directed-energy systems for space superiority
* Space Force's new delta organizations will help the service keep up with growing launch cadence

# The Hacker Corner

**Conferences**

* 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)
* How To Sponsor Cybersecurity Conferences

**Google Zero Day Project**

* Fuzzing iOS code on macOS at native speed
* Designing sockfuzzer, a network syscall fuzzer for XNU

**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.

* CTFZone 2021
* Hack-A-Sat 2 Qualifiers
* Hacky Holidays - Space Race
* CyberThreatForce CTF | 2021
* 0CTF/TCTF 2021 Quals
* redpwnCTF 2021
* ENOWARS 5
* Google Capture The Flag 2021
* RuCTF 2021
* ImaginaryCTF 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

* Hashcat Advanced Password Recovery 6.2.2 Source Code
* Hashcat Advanced Password Recovery 6.2.2 Binary Release
* TOR Virtual Network Tunneling Tool 0.4.6.5
* tcpdump 4.99.1
* nfstream 6.3.2
* GNU Privacy Guard 2.2.28
* Petalus 1.0.0
* SQLMAP - Automatic SQL Injection Tool 1.5.6
* Flawfinder 2.0.17
* Wireshark Analyzer 3.4.6

### Kali Linux Tutorials

* defenselessV1 : Just Another Vulnerable Web Application
* TChopper : Conduct Lateral Movement Attack By Leveraging Unfiltered Services Display Name To Smuggle
* ColdFire : Golang Malware Development Library
* Neurax : A Framework For Constructing Self-Spreading Binaries
* Nebula : Cloud C2 Framework, Which At The Moment Offers Reconnaissance, Enumeration, Exploitation, Po
* Bn-Uefi-Helper : Helper Plugin For Analyzing UEFI Firmware
* Penglab : Abuse Of Google Colab For Cracking Hashes
* RedWarden : Flexible CobaltStrike Malleable Redirector
* Kaiju : A Binary Analysis Framework Extension For The Ghidra Software Reverse Engineering Suite
* Link : A Command And Control Framework Written In Rust

### GBHackers Analysis

* How to Protect Your Email From Hacking?
* EA Sports Hacked - Hackers Stolen Source Code With 780 GB of Data
* Russian Hacker Jailed for Running a Darkweb Market Place that Sells Stolen Credit card Details
* Russian Hacker Group Nobelium Attack U.S Gov Agencies By Targeting 3,000 Email Accounts
* Hackers Exploited Fortinet Vulnerabilities to Gain Access of a U.S. Municipal Government Webserver

# Weekly Cyber Security Video and Podcasts

**SANS DFIR**

* SANS Threat Analysis Rundown
* Mobile Validation - Working together for the Common Good
* FOR500: Windows Forensic Analysis course: What to expect
* Why take the FOR500: Windows Forensic Analysis course

**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**

* OMG: This Malicious Crypto Wallet Steals Bitcoin
* HakByte: Remotely Track Devices over Wi-Fi with the ESP Bug [AUDIO-FIXED]
* 7 Year Old Linux Flaw Newly Discovered - ThreatWire

**The PC Security Channel [TPSC]**

* Windows Defender vs Malware in 2021
* Darkside Ransomware: The threat behind the state of emergency in the US

**Eli the Computer Guy**

* "Easy" SMS with Twilio (Add SMS to Your Coding Projects)
* "Easy" Computer Vision with Azure and AWS
* DNS for Cybersecurity
* Apply to Jobs You are UNDER QUALIFIED for - Tech Career Advice

**Security Now**

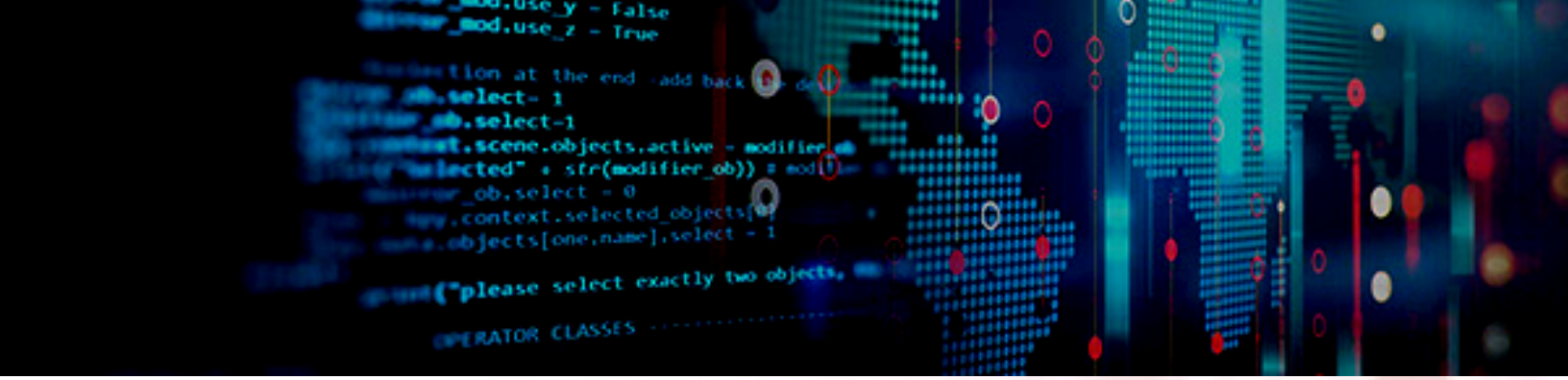
* TLS Confusion Attacks - TikTok Privacy, iOS 14.5 Tracking Permission, Industry-Wide Patch Tuesday
* Extrinsic Password Managers - Great CyberSecurity Awakening of 2021, NAT vs IPv6, Tavis Ormandy

**Troy Hunt**

* Weekly Update 248

**Intel Techniques: The Privacy, Security, & OSINT Show**

* 221-Anonymous Mobile Devices
* 220-Privacy, Security, & OSINT Potluck



## 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

* 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
* TrickBot: Get to Know the Malware That Refuses to Be Killed
* SolarWinds: Illuminating the Hidden Patterns That Advance the Story
* For Threat Actors, Shadow Z118 is the Kit That Keeps on Giving

## FireEye

* Metasploit Wrap-Up
* Rapid7 Releases New Industry Cyber-Exposure Report (ICER): Deutsche Börse Prime Standard
* Attack Surface Analysis Part 2: Penetration Testing
* Automated remediation level 1: Lock down fundamentals
* Metasploit Wrap-Up
* Attack Surface Analysis Part 1: Vulnerability Scanning
* [Security Nation] Jeff Man on Mapping the MITRE ATT&CK Framework Against PCI
* Akkadian Provisioning Manager Multiple Vulnerabilities Disclosure (Fixed)
* Patch Tuesday - June 2021
* Action! Start putting automation into practice.


# Proof of Concept (PoC) & Exploits

### Packet Storm Security

* Windows Kerberos AppContainer Enterprise Authentication Capability Bypass
* Microsoft SharePoint Unsafe Control And ViewState Remote Code Execution
* Cisco HyperFlex HX Data Platform File Upload / Remote Code Execution
* Dup Scout 13.5.28 Unquoted Service Path
* Trojan.Win32.Alien.erf Buffer Overflow
* Unified Office Total Connect Now 1.0 SQL Injection
* Samsung NPU npu_session_format Out-Of-Bounds Write
* VeryFitPro 3.2.8 Insecure Transit
* VX Search 13.5.28 Unquoted Service Path
* Zoho ManageEngine ServiceDesk Plus 9.4 User Enumeration
* Trojan.Win32.Alien.erf Denial Of Service
* Workspace ONE Intelligent Hub 20.3.8.0 Unquoted Service Path
* Online Shopping Portal 3.1 Shell Upload
* Email-Worm.Win32.Kipis.a Code Execution
* OpenEMR 5.0.1.3 Authentication Bypass
* Sync Breeze 13.6.18 Sync Breeze 13.6.18 Unquoted Service Path
* Disk Savvy 13.6.14 Unquoted Service Path
* Cotonti Siena 0.9.19 Cross Site Scripting
* CKEditor 3 Server-Side Request Forgery
* Teachers Record Management System 1.0 SQL Injection
* Teachers Record Management System 1.0 Cross Site Scripting
* Disk Sorter Server 13.6.12 Unquoted Service Path
* DiskPulse 13.6.14 Unquoted Service Path
* SAP Netweaver JAVA 7.50 Missing Authorization
* Client Management System 1.1 SQL Injection

### CXSecurity

* Post-it 5.0.1 Denial of Service (PoC)
* Sticky Notes Widget Version 3.0.6 Denial of Service (PoC)
* memono Notepad 4.2 Denial Of Service
* Sticky Notes Widget 3.0.6 Denial Of Service
* Microsoft SharePoint Server 16.0.10372.20060 Server-Side Request Forgery
* Ability FTP Server 2.34 Denial Of Service
* FreeFloat FTP Server 1.0 Denial Of Service


# Proof of Concept (PoC) & Exploits

**Exploit Database**

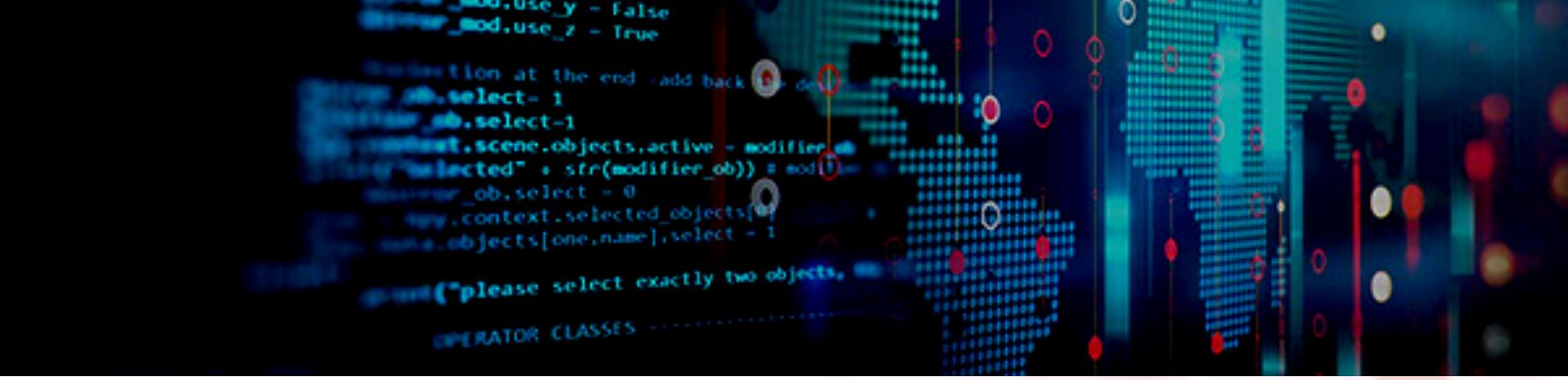
* [local] Remote Mouse GUI 3.008 - Local Privilege Escalation
* [webapps] Customer Relationship Management System (CRM) 1.0 - Remote Code Execution
* [local] Lexmark Printer Software G2 Installation Package 1.8.0.0 - 'LM__bdsvc' Unquoted Service Path
* [webapps] Simple CRM 3.0 - 'name' Stored Cross site scripting (XSS)
* [webapps] Simple CRM 3.0 - 'Change user information' Cross-Site Request Forgery (CSRF)
* [webapps] Websvn 2.6.0 - Remote Code Execution (Unauthenticated)
* [local] iFunbox 4.2 - 'Apple Mobile Device Service' Unquoted Service Path
* [remote] Solaris SunSSH 11.0 x86 - libpam Remote Root (3)
* [local] Wise Care 365 5.6.7.568 - 'WiseBootAssistant' Unquoted Service Path
* [webapps] OpenEMR 5.0.1.7 - 'fileName' Path Traversal (Authenticated)
* [webapps] Node.JS - 'node-serialize' Remote Code Execution (3)
* [remote] Dlink DSL2750U - 'Reboot' Command Injection
* [webapps] ICE Hrm 29.0.0.OS - 'xml upload' Stored Cross-Site Scripting (XSS)
* [webapps] ICE Hrm 29.0.0.OS - 'Account Takeover' Cross-Site Request Forgery (CSRF)
* [webapps] ICE Hrm 29.0.0.OS - 'Account Takeover' Cross-Site Scripting and Session Fixation
* [webapps] Online Shopping Portal 3.1 - Remote Code Execution (Unauthenticated)
* [local] Workspace ONE Intelligent Hub 20.3.8.0 - 'VMware Hub Health Monitoring Service' Unquoted Serv
* [webapps] Zoho ManageEngine ServiceDesk Plus MSP 9.4 - User Enumeration
* [local] VX Search 13.5.28 - 'Multiple' Unquoted Service Path
* [local] Dup Scout 13.5.28 - 'Multiple' Unquoted Service Path
* [local] Disk Savvy 13.6.14 - 'Multiple' Unquoted Service Path
* [local] Sync Breeze 13.6.18 - 'Multiple' Unquoted Service Path
* [webapps] Unified Office Total Connect Now 1.0 - 'data' SQL Injection
* [webapps] CKEditor 3 - Server-Side Request Forgery (SSRF)

**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*

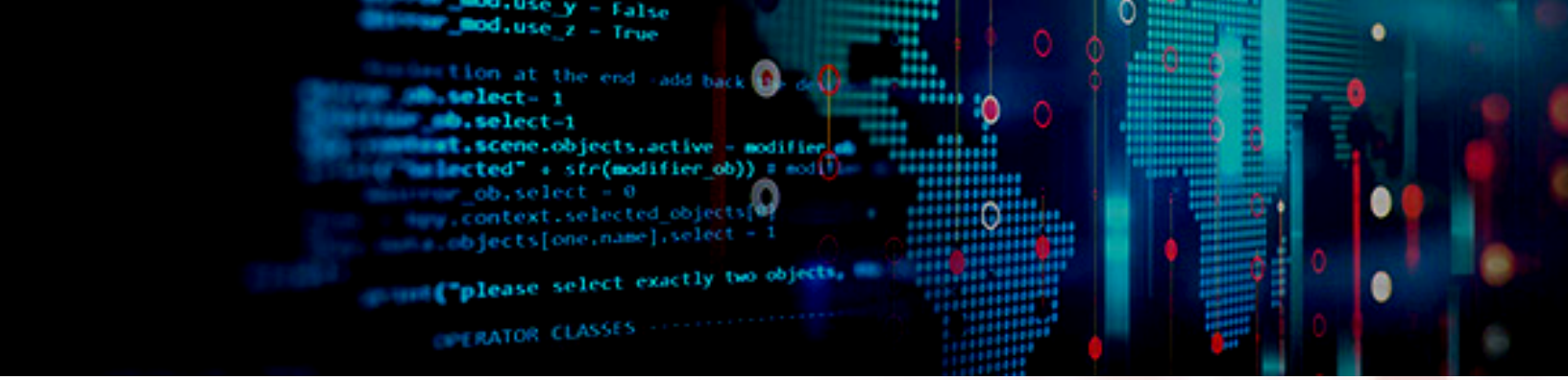
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit".  It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



# Latest Hacked Websites

**Published on Zone-h.org**

http://bursasulamabirligi.gov.tr/index.php
http://bursasulamabirligi.gov.tr/index.php notified by B3g0k[Kurdish Hacker]
http://diyarbakirakb.gov.tr
http://diyarbakirakb.gov.tr notified by B3g0k[Kurdish Hacker]
http://lpg1.go.th/hi.htm
http://lpg1.go.th/hi.htm notified by YIIX103
https://lebongkab.go.id/by_Panataran.html
https://lebongkab.go.id/by_Panataran.html notified by Panataran
http://herbaryum.tagem.gov.tr
http://herbaryum.tagem.gov.tr notified by B3g0k[Kurdish Hacker]
https://dumaikota.go.id/google3e4747cac4271855.html
https://dumaikota.go.id/google3e4747cac4271855.html notified by Mc'Sl0vv
http://wiangkarn.go.th/pun10.html
http://wiangkarn.go.th/pun10.html notified by Jakarta Blackhat
http://dongichan.go.th/pun10.html
http://dongichan.go.th/pun10.html notified by Jakarta Blackhat
http://nasum.go.th/pun10.html
http://nasum.go.th/pun10.html notified by Jakarta Blackhat
http://panna.go.th/pun10.html
http://panna.go.th/pun10.html notified by Jakarta Blackhat
http://maelaluang.go.th/pun10.html
http://maelaluang.go.th/pun10.html notified by Jakarta Blackhat
http://changkerng.go.th/pun10.html
http://changkerng.go.th/pun10.html notified by Jakarta Blackhat
http://nasaklampang.go.th/pun10.html
http://nasaklampang.go.th/pun10.html notified by Jakarta Blackhat
http://maesuad.go.th/pun10.html
http://maesuad.go.th/pun10.html notified by Jakarta Blackhat
http://yangkham.go.th/pun10.html
http://yangkham.go.th/pun10.html notified by Jakarta Blackhat
http://phocaipiboon.go.th/pun10.html
http://phocaipiboon.go.th/pun10.html notified by Jakarta Blackhat
http://bankhon.go.th/pun10.html
http://bankhon.go.th/pun10.html notified by Jakarta Blackhat



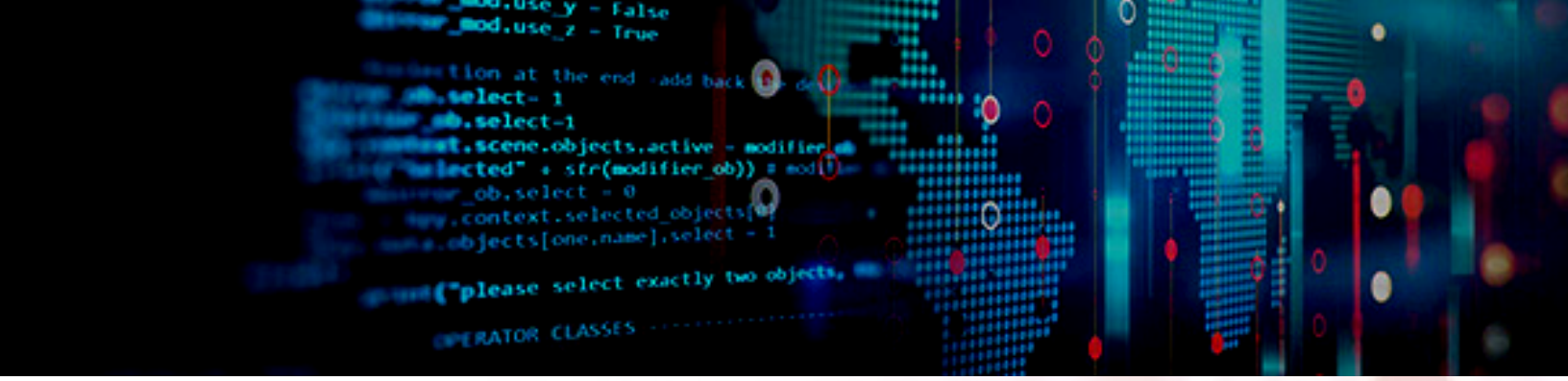
# Dark Web News

**Darknet Live**

Connecticut Man Admits Selling Counterfeit Oxycodone
A Connecticut man admitted participating in the production and distribution of counterfeit oxycodone pills through the darkweb. (via darknetlive.com)
Austrian Man Arrested for Buying Drugs on the Darkweb
Authorities in Upper Austria arrested a man suspected of importing drugs purchased through the darkweb. (via darknetlive.com)
OM: Sentence an IS-Supporting Vendor to Eight Years
The Dutch Public Prosecution Service demanded an eight year prison sentence for an IS-supporting darkweb drug vendor. (via darknetlive.com)
Canadian Man Bought a Glock from an Undercover U.S. Fed
A Canadian man was sentenced to prison for purchasing a Glock 19 from an undercover fed on the darkweb. (via darknetlive.com)

**Dark Web Link**

Crypto Coin Exchanges: What Is Happening Right Now?
The majority of the top cryptocurrencies are lately trading in red, with Ethereum (ETH) and Bitcoin (BTC) down around 3% in the past 24 hours. The global crypto market capitalization is currently at $1.51 trillion, which is a sharp decline of 3.40% over the previous day. The world's largest cryptocurrency, Bitcoin, has dropped as much [...] The post Crypto Coin Exchanges: What Is Happening Right Now? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Clop Ransomware Gang Oozes Out Cash In The Ukrainian Raid
The Ukrainian cops have conducted almost two dozen raids that targeted the alleged associates of the Clop ransomware gang. The ransomware gang is a Russian-speaking group that has been blamed for a half-billion dollars cyber attack as well as extortion in the United States and South Korea.  On Wednesday, a police statement mentioned that 21 [...] The post Clop Ransomware Gang Oozes Out Cash In The Ukrainian Raid appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Dark Web Carding: All Information That You Need To Know
The Dark Web is the haven for illegal activities and carding is no different. Massive data breaches have resulted in the spike of dark web carding (especially credit card fraud) and related activities causing loss to both individuals and organizations of varied sizes. The dark web skimmers are employing new techniques to hack the credit [...] The post Dark Web Carding: All Information That You Need To Know appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



# Advisories

**US-Cert Alerts & bulletins**

* Google Releases Security Updates for Chrome
* Cisco Releases Security Updates for Multiple Products
* Apple Releases Security Updates for iOS 12.5.4
* CISA Releases Advisory on ZOLL Defibrillator Dashboard
* Google Releases  Security Updates for Chrome
* CISA Addresses the Rise in Ransomware Targeting Operational Technology Assets
* SAP Releases June 2021 Security Updates
* Adobe Releases Security Updates for Multiple Products
* 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 June 14, 2021
* Vulnerability Summary for the Week of June 7, 2021

**Zero Day Initiative Advisories**

ZDI-CAN-14112: Fatek 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 'xina1i' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14039: Fatek 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 'xina1i' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14066: Oracle
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 'Anonymous' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-13818: TeamViewer
A CVSS score 3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by '@Kharosx0' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14186: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14183: OpenText
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend

Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14184: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14185: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14180: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14182: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14167: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14166: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14179: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14181: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14169: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14178: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14177: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14172: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14162: ESET

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14170: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14173: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14171: OpenText

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14165: OpenText

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 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-14174: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-06-18, 3 days ago. The vendor is given until 2021-10-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

**Packet Storm Security - Latest Advisories**

Red Hat Security Advisory 2021-2479-01

Red Hat Security Advisory 2021-2479-01 - Red Hat OpenShift Container Storage is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Container Storage is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform. Issues addressed include a cross site scripting vulnerability.

Ubuntu Security Notice USN-4990-1

Ubuntu Security Notice 4990-1 - It was discovered that Nettle incorrectly handled RSA decryption. A remote attacker could possibly use this issue to cause Nettle to crash, resulting in a denial of service. It was discovered that Nettle incorrectly handled certain padding oracles. A remote attacker could possibly use this issue to perform a variant of the Bleichenbacher attack. This issue only affected Ubuntu 18.04 LTS. Various other issues were also addressed.

Red Hat Security Advisory 2021-2476-01

Red Hat Security Advisory 2021-2476-01 - Red Hat Decision Manager is an open source decision management platform that combines business rules management, complex event processing, Decision Model & Notation execution, and Business Optimizer for solving planning problems. It automates business decisions and makes that logic available to the entire business. This release of Red Hat Decision Manager 7.11.0 serves as an update to Red Hat Decision Manager 7.10.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include XML injection, code execution, denial of service, and server-side request forgery vulnerabilities.

Trojan.Win32.Alien.erf Directory Traversal

Trojan.Win32.Alien.erf malware suffers from a directory traversal vulnerability.

Red Hat Security Advisory 2021-2475-01

Red Hat Security Advisory 2021-2475-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This release of Red Hat Process Automation Manager 7.11.0 serves as an update to Red Hat Process Automation Manager 7.10.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include XML injection, code execution, denial of service, and server-side request forgery vulnerabilities.

Red Hat Security Advisory 2021-2472-01

Red Hat Security Advisory 2021-2472-01 - This release adds the new Apache HTTP Server 2.4.37 Service Pack 8 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Pack Apache Server 2.4.37 Service Pack 7 and includes bug fixes and enhancements. Issues addressed include null pointer and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2469-01

Red Hat Security Advisory 2021-2469-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-2471-01

Red Hat Security Advisory 2021-2471-01 - Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience. This release adds the new Apache HTTP Server 2.4.37 Service Pack 8 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Pack Apache Server 2.4.37 Service Pack 7 and includes bug fixes and enhancements. Issues addressed include null pointer and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-2467-01

Red Hat Security Advisory 2021-2467-01 - GLib provides the core application building blocks for libraries and applications written in C. It provides the core object system used in GNOME, the main loop implementation, and a large

set of utility functions for strings and common data structures. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2021-2461-01

Red Hat Security Advisory 2021-2461-01 - Red Hat Advanced Cluster Management for Kubernetes 2.2.4 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—with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs and security issues. Issues addressed include denial of service and integer overflow vulnerabilities.

Ubuntu Security Notice USN-4989-2

Ubuntu Security Notice 4989-2 - USN-4989-1 fixed several vulnerabilities in BlueZ. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that BlueZ incorrectly checked certain permissions when pairing. A local attacker could possibly use this issue to impersonate devices. Various other issues were also addressed.

Ubuntu Security Notice USN-4989-1

Ubuntu Security Notice 4989-1 - It was discovered that BlueZ incorrectly checked certain permissions when pairing. A local attacker could possibly use this issue to impersonate devices. Jay LV discovered that BlueZ incorrectly handled redundant disconnect MGMT events. A local attacker could use this issue to cause BlueZ to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. Various other issues were also addressed.

Red Hat Security Advisory 2021-2459-01

Red Hat Security Advisory 2021-2459-01 - GUPnP is an object-oriented open source framework for creating UPnP devices and control points, written in C using GObject and libsoup. The GUPnP API is intended to be easy to use, efficient and flexible.

Red Hat Security Advisory 2021-2456-01

Red Hat Security Advisory 2021-2456-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include denial of service and memory leak vulnerabilities.

Red Hat Security Advisory 2021-2445-01

Red Hat Security Advisory 2021-2445-01 - Red Hat Ceph Storage is a scalable, open, software-defined storage platform that combines the most stable version of the Ceph storage system with a Ceph management platform, deployment utilities, and support services. The ceph-ansible package provides Ansible playbooks for installing, maintaining, and upgrading Red Hat Ceph Storage. The tcmu-runner packages provide a service that handles the complexity of the LIO kernel target's userspace passthrough interface. It presents a C plugin API for extension modules that handle SCSI requests in ways not possible or suitable to be handled by LIO's in-kernel backstores. Issues addressed include cross site scripting and remote shell upload vulnerabilities.

SAP Solution Manager 7.20 Missing Authorization

Due to a missing authorization check in the SAP Solution Manager version 7.20 LM-SERVICE component, a remote authenticated attacker could be able to execute privileged actions in the affected system, including the execution of operating system commands.

Red Hat Security Advisory 2021-2439-01

Red Hat Security Advisory 2021-2439-01 - Open Liberty is a lightweight open framework for building fast and efficient cloud-native Java microservices. This release of Open Liberty 21.0.0.6 serves as a replacement for Open Liberty 21.0.0.3, and includes a security fix and enhancements. For specific information about this release, see links in the References section. Issues addressed include a cross site request forgery vulnerability.

Red Hat Security Advisory 2021-2417-01

Red Hat Security Advisory 2021-2417-01 - GUPnP is an object-oriented open source framework for creating UPnP devices and control points, written in C using GObject and libsoup. The GUPnP API is intended to be easy to use, efficient and flexible.

SAP XMII Remote Code Execution

By abusing a code injection vulnerability in SAP MII, an authenticated user with SAP XMII developer privileges could

execute code (including OS commands) on the server. Versions affected include XMII 15.1 lower than SP006 PL 000062, XMII 15.2 lower than SP003 PL 000038, XMII 15.3 lower than SP001 PL 000022, and XMII 15.4 lower than SP001 PL 000007.

SAP Solution Manager 7.2 Missing Authorization

Any authenticated user of the SAP Solution Manager version 7.2 is able to craft, upload, and execute EEM scripts on the SMDAgents affecting its integrity, confidentiality and availability.

SAP Solution Manager 7.2 File Disclosure / Denial Of Service

The End-User Experience Monitoring (EEM) application, part of the SAP Solution Manager version 7.2, is vulnerable to path traversal. As a consequence, an unauthorized attacker would be able to read sensitive OS files and affect the availability of the EEM robots connected to the SolMan.

SAP Wily Introscope Enterprise Default Hard-Coded Credentials

SAP Wily Introscope Enterprise versions 9.7, 10.1, 10.5, and 10.7 suffer from having default hard-coded credentials.

Red Hat Security Advisory 2021-2420-01

Red Hat Security Advisory 2021-2420-01 - The Dynamic Host Configuration Protocol is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network. Issues addressed include a buffer overflow vulnerability.

SAP Wily Introscope Enterprise OS Command Injection

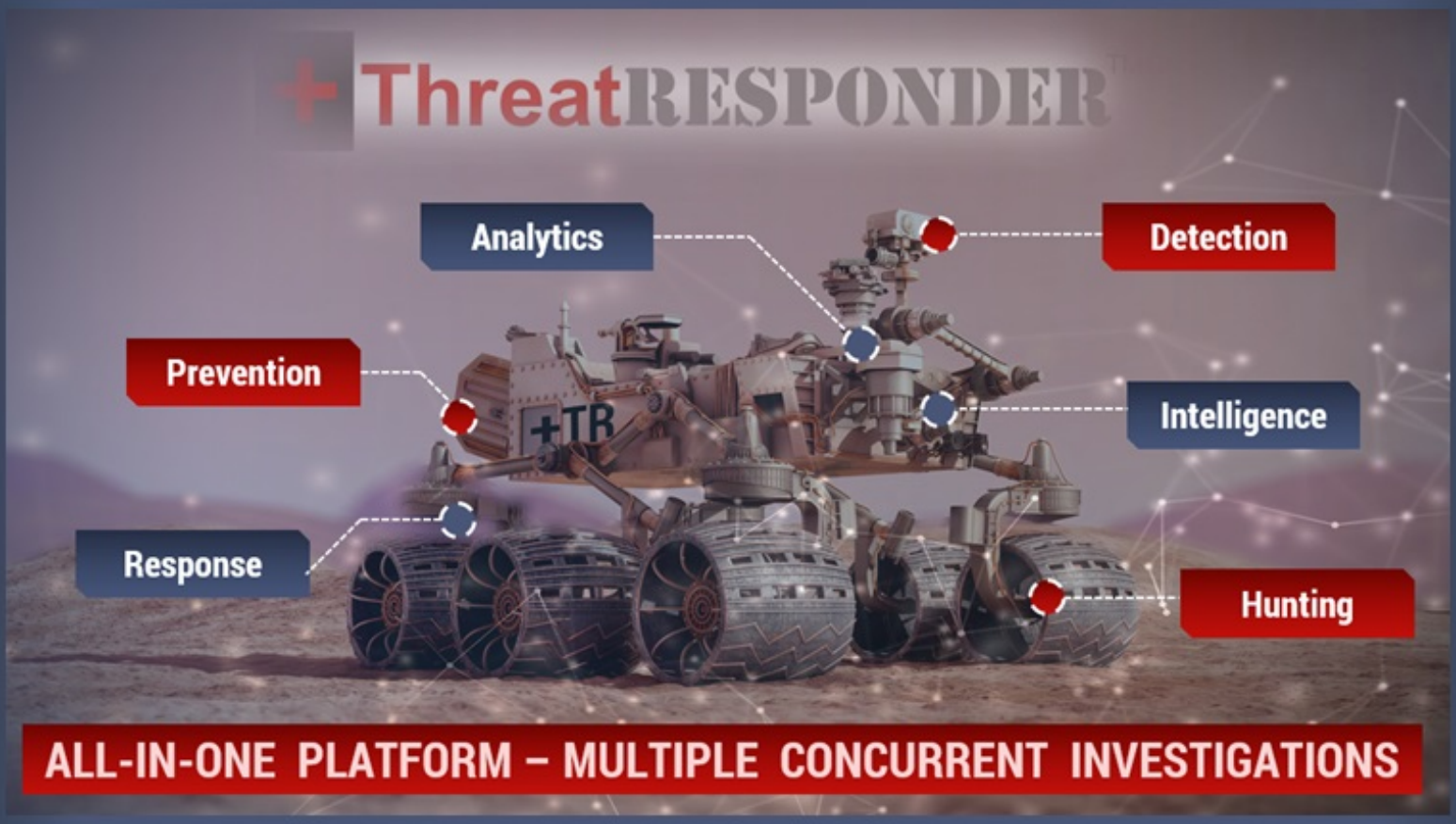
SAP Wily Introscope Enterprise versions 9.7, 10.1, 10.5, and 10.7 suffer from a command injection vulnerability.

## 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:**

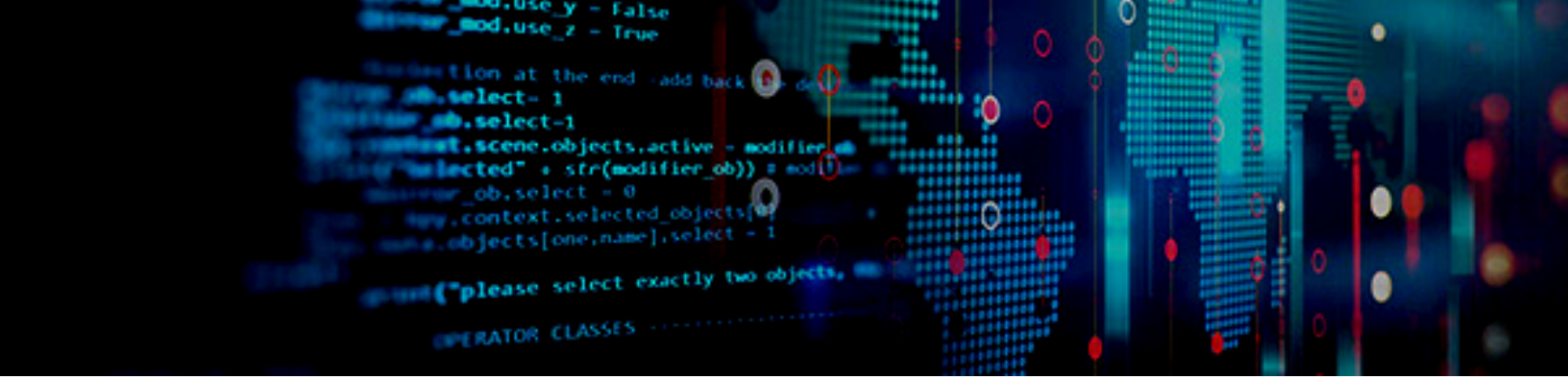
PDF: Installation Document (CSI Linux Virtual Appliance)
PDF: Installation Document (CSI Linux Bootable)
Many more Tutorials can be found HERE

**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

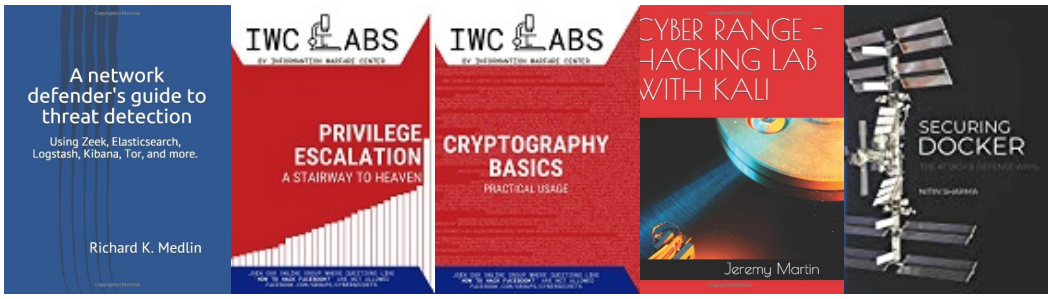


# The Cyber Secrets publications on Amazon

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