Feb-15-21

# CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

# CYBER WEEKLY AWARENESS REPORT

## February 15, 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*

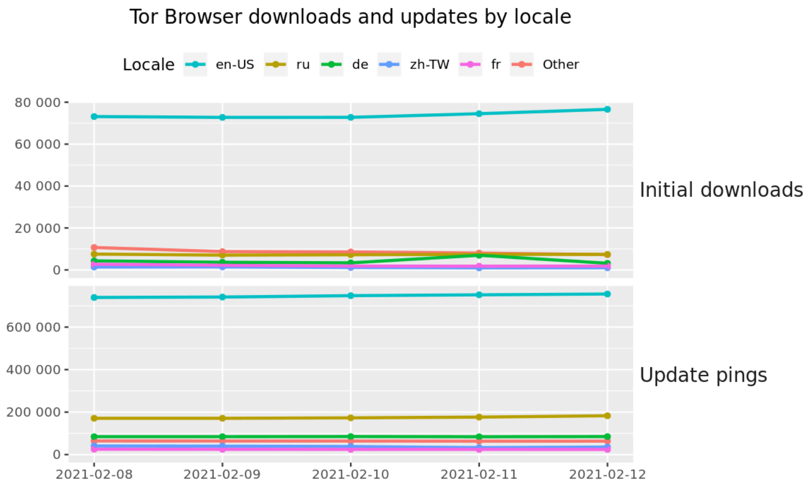
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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/2UulG9B]

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



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

## Interesting News

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

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

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

# Index of Sections

Current News

* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:

* Security Conferences
* Google Zero Day Project

Cyber Range Content

* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques

* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week

* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts

* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified

* CyberCrime-Tracker

Advisories

* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products

* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

# LATEST NEWS

### Packet Storm Security

* Singtel Suffers Zero-Day Cyberattack, Damage Unknown
* Egregor Ransomware Operators Arrested In Ukraine
* mHealth Apps Expose Millions To Cyberattacks
* A Windows Defender Vuln Lurked Undetected For 12 Years
* Brazil Probes Data Leak Of 102 Million Consumers
* Military, Nuclear Entities Under Target By Novel Android Malware
* Pre-Valentine's Day Malware Attack Mimics Flower, Lingerie Stores
* Microsoft Is Seeing A Big Spike In Web Shell Use
* Hacker Sets Alleged Auction For Witcher 3 Source Code
* Researchers Identify 223 Vulns Used In Ransomware Attacks
* PayPal Fixed A Cross Site Scripting Vulnerability
* KeepChange Said It Stopped Hackers From Stealing User Funds, But Not Personal Data
* Actively Exploited Windows Kernel EoP Bug Allows Takeover
* Attackers Exploit Critical Adobe Flaw To Target Windows Users
* Bitcoin Consumes More Electricity Than Argentina
* Authorities Arrest SIM Swapping Gang That Targeted Celebrities
* Cyberpunk 2077 Makers CD Projekt Hit By Ransomware Hack
* Billions Of Passwords Offered For $2 In The Underground
* Hacker Tried To Poison Florida City's Water Supply
* Facebook Sued For Losing Control Of Users' Data
* Big Jump In RDP Attacks As Hackers Target Staff Working From Home
* Government Censorship Threats Over TikTok Spiked Interest In VPNs
* Iran Hides Spyware In Wallpaper, Restaurant, And Game Apps
* Google Chrome Zero-Day Afflicts Windows, Mac Users
* DDoSers Are Abusing Plex Media Server To Make Attacks More Potent

### Krebs on Security

* What's most interesting about the Florida water system hack? That we heard about it at all.
* Microsoft Patch Tuesday, February 2021 Edition
* Arrest, Raids Tied to 'U-Admin' Phishing Kit
* Facebook, Instagram, TikTok and Twitter Target Resellers of Hacked Accounts
* 'ValidCC,' a Major Payment Card Bazaar and Looter of E-Commerce Sites, Shuttered
* U.K. Arrest in 'SMS Bandits' Phishing Service
* The Taxman Cometh for ID Theft Victims
* Arrest, Seizures Tied to Netwalker Ransomware
* International Action Targets Emotet Crimeware
* DDoS-Guard To Forfeit Internet Space Occupied by Parler

# LATEST NEWS

**Dark Reading**

* 100+ Financial Services Firms Targeted in Ransom DDoS Attacks in 2020
* How to Submit a Column to Dark Reading
* Water Utility Hack Could Inspire More Intruders
* You've Got Cloud Security All Wrong: Managing Identity in a Cloud World
* Ransomware Attackers Set Their Sights on SaaS
* Growing Collaboration Among Criminal Groups Heightens Ransomware Threat for Healthcare Sector
* Pandemic Initially Led to Fewer Disclosed Vulnerabilities, Data Suggests
* Microsoft Launches Phase 2 Mitigation for Zerologon Flaw
* Game Over: Stopping DDoS Attacks Before They Start
* 7 Things We Know So Far About the SolarWinds Attacks
* Unemployment Fraud: As If Being Out of Work Wasn't Bad Enough
* Cloud-Native Apps Make Software Supply Chain Security More Important Than Ever
* On the Radar: Twingate Offers an Easy-to-Use Zero-Trust Access Service
* High-Severity Vulnerabilities Discovered in Multiple Embedded TCP/IP Stacks
* SASE Surge: Why the Market Is Poised to Grow
* Zero Trust in the Real World
* Multivector Attacks Demand Security Controls at the Messaging Level
* Florida Water Utility Hack Highlights Risks to Critical Infrastructure
* Microsoft Fixes Windows Zero-Day in Patch Tuesday Rollout
* SentinelOne Buys Data Analytics Company Scalyr

**The Hacker News**

* Apple will proxy Safe Browsing requests to hide iOS users' IP from Google
* Yandex Employee Caught Selling Access to Users' Email Inboxes
* Secret Chat in Telegram Left Self-Destructing Media Files On Devices
* Researchers Uncover Android Spying Campaign Targeting Pakistan Officials
* The Weakest Link in Your Security Posture: Misconfigured SaaS Settings
* 10 SIM Swappers Arrested for Stealing  $100M in Crypto from Celebrities
* Poor Password Security Led to Recent Water Treatment Facility Hack
* Iranian Hackers Utilize ScreenConnect to Spy On UAE, Kuwait Government Agencies
* Dependency Confusion Supply-Chain Attack Hit Over 35 High-Profile Companies
* LodaRAT Windows Malware Now Also Targets Android Devices
* Apple Patches 10-Year-Old macOS SUDO Root Privilege Escalation Bug
* Microsoft Issues Patches for In-the-Wild 0-day and 55 Others Windows Bugs
* Webinar and eBook: The Dark Side of EDR. Are You Prepared?
* Ukrainian Police Arrest Author of World's Largest Phishing Service U-Admin
* Hacker Tried Poisoning Water Supply After Breaking Into Florida's Treatment System

# LATEST NEWS

### Security Week

* Vendor Ships Unofficial Patch for IE Zero-Day Vulnerability
* Cybersecurity M&A Roundup for Week of Feb. 8, 2021
* Vulnerability in VMware vSphere Replication Can Facilitate Attacks on Enterprises
* Accellion to Retire File Transfer Service Targeted in Attacks
* Computer Malware Fraudster Gets 2 Years in Prison
* Vast Majority of Phishing and Malware Campaigns Are Small-Scale and Short-Lived
* U.S. Gov Warning on Water Supply Hack: Get Rid of Windows 7
* 'Money Mule' Operator Gets Seven-Year Prison Sentence
* Vulnerabilities in TCP/IP Stacks Allow for TCP Connection Hijacking, Spoofing
* Apax Partners Buys Majority Stake in Herjavec Group
* Industry Reactions to U.S. Water Plant Hack: Feedback Friday
* Report Highlights Cyber Risks to US Election Systems
* Data Privacy Management Firm WireWheel Raises $20 Million
* The Intelligent Edge: An Increasing Target for Bad Actors
* SecurityWeek to Host Supply Chain Security Summit on March 10, 2021
* Autonomous Vehicle Security Firm AUTOCRYPT Raises $15 Million
* Newly Discovered Android Spyware Linked to State-Sponsored Indian Hackers
* Biden Team Asks Court to Pause Move to Ban TikTok in US
* Mobile Health Apps Found to Expose Records of Millions of Users
* SecurityWeek Announces Virtual Cybersecurity Event Schedule for 2021

### Infosecurity Magazine

* SBRC Adds Ransomware Scenario to Security Training Program
* Duo Charged with Multimillion-Dollar Dark Web Drugs Scheme
* Yandex Insider Breach Hits Nearly 5000 Inboxes
* Police Reportedly Arrest Egregor Ransomware Members
* Three Charged Over Fraudulent Vaccine Website
* US Jails Money Mule Kingpin
* Diners Devour Made-to-Order Fraud
* Real Bug Volumes in 2020 Exceed Official CVEs by 29%: Report
* Nearly Two-Thirds of CVEs Are Low Complexity
* Singtel Supply Chain Breach Traced to Zero-Day Bug
* Queen's University Belfast Recognized for Role in Growing Cybersecurity Awareness
* India Calls Out Twitter for Differential Treatment

# LATEST NEWS

### KnowBe4 Security Awareness Training Blog RSS Feed

* A Ransomware Victim Refuses to Pay
* New Novel Campaign Targeting Security Researchers Uses Really Creative Social Engineering to Fool Vic
* New Phishing Scam Uses Fake PPP Loans to Trick Victims into Giving Up Personal Information
* Dutch Intelligence Agencies Warn About Chinese and Russian Cyber Espionage
* [Heads Up] Growing Collaboration Among Criminal Groups Heightens Ransomware Triple Threat
* [Scary?] AI Can Now Learn To Manipulate Human Behavior
* Phishing for Love
* [New E-Book] Comprehensive Anti-Phishing Guide
* It's Not Only About the URL
* [HEADS UP] NHS Issues Warning as UK COVID-19 Vaccine Scams Are Still Running Rampant

### ISC2.org Blog

* Cybersecurity Predictions for 2021 from the (ISC)&sup2; Community of Security Professionals (Part 2)
* Exceptions to Security Policy - What are they and how to deal with them?
* Quick Survey: SolarWinds Incident
* The Importance of a Good Software Security Policy
* How Small Businesses and Big Enterprises Structure Their Cybersecurity Teams

### HackRead

* Hacked Finnish psychotherapy clinic files for bankruptcy
* Is It Illegal To Watch Netflix Using a VPN?
* 12-Year-Old vulnerability in Windows Defender risked 1 billion devices
* How cloud data distracts businesses from correct data security practices
* Vulnerability in Chess.com allowed access to 50 Million user records
* Novel Confucius Android spyware hits military, nuclear entities in Pakistan
* Slack email asking Android app users to change their passwords

### Koddos

* Hacked Finnish psychotherapy clinic files for bankruptcy
* Is It Illegal To Watch Netflix Using a VPN?
* 12-Year-Old vulnerability in Windows Defender risked 1 billion devices
* How cloud data distracts businesses from correct data security practices
* Vulnerability in Chess.com allowed access to 50 Million user records
* Novel Confucius Android spyware hits military, nuclear entities in Pakistan
* Slack email asking Android app users to change their passwords

# LATEST NEWS

### Naked Security

* Egregor ransomware criminals allegedly busted in Ukraine
* Fallen victim to online fraud? Here's what to do&hellip;
* SMS tax scam unmasked: Bogus but believable - don't fall for it!
* S3 Ep19: Chrome zero-day, coffee hacking and Perl.com stolen [Podcast]
* Patch now to stop hackers blindly crashing your Windows computers
* Beware of technical "experts" bombarding you with bug reports
* Safer Internet Day - Why not up your game?
* Naked Security Live - Jargonbuster: Bugs, vulns, 0-days and exploits
* Perl.com gets its domain back - normal service restored!
* Chrome zero-day browser bug found - patch now!

### Threat Post

* mHealth Apps Expose Millions to Cyberattacks
* Yandex Data Breach Exposes 4K+ Email Accounts
* 'Annoyingly Believable' Tax Scam Targets Mobile Users
* Singtel Suffers Zero-Day Cyberattack, Damage Unknown
* Florida Water Plant Hack: Leaked Credentials Found in Breach Database
* Pre-Valentine's Day Malware Attack Mimics Flower, Lingerie Stores
* Celeb SIM-Swap Crime Ring Stole $100M from U.S. Victims
* How Email Attacks are Evolving in 2021
* Various Malware Lurks in Discord App to Target Gamers
* Military, Nuclear Entities Under Target By Novel Android Malware

### Null-Byte

* This VPN Will Give You a Lifetime of Security for Just $18
* How to Write Your Own Bash Scripts to Automate Tasks on Linux
* Start Learning How to Code in Just a Week
* Create a USB Mouse Jiggler to Keep a Target Computer from Falling Asleep (& Prank Friends Too)
* Boost Your Security with a VPN & Private Email Service
* How to Use RedRabbit for Pen-Testing & Post-Exploitation of Windows Machines
* This Top-Rated Audio & Video Production Bundle Is on Sale for $40
* Null Byte's Hacker Guide to Buying an ESP32 Camera Module That's Right for Your Project
* This HD Infographic Design Software Is on Sale for $45
* How to Perform Keystroke Injection Attacks Over Wi-Fi with Your Smartphone

# LATEST NEWS

**IBM Security Intelligence**

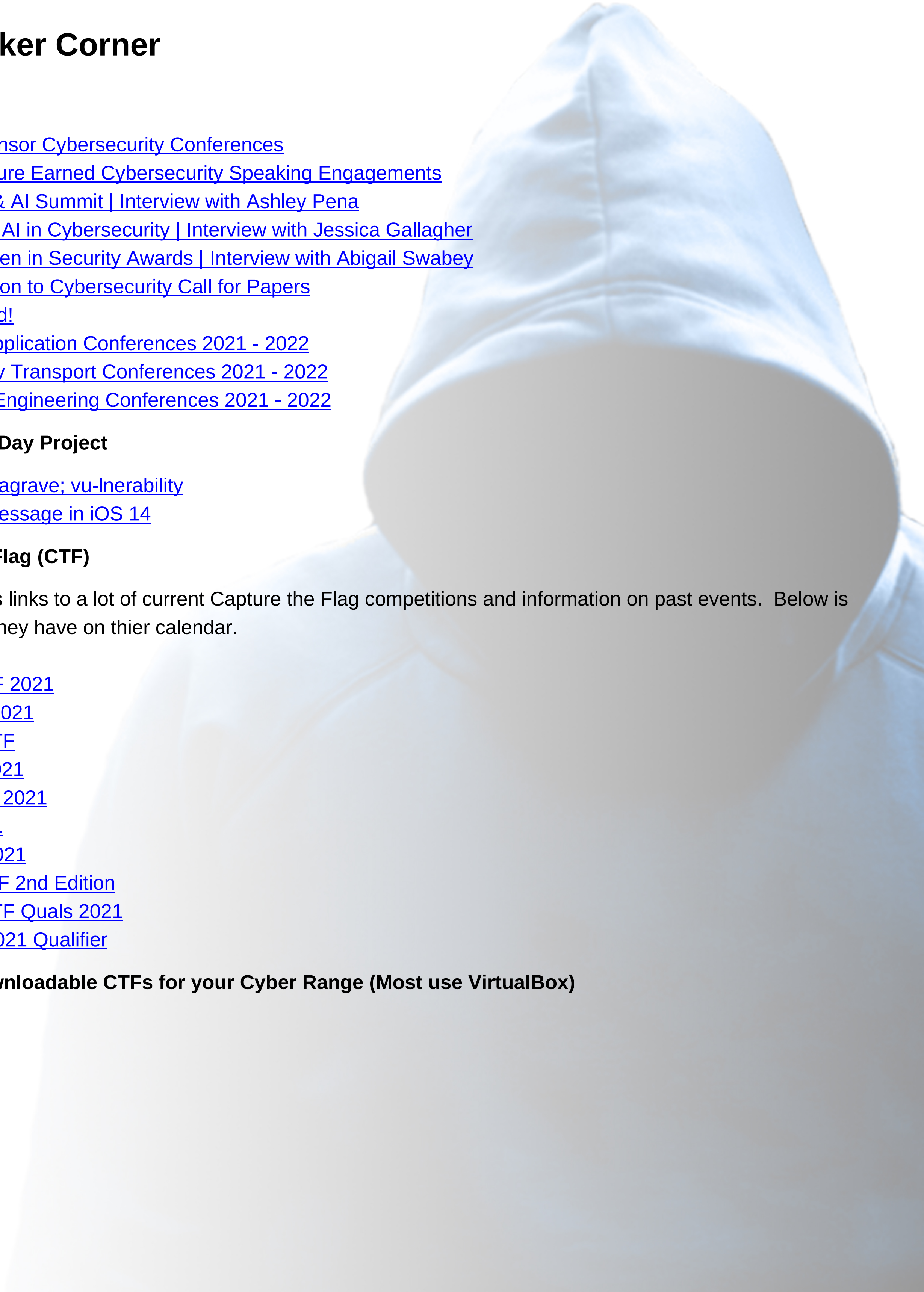
* Beyond Text Messages: How to Secure 2FA Against Phone Authentication Scams
* Why Every Company Needs a Software Update Schedule
* 5 Ways to Overcome Cloud Security Challenges
* AI Security: Curation, Context and Other Keys to the Future
* Hiring Cloud Experts, Despite the Cybersecurity Skills Gap
* Smell the Attack? Sensory-Immersive Cyber Range Training for Industry 4.0
* Boost Your Organization's Digital Security With Zero Trust
* Employee Mental Health: Managing Stress and Trauma
* Cloud Security Considerations to Watch Out for During Mergers and Acquisitions
* Intro to DevSecOps: Why Integrated Security is Key in 2021

**InfoWorld**

* How to work with record types in C#
* Boosting science and engineering in the cloud
* Programming jobs for losers - and how to escape them
* JDK 16: The new features in Java 16
* TypeScript 4.2 tunes tuple types
* 3 must-haves for your multicloud architecture
* What's new in Rust 1.50
* Angular 12 beta preview arrives
* "Do More with R" video tutorials
* Go language gets graph-based ORM

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

* Leonardo's cyber, AI expert becomes Italy's 'green transition' minister
* For US and allies, prepping for AI warfare starts with the data
* Space Force begins adding cyber warriors
* National Guard task force that supports Cyber Command changes over
* The tiny tech lab that put AI on a spyplane has another secret project
* NAVAIR looking for emerging cyber research and development
* SDA to launch several demonstration satellites in 2021
* How the Biden administration can avoid another SolarWinds attack
* White House names leader for SolarWinds hack response after criticism
* Protecting people from disinformation requires a cognitive security proving ground



# The Hacker Corner

### Conferences

* How To Sponsor Cybersecurity Conferences
* How To Secure Earned Cybersecurity Speaking Engagements
* World RPA & AI Summit | Interview with Ashley Pena
* The State of AI in Cybersecurity | Interview with Jessica Gallagher
* AWSN Women in Security Awards | Interview with Abigail Swabey
* An Introduction to Cybersecurity Call for Papers
* We've Moved!
* Best Web Application Conferences 2021 - 2022
* Best Security Transport Conferences 2021 - 2022
* Best Social Engineering Conferences 2021 - 2022

### Google Zero Day Project

* D&eacute;j&agrave; vu-lnerability
* A Look at iMessage in iOS 14

### Capture the Flag (CTF)

**CTF Time** has links to a lot of current Capture the Flag competitions and information on past events.  Below is a list if CTFs they have on thier calendar.

* Tenable CTF 2021
* Union CTF 2021
* darkCON CTF
* Aero CTF 2021
* zer0pts CTF 2021
* UTCTF 2021
* LINE CTF 2021
* PoseidonCTF 2nd Edition
* SPRUSH CTF Quals 2021
* VolgaCTF 2021 Qualifier

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

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

# Tools & Techniques

### Packet Storm Security Tools Links

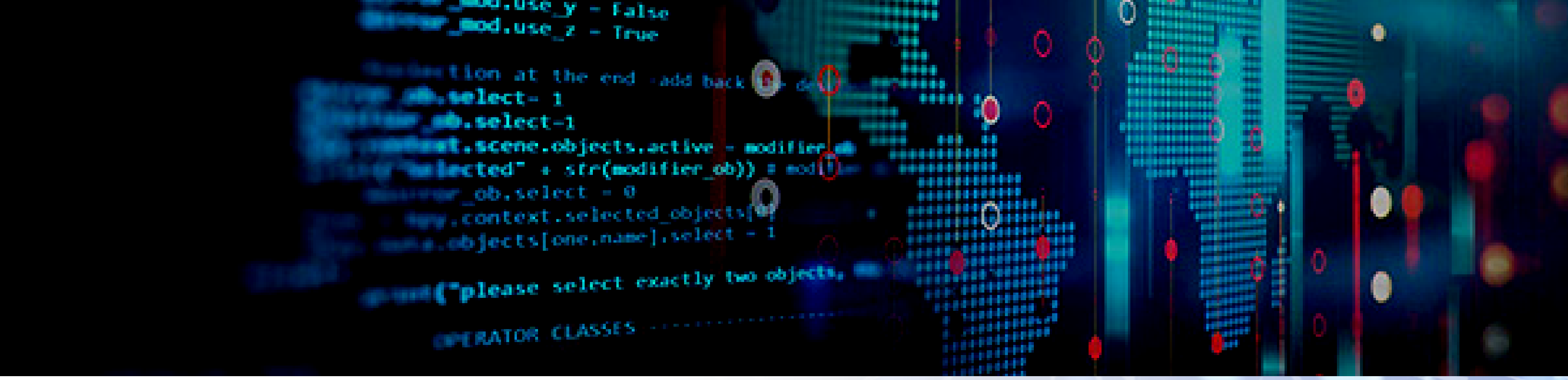
* AIDE 0.17.3
* AIDE 0.17.2
* TOR Virtual Network Tunneling Tool 0.4.4.7
* Clam AntiVirus Toolkit 0.103.1
* Mandos Encrypted File System Unattended Reboot Utility 1.8.14
* SQLMAP - Automatic SQL Injection Tool 1.5.2
* Wireshark Analyzer 3.4.3
* AIDE 0.17.1
* Sifter 11.5
* AIDE 0.17

### Kali Linux Tutorials

* What is DNS Filtering and How to Use It for Safe Browsing
* Pineapple MK7 REST Client : WiFi Hacking Workflow With Pineapple Mark 7 API
* K55 : Linux X86_64 Process Injection Utility
* RadareEye : A Tool Made For Specially Scanning Nearby devices
* ProtOSINT : Script Helps To Investigate Protonmail Accounts & ProtonVPN IP Addresses
* Sigurls : A Reconnaissance Tool & It Fetches URLs From AlienVault's OTX
* PongoOS : A Pre-Boot Execution Environment For Apple Boards
* Wprecon : A Vulnerability Recognition Tool In CMS WordPress
* Mud-Visualizer : A Tool To Visualize MUD Files
* Pidrila : Python Interactive Deepweb-Oriented Rapid Intelligent Link Analyzer

### GBHackers Analysis

* Microsoft will Enable Domain Controller Enforcement Mode to Address Zerologon Flaw
* Hackers Using 4 Zero-day Vulnerabilities to Attack Windows and Android Devices Remotely
* Secret Backdoor found Installed in Zyxel Firewall and VPN
* Critical Dell Wyse Bugs Let Attackers to Execute Code and Access Files and Credentials
* WordPress Easy WP SMTP zero-day Vulnerability Exposes Hundreds of Thousands of Sites to Hack



## Weekly Cyber Security Video and Podcasts

### SANS DFIR

* Episode 171: Apple Forensics: Magic Keystrokes - Target Disk Mode key
* Episode 170: Apple Forensics: Magic Keystrokes - Recovery Mode key
* Episode 169: Apple Forensics: Magic Keystrokes - Single User Mode key
* Episode 168: Apple Forensics: Magic Keystrokes - alt/option key

### Defcon Conference

* DEF CON 2020 NYE   ZEE   DJ Music Video
* DEF CON 2020 NYE   Yesterday & Tomorrow   DJ Music Video
* DEF CON 2020 NYE   Skittish & Bus   DJ Music Video
* Hacker History Project - The Dark Tangent Interviewed at DEF CON 5 - courtesy of ZDnet

### Hak5

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

### The PC Security Channel [TPSC]

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

### Eli the Computer Guy

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

### Security Now

* SCADA Scandal - Defender Thinks Chrome is Malware, Plex Media Servers in DDoS Attacks
* NAT Slipstreaming 2.0 - SUDO Was Pseudo Secure, BigNox Supply-Chain Attack, iMessage in a Sandbox

### Troy Hunt

* Weekly Update 230

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

* 206-Website Analytics Concerns & Solutions
* 205-Five Shows In One

# Proof of Concept (PoC) & Exploits

### Packet Storm Security

* SolarWinds Serv-U FTP Server 15.2.1 Cross Site Scripting
* SolarWinds Serv-U FTP Server 15.2.1 Path Traversal
* School Event Attendance Monitoring System 1.0 Cross Site Scripting
* School File Management System 1.0 Cross Site Scripting
* PDFCOMPLETE Corporate Edition 4.1.45 Unquoted Service Path
* Backdoor.Win32.BackAttack.18 Missing Authentication
* Online Marriage Registration System 1.0 Remote Code Execution
* Openlitespeed WebServer 1.7.8 Command Injection
* Backdoor.Win32.Augudor.a Code Execution
* PEEL Shopping 9.3.0 Cross Site Scripting
* Huawei MBAMainService Unquoted Service Path
* Micro Focus Operations Bridge Manager Remote Code Execution
* Microsoft Windows Server Silo Registry Key Symbolic Link Privilege Escalation
* Adobe Magento Commerce Cross Site Scripting
* b2evolution CMS 6.11.6 Cross Site Scripting
* b2evolution CMS 6.11.6 Open Redirection
* Online Car Rental 1.0 Shell Upload
* Backdoor.Win32.Aphexdoor.LiteSock Buffer Overflow
* Node.JS Remote Code Execution
* Chrome ClipboardWin::WriteBitmap Heap Buffer Overflow
* Chrome SkBitmapOperations::UnPreMultiply Heap Buffer Overflow
* Backdoor.Win32.NetTerrorist Authentication Bypass / Code Execution
* Discord Probot Arbitrary File Upload
* Trojan.Win32.Cafelom.bu Heap Corruption
* AnyTXT Searcher 1.2.394 Unquoted Service Path

### CXSecurity

* SEO Panel 4.6.0 Remote Code Execution (2)
* PhreeBooks 5.2.3 Remote Code Execution
* Solaris 10 1/13 (SPARC) dtprintinfo Local Privilege Escalation
* PEAR Archive_Tar Arbitrary File Write
* Quick.CMS 6.7 Remote Code Execution
* Metasploit Framework 6.0.11 Command Injection
* PRTG Network Monitor Remote Code Execution

# Proof of Concept (PoC) & Exploits

### Exploit Database

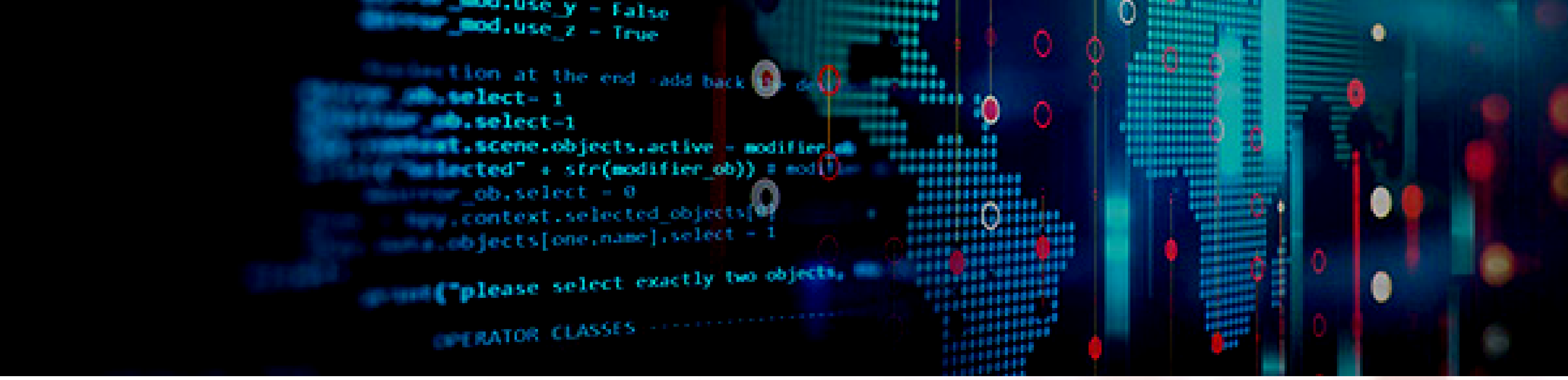
* [local] Tasks 9.7.3 - Insecure Permissions
* [webapps] Teachers Record Management System 1.0 - 'searchteacher' SQL Injection
* [webapps] TestLink 1.9.20 - Unrestricted File Upload (Authenticated)
* [webapps] School Event Attendance Monitoring System 1.0 - 'Item Name' Stored Cross-Site Scripting
* [webapps] School File Management System 1.0 - 'multiple' Stored Cross-Site Scripting
* [local] PDFCOMPLETE Corporate Edition 4.1.45 - 'pdfcDispatcher' Unquoted Service Path
* [webapps] Online Marriage Registration System (OMRS) 1.0 - Remote code execution (3)
* [webapps] Openlitespeed WebServer 1.7.8 - Command Injection (Authenticated) (2)
* [webapps] b2evolution 6.11.6 - 'tab3' Reflected XSS
* [webapps] b2evolution 6.11.6 - 'redirect_to' Open Redirect
* [webapps] PEEL Shopping 9.3.0 - 'address' Stored Cross-Site Scripting
* [webapps] Node.JS - 'node-serialize' Remote Code Execution (2)
* [webapps] b2evolution 6.11.6 - 'plugin name' Stored XSS
* [webapps] Adobe Connect 10 - Username Disclosure
* [local] AnyTXT Searcher 1.2.394 - 'ATService' Unquoted Service Path
* [local] Epson USB Display 1.6.0.0 - 'EMP_UDSA' Unquote Service Path
* [webapps] Online Car Rental System 1.0 - Stored Cross Site Scripting
* [webapps] WordPress Plugin Supsystic Backup 2.3.9 - Local File Inclusion
* [webapps] WordPress Plugin Supsystic Contact Form 1.7.5 - Multiple Vulnerabilities
* [webapps] WordPress Plugin Supsystic Data Tables Generator 1.9.96 - Multiple Vulnerabilities
* [webapps] WordPress Plugin Supsystic Digital Publications 1.6.9 - Multiple Vulnerabilities
* [local] Microsoft Internet Explorer 11 32-bit - Use-After-Free
* [webapps] WordPress Plugin Supsystic Membership 1.4.7 - 'sidx' SQL injection
* [webapps] WordPress Plugin Supsystic Newsletter 1.5.5 - 'sidx' SQL injection
* [webapps] Alt-N MDaemon webmail 20.0.0 - 'file name' Stored Cross Site Scripting (XSS)

### Exploit Database for offline use

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

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

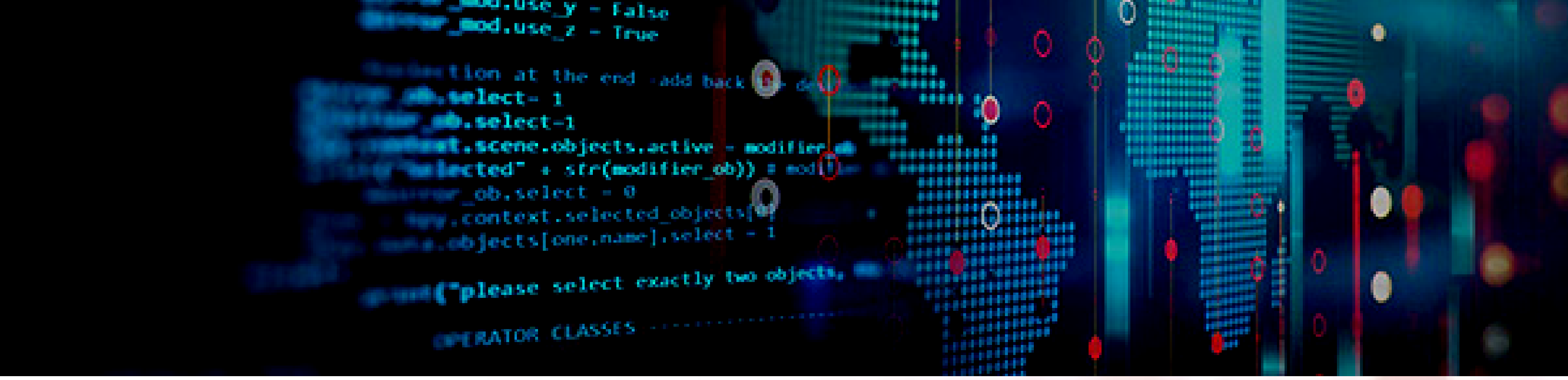
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


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

# Latest Hacked Websites

**Published on Zone-h.org**

http://www.corpocaldas.gov.co/index.txt
http://www.corpocaldas.gov.co/index.txt notified by Mamad Warning
http://bkpw.go.th/nkri.txt
http://bkpw.go.th/nkri.txt notified by Xyp3r2667
http://www.phayumoph.go.th/nkri.txt
http://www.phayumoph.go.th/nkri.txt notified by Xyp3r2667
https://maeteep-ngao.go.th/nkri.txt
https://maeteep-ngao.go.th/nkri.txt notified by Xyp3r2667
http://dgda.gov.bd/read.htm
http://dgda.gov.bd/read.htm notified by Mr.L3RB1
http://www.srisamran-sm.go.th/me.html
http://www.srisamran-sm.go.th/me.html notified by Mr V
http://coges.regione.marche.it/krz.html
http://coges.regione.marche.it/krz.html notified by Mr.Kro0oz.305
https://trawas.mojokertokab.go.id/readme.htm
https://trawas.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://puri.mojokertokab.go.id/readme.htm
https://puri.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://rsudsoekandar.mojokertokab.go.id/readme.htm
https://rsudsoekandar.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://kutorejo.mojokertokab.go.id/readme.htm
https://kutorejo.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://puskesmas-pungging.mojokertokab.go.id/readme.htm
https://puskesmas-pungging.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://pungging.mojokertokab.go.id/readme.htm
https://pungging.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://mojosari.mojokertokab.go.id/readme.htm
https://mojosari.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://organisasi.mojokertokab.go.id/readme.htm
https://organisasi.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://mojoanyar.mojokertokab.go.id/readme.htm
https://mojoanyar.mojokertokab.go.id/readme.htm notified by TangerangXploit Team
https://jatirejo.mojokertokab.go.id/readme.htm
https://jatirejo.mojokertokab.go.id/readme.htm notified by TangerangXploit Team


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

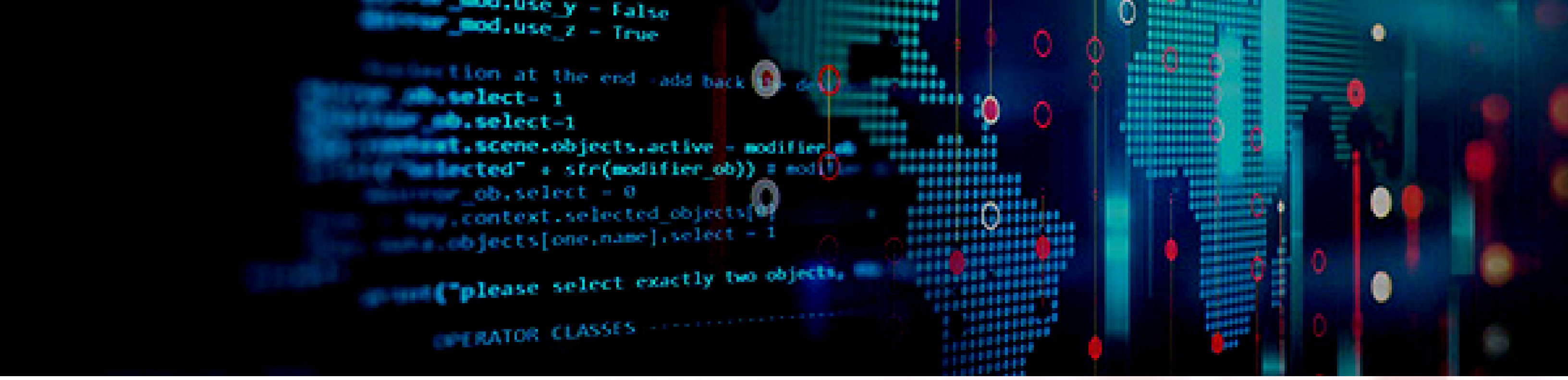
# Dark Web News

### Darknet Live

[Feds Traced Bitcoin Transactions to a Drug Dealer's Apartment]()
Feds identified a darkweb vendor by linking Bitcoin transactions to an apartment I.P. address. They also monitored his internet traffic. (via darknetlive.com)
[A Message From Dread Admins on the Topic of Stability]()
In recent posts, administrators of Dread outlined ongoing availability issues as well as a plan for the future. (via darknetlive.com)
[Prolific DarkMarket Vendor Arrested in Germany]()
German law enforcement agencies announced the arrest of a high-profile DarkMarket vendor. (via darknetlive.com)
[FBI: Wisconsin Woman Tried to Hire a Hitman on the Darkweb]()
A Wisconsin woman used a murder-for-hire site on the darkweb to have someone killed, according to the Federal Bureau of Investigation. (via darknetlive.com)

### Dark Web Link

[Dark Web Drug Distribution: Florida Darknet Trafficker Found Guilty]()
A Florida-based darknet drug trafficker has pleaded guilty to unlawful dark web drug distribution. He had been distributing thousands of prescription drugs (opioid pills) in exchange for more than half a million dollars. As the court document mentions, the accused Daren James Reid aged 35 years from Fort Lauderdale had been using the dark web [...] The post [Dark Web Drug Distribution: Florida Darknet Trafficker Found Guilty]() appeared first on [Dark Web Link | Deep web Onion Links | Darknet News]().
[CD Projekt Red: Source Code Sold On The Dark Web]()
After a targeted cyber attack, the source codes of CD Projekt Red games got stolen and reportedly sold at the dark web auction for $7 million. The game included The Witcher 3 (contained the unreleased version), Gwent: The Witcher Card Game and Cyberpunk 2077. Following the cyber attack, a ransomware note had been delivered to [...] The post [CD Projekt Red: Source Code Sold On The Dark Web]() appeared first on [Dark Web Link | Deep web Onion Links | Darknet News]().
[Dark Web Videos: Man Jailed On Uploading Teen Washroom Scenes]()
A shocking incident has massively affected people. The young teenagers who had visited Cork from Europe were filmed in the shower and the washroom of a guesthouse in Cork secretly. Some of the dark web videos on the same situation had been spotted on the darknet that was uploaded on various paedophile sites. The accused had been [...] The post [Dark Web Videos: Man Jailed On Uploading Teen Washroom Scenes]() appeared first on [Dark Web Link | Deep web Onion Links | Darknet News]().



## Trend Micro Anti-Malware Blog

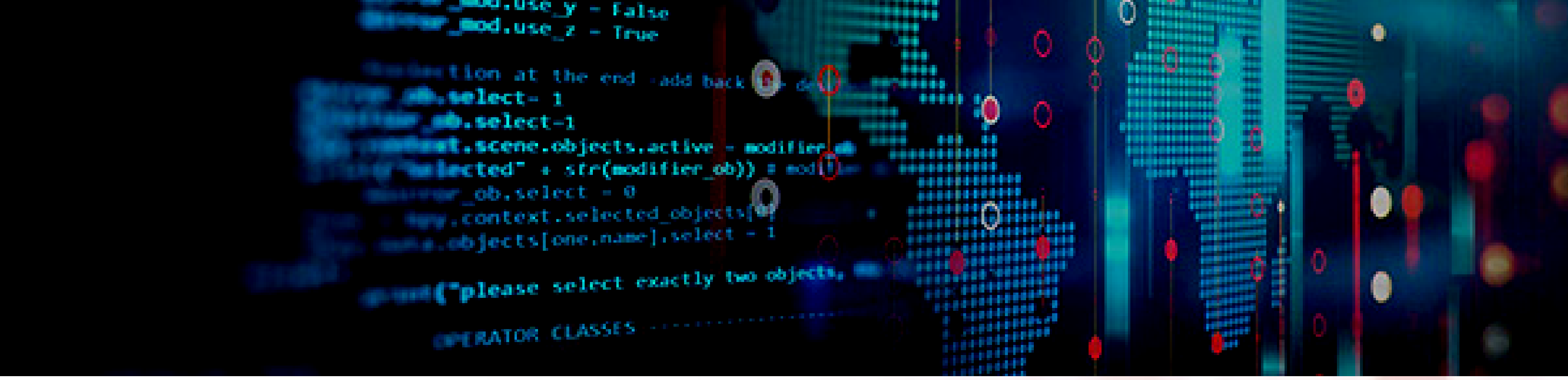
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing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

## RiskIQ

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

## FireEye

* Metasploit Wrap-Up
* Talkin' SMAC: Alert Labeling and Why It Matters
* New InsightVM Dashboard Helps You Discover Significant Changes in Your Environment from the Past 30 D
* CVE-2021-22652: Advantech iView Missing Authentication RCE (FIXED)
* SOAR Tools: What to Look for When Investing in Security Automation Tech
* Patch Tuesday - February 2021
* Metasploit Wrap-Up
* Cisco Patches Recently Disclosed "sudo" Vulnerability (CVE-2021-3156) in Multiple Products
* SonicWall SNWLID-2021-0001 Zero-Day and SolarWinds' 2021 CVE Trifecta: What You Need to Know
* Vulnerability Scanning With the Metasploit Remote Check Service (Beta Release)



# Advisories

### US-Cert Alerts & bulletins

* VMware Releases Security Update
* Compromise of U.S. Water Treatment Facility
* Verify Your Valentine
* Microsoft Launches Phase 2 Mitigation for Netlogon Remote Code Execution Vulnerability (CVE-2020-1472
* Microsoft Releases February 2021 Security Updates
* Apple Releases Security Updates
* Adobe Releases Security Updates
* Microsoft Warns of Windows Win32k Privilege Escalation
* AA21-042A: Compromise of U.S. Water Treatment Facility
* AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
* Vulnerability Summary for the Week of February 8, 2021
* Vulnerability Summary for the Week of February 1, 2021

### Zero Day Initiative Advisories

ZDI-CAN-12814: GoPro
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'garmin' was reported to the affected vendor on: 2021-02-15, 0 days ago. The vendor is given until 2021-06-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13041: GoPro
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-15, 0 days ago. The vendor is given until 2021-06-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12710: OpenText
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12711: OpenText
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12712: OpenText
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a

fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12890: Arlo

A CVSS score 6.8 (AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Team FLASHBACK: Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) + Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12718: OpenText

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12716: OpenText

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12717: OpenText

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12715: OpenText

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13039: Advantech

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13038: Advantech

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12579: Apple

A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'mipu94 of SEFCOM lab, ASU.' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13244: Foxit

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13245: Foxit

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13131: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-12, 3 days ago. The vendor is given until 2021-06-12 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12986: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12919: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12984: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13227: Microsoft

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anthony Fuller of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12708: OpenText

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12987: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'xina1i at SecZone' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13241: Foxit

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13101: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xu Peng from UCAS and Wang Yanhao from QiAnXin Technology Research Institute ' was reported to the affected vendor on: 2021-02-10, 5 days ago. The vendor is given until 2021-06-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Ubuntu Security Notice USN-4734-1

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

Red Hat Security Advisory 2021-0497-01

Red Hat Security Advisory 2021-0497-01 - 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 2021-0495-01

Red Hat Security Advisory 2021-0495-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache Tomcat Servlet container, JBoss HTTP Connector, the PicketLink Vault extension for Apache Tomcat, and the Tomcat Native library. This release of Red Hat JBoss Web Server 5.4.1 serves as a replacement for Red Hat JBoss Web Server 5.4.0, and includes bug fixes, enhancements, and component upgrades, which are documented in the Release Notes, linked to in the References. Issues addressed include information leakage and null pointer vulnerabilities.

Red Hat Security Advisory 2021-0494-01

Red Hat Security Advisory 2021-0494-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache Tomcat Servlet container, JBoss HTTP Connector, the PicketLink Vault extension for Apache Tomcat, and the Tomcat Native library. This release of Red Hat JBoss Web Server 5.4.1 serves as a replacement for Red Hat JBoss Web Server 5.4.0, and includes bug fixes, enhancements and component upgrades, which are documented in the Release Notes, linked to in the References. Issues addressed include information leakage and null pointer vulnerabilities.

Red Hat Security Advisory 2021-0491-01

Red Hat Security Advisory 2021-0491-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache HTTP Server, the Apache Tomcat Servlet container, Apache Tomcat Connector, JBoss HTTP Connector, Hibernate, and the Tomcat Native library. This release of Red Hat JBoss Web Server 3.1 Service Pack 11 serves as a replacement for Red Hat JBoss Web Server 3.1, and includes bug fixes, which are documented in the Release Notes document linked to in the References. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2021-0489-01

Red Hat Security Advisory 2021-0489-01 - Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache HTTP Server, the Apache Tomcat Servlet container, Apache Tomcat Connector, JBoss HTTP Connector, Hibernate, and the Tomcat Native library. This release of Red Hat JBoss Web Server 3.1 Service Pack 11 serves as a replacement for Red Hat JBoss Web Server 3.1, and includes bug fixes, which are documented in the Release Notes document linked to in the References. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2021-0485-01

Red Hat Security Advisory 2021-0485-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include HTTP request smuggling, denial of service, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-0488-01

Red Hat Security Advisory 2021-0488-01 - 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 6 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 5 and includes bug fixes and enhancements. Issues addressed include a null pointer vulnerability.

Ubuntu Security Notice USN-4733-1

Ubuntu Security Notice 4733-1 - Yi&#287;it Can Y&#305;lmaz discovered that GNOME Autoar could extract files outside of the intended directory. If a user were tricked into extracting a specially crafted archive, a remote attacker could create files in arbitrary locations, possibly leading to code execution.

Ubuntu Security Notice USN-4732-1

Ubuntu Security Notice 4732-1 - It was discovered that SQLite incorrectly handled certain sub-queries. An attacker could use this issue to cause SQLite to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2021-0486-01

Red Hat Security Advisory 2021-0486-01 - This release adds the new Apache HTTP Server 2.4.37 Service Pack 6 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 5 and includes bug fixes and enhancements. Issues addressed include a null pointer vulnerability.

Ubuntu Security Notice USN-4731-1

Ubuntu Security Notice 4731-1 - It was discovered that JUnit 4 contains a local information disclosure vulnerability. An attacker could possibly use this issue to obtain sensitive information.

Ubuntu Security Notice USN-4730-1

Ubuntu Security Notice 4730-1 - It was discovered that PostSRSd mishandled certain input. A remote attacker could use this vulnerability to cause a denial of service via a long timestamp tag in an SRS address.

Red Hat Security Advisory 2021-0476-01

Red Hat Security Advisory 2021-0476-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.103 and .NET Runtime 5.0.3. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0474-01

Red Hat Security Advisory 2021-0474-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 2.1.521 and .NET Core Runtime 2.1.25. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0470-01

Red Hat Security Advisory 2021-0470-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 2.1.521 and .NET Core Runtime 2.1.25. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0472-01

Red Hat Security Advisory 2021-0472-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 3.1.112 and .NET Core Runtime 3.1.12. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0473-01

Red Hat Security Advisory 2021-0473-01 - .NET is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET that address a security vulnerability are now available. The updated versions are .NET SDK 5.0.103 and .NET Runtime 5.0.3. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-0471-01

Red Hat Security Advisory 2021-0471-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address a security vulnerability are now available. The updated versions are .NET Core SDK 3.1.112 and .NET Core Runtime 3.1.12. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-4729-1

Ubuntu Security Notice 4729-1 - Joakim Hindersson discovered that Open vSwitch incorrectly parsed certain network packets. A remote attacker could use this issue to cause a denial of service, or possibly alter packet classification.

Ubuntu Security Notice USN-4713-2

Ubuntu Security Notice 4713-2 - It was discovered that the LIO SCSI target implementation in the Linux kernel performed insufficient identifier checking in certain XCOPY requests. An attacker with access to at least one LUN in a multiple backstore environment could use this to expose sensitive information or modify data.

Ubuntu Security Notice USN-4727-1

Ubuntu Security Notice 4727-1 - Alexander Popov discovered that multiple race conditions existed in the AF_VSOCK implementation in the Linux kernel. A local attacker could use this to cause a denial of service or execute arbitrary code.

Ubuntu Security Notice USN-4728-1

Ubuntu Security Notice 4728-1 - Gilad Reti discovered that snapd did not correctly specify cgroup delegation when generating systemd service units for various container management snaps. This could allow a local attacker to escalate privileges via access to arbitrary devices of the container host from within a compromised or malicious container.

Ubuntu Security Notice USN-4726-1

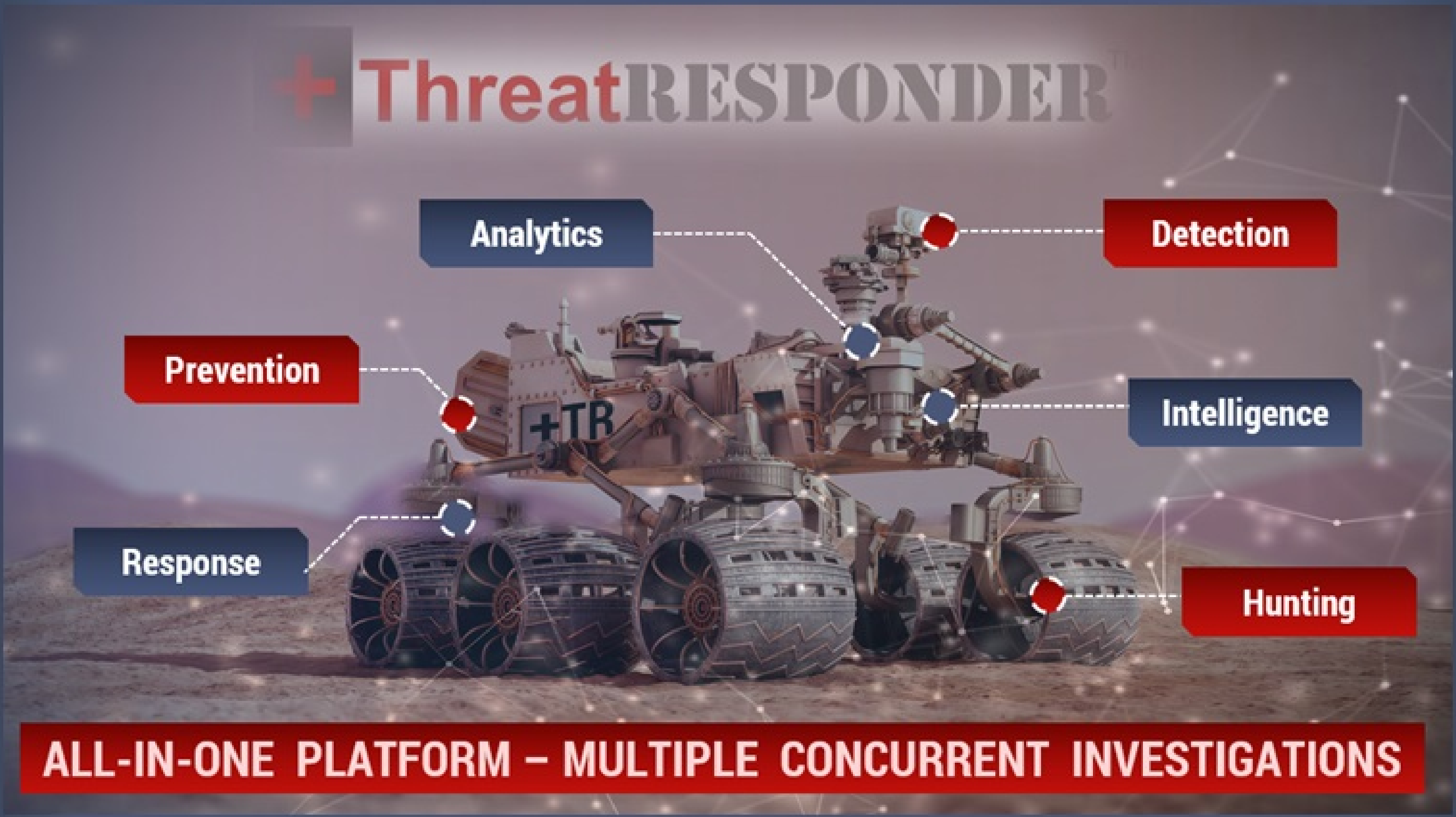
Ubuntu Security Notice 4726-1 - It was discovered that OpenJDK incorrectly handled the direct buffering of characters. An attacker could use this issue to cause OpenJDK to crash, resulting in a denial of service, or cause other unspecified impact.

## 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



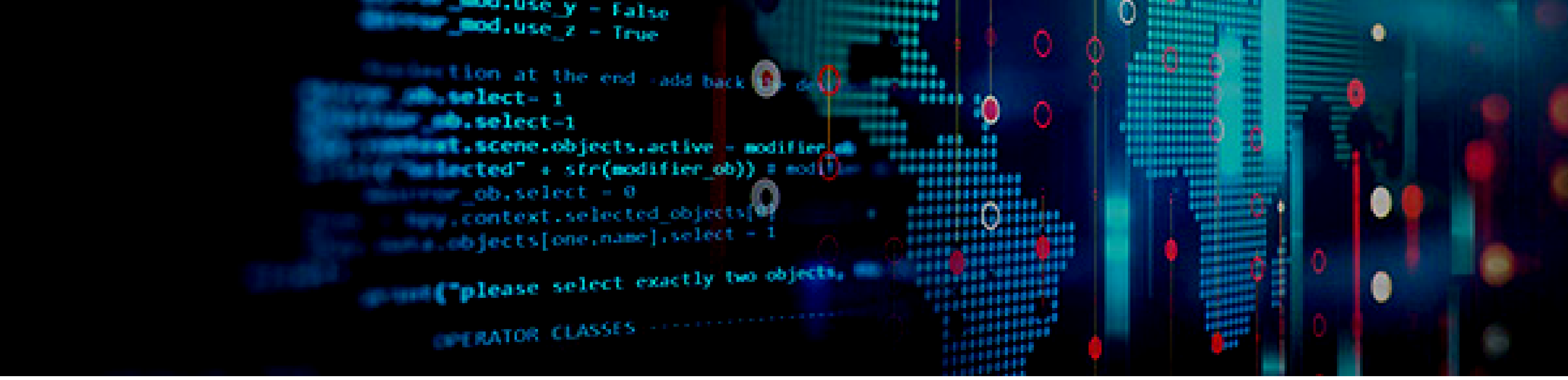
## The Solution – ThreatResponder® Platform

**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**

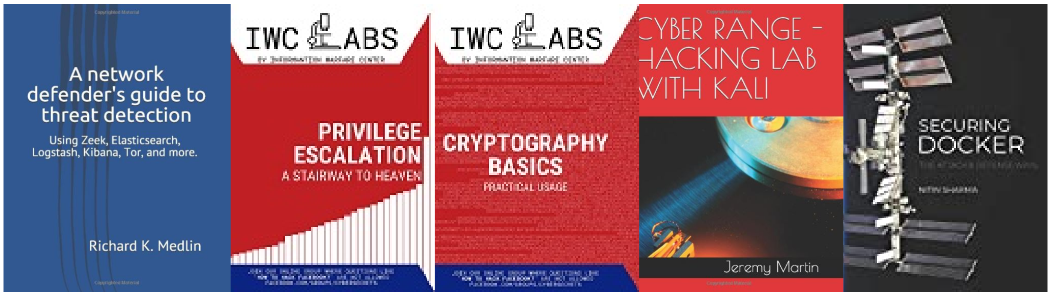

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
"Selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

# 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**