Feb-08-21

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 8, 2021

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

Internet Storm Center Infocon Status

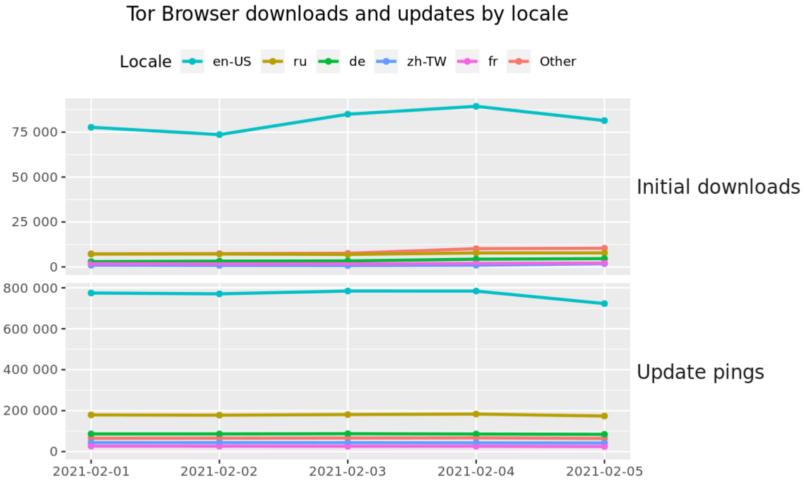
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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/2UuIG9B

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



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

Interesting News

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

* 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

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* 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
* Amazon Faces Spying Claims Over AI Cameras In Van
* Industrial Control System Vulnerabilities Up 25 Percent In 2020
* Spy Planes Grounded In US Following Privacy Battle
* Google Chrome Sync Feature Can Be Abused For C&C And Data Exfiltration
* Instagram Unmasks High Profile OG Account Stealers
* Bug Bounty Failure Stories To Learn From
* Nespresso Smart Cards Hacked To Provide Infinite Coffee After Someone Wasn't Too Perky About Security
* Discord Servers Targeted In Cryptocurrency Exchange Scam Wave
* Security Firm Stormshield Discloses Data Breach, Theft Of Source Code
* Clearview Facial Recognition Technology Ruled Illegal In Canada
* Agent Tesla Trojan Kneecaps MS Anti-Malware Interface
* Crypto Crook Hired Steven Seagal To Promote Scam, Now Faces Charges
* Three New SolarWinds Vulnerabilities Found And Patched
* Recent Root Giving Sudo Bug Also Impacts macOS
* Apple Face ID To Work For Mask Wearers
* Hackers Are Exploiting A Critical Zero Day In Devices From SonicWall
* SolarWinds Hack Prompts Congress To Put NSA In Encryption Hot Seat
* Identity Theft Spikes Due To COVID-19 Relief
* This Linux Malware Is Hijacking Supercomputers Globally
* Malware Inserted Into NoxPlayer Android Emulator

Krebs on Security

* 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
* New Charges Derail COVID Release for Hacker Who Aided ISIS
* Joker's Stash Carding Market to Call it Quits

LATEST NEWS

Dark Reading

* Emotet Takedown: Short-Term Celebration, Long-Term Concerns
* Malicious Code Injected via Google Chrome Extension Highlights App Risks
* Hacker Raised Chemical Settings at Water Treatment Plant to Dangerous Levels
* What's the Difference Between 'Observability' and 'Visibility' in Security?
* Android App Infects Millions of Devices With a Single Update
* Hidden Dangers of Microsoft 365's Power Automate and eDiscovery Tools
* Spotify Hit With Another Credential-Stuffing Attack
* Security Researchers Push for 'Bug Bounty Program of Last Resort'
* Pro Tip: Don't Doubt Yourself
* Cybercrime Goes Mainstream
* AI and APIs: The A+ Answers to Keeping Data Secure and Private
* Google's Payout to Bug Hunters Hits New High
* IBM Offers $3M in Grants to Defend Schools from Cyberattacks
* Microsoft Says It's Time to Attack Your Machine-Learning Models
* Web Application Attacks Grow Reliant on Automated Tools
* Is $50,000 for a Vulnerability Too Much?
* Concerns Over API Security Grow as Attacks Increase
* Patch Imperfect: Software Fixes Failing to Shut Out Attackers
* An Observability Pipeline Could Save Your SecOps Team
* SolarWinds Attackers Spent Months in Corporate Email System: Report

The Hacker News

* Detailed: Here's How Iran Spies on Dissidents with the Help of Hackers
* Top 5 Bug Bounty Programs to Watch in 2021
* WARNING - Hugely Popular 'The Great Suspender' Chrome Extension Contains Malware
* Cybercriminals Now Using Plex Media Servers to Amplify DDoS Attacks
* Critical Flaws Reported in Cisco VPN Routers for Businesses-Patch ASAP
* New Chrome Browser 0-day Under Active Attack-Update Immediately!
* How to Audit Password Changes in Active Directory
* Beware: New Matryosh DDoS Botnet Targeting Android-Based Devices
* Why Human Error is #1 Cyber Security Threat to Businesses in 2021
* Critical Bugs Found in Popular Realtek Wi-Fi Module for Embedded Devices
* Over a Dozen Chrome Extensions Caught Hijacking Google Search Results for Millions
* 3 New Severe Security Vulnerabilities Found In SolarWinds Software
* Guide: How Security Consolidation Helps Small Cybersecurity Teams
* A New Linux Malware Targeting High-Performance Computing Clusters
* Agent Tesla Malware Spotted Using New Delivery & Evasion Techniques

LATEST NEWS

Security Week

* Remote Hacker Caught Poisoning Florida City Water Supply
* Over 1,200 Iranians Targeted in Domestic Surveillance Campaign
* Google Launches Database for Open Source Vulnerabilities
* Web Developer Hub SitePoint Discloses Data Breach
* Government Providers Dominate Cybersecurity M&A Roundup for Week of Feb. 1, 2021
* Attackers Leverage Locally-Loaded Chrome Extension for Data Exfiltration
* Google Moves Away From Diet of 'Cookies' to Track Users
* Google Chrome, Microsoft IE Zero-Days in Crosshairs
* Packaging Giant WestRock Says Ransomware Attack Hit Production
* Plex Media Server Abused for DDoS Attacks
* Open Source Tool Helps Organizations Secure GE CIMPLICITY HMI/SCADA Systems
* Google Paid Out $6.7 Million in Bug Bounty Rewards in 2020
* Microsoft Says Its Services Not Used as Entry Point by SolarWinds Hackers
* Trucking Giant Says Ransomware Attack Had $7.5M Impact
* Cisco Patches Critical Vulnerabilities in Small Business Routers, SD-WAN
* New 'Hildegard' Malware Targets Kubernetes Systems
* Airbus CyberSecurity Subsidiary Stormshield Discloses Data Breach
* Number of ICS Vulnerabilities Continued to Increase in 2020: Report
* Vulnerabilities in Realtek Wi-Fi Module Expose Many Devices to Remote Attacks
* Canada Probe Concludes Clearview AI Breached Privacy Laws

Infosecurity Magazine

* Paralegal's Pal Admits Outing Witnesses
* Law Firm Data Breach Impacts UPMC Patients
* Emsisoft Suffers System Breach
* Remote Desktop Protocol Attacks Surge by 768%
* NHS Staff Hit by Almost 140,000 Malicious Emails in 2020
* Europol Breaks $14m Card Fraud Ring
* Tens of Thousands of Patient Files Leaked in US Hospital Attacks
* Crypto Fund Founder Pleads Guilty to $100m Fraud Scheme
* South Carolina Plans Cyber-Ecosystem
* Cyber-Attack on Woodland Trust
* National Cyber League Expands HBCU Scholarship Program
* BA Data Breach Victims Granted Extension to File Claims

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* There's Still No Real Answer to the Ransomware Epidemic
* Every Employee is Part of Your Security
* Cold Reality Dawns: Covid-19 Is Likely Here to Stay But Your Employees Are Vulnerable
* How the United States Lost to Hackers, And Why The New President Wants To Fix It With 10 Billion Doll
* One-Fourth of a SOC's Life Is Researching Sketchy Emails
* SOC teams spend nearly a quarter of their day handling suspicious emails
* Hackers are Winning the Cyberwar, Largely Because They Target People
* Using Legitimate Services to Bypass Phishing Protections
* A Master Class on IT Security: Roger Grimes Teaches Ransomware Mitigation
* CyberheistNews Vol 11 #05 [Heads Up] CISA's New War on Ransomware Awareness Campaign

ISC2.org Blog

* Using a Crisis Wisely
* Addressing the Human Element of Security: Awareness & Training Programs
* CISSPs from Around the Globe: An Interview with Melissa Parsons
* Employment for Security Analysts to Grow 31% by 2029
* Remote Work During the Pandemic: What We Got Wrong

HackRead

* Threat actor selling 158,000 Canadian, US credit card data
* Top Barcode Scanner app infected 10 million users with malware
* Hundred thousand Spotify accounts leaked in credential stuffing attack
* Best Torrent Sites for 2021
* Generation Z least likely to share their location data with government
* The Great Suspender Chrome extension used by millions was malware
* Malicious Chrome extensions can steal data by abusing Sync feature

Koddos

* Threat actor selling 158,000 Canadian, US credit card data
* Top Barcode Scanner app infected 10 million users with malware
* Hundred thousand Spotify accounts leaked in credential stuffing attack
* Best Torrent Sites for 2021
* Generation Z least likely to share their location data with government
* The Great Suspender Chrome extension used by millions was malware
* Malicious Chrome extensions can steal data by abusing Sync feature

LATEST NEWS

Naked Security

* 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!
* S3 Ep18: Apple emergency, crypto blunder and botnet takedown [Podcast]
* Free coffee! Belgian researcher hacks prepaid vending machines
* What should you say if you have a data breach? Catch up with Jason Nurse at Sophos Evolve
* Naked Security Live - What if my password manager gets hacked?
* Emotet takedown - Europol attacks "world's most dangerous malware"
* GnuPG crypto library can be pwned during decryption - patch now!

Threat Post

* Billions of Passwords Offered for $2 in Cyber-Underground
* Critical WordPress Plugin Flaw Allows Site Takeover
* Ransomware Demands Spike 320%, Payments Rise
* Fake Forcepoint Google Chrome Extension Hacks Windows Users
* WestRock Ransomware Attack Hinders Packaging Production
* Industrial Networks See Sharp Uptick in Hackable Security Holes
* Unpatched WordPress Plugin Code-Injection Bug Afflicts 50K Sites
* Google Chrome Zero-Day Afflicts Windows, Mac Users
* Ransomware Attacks Hit Major Utilities
* Android Devices Prone to Botnet's DDoS Onslaught

Null-Byte

* 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
* Stay Fully in Sync with Your Remote Team Using TimeSync Pro
* How to Get an Internet Connection in the Middle of Nowhere to Hack Remotely

LATEST NEWS

IBM Security Intelligence

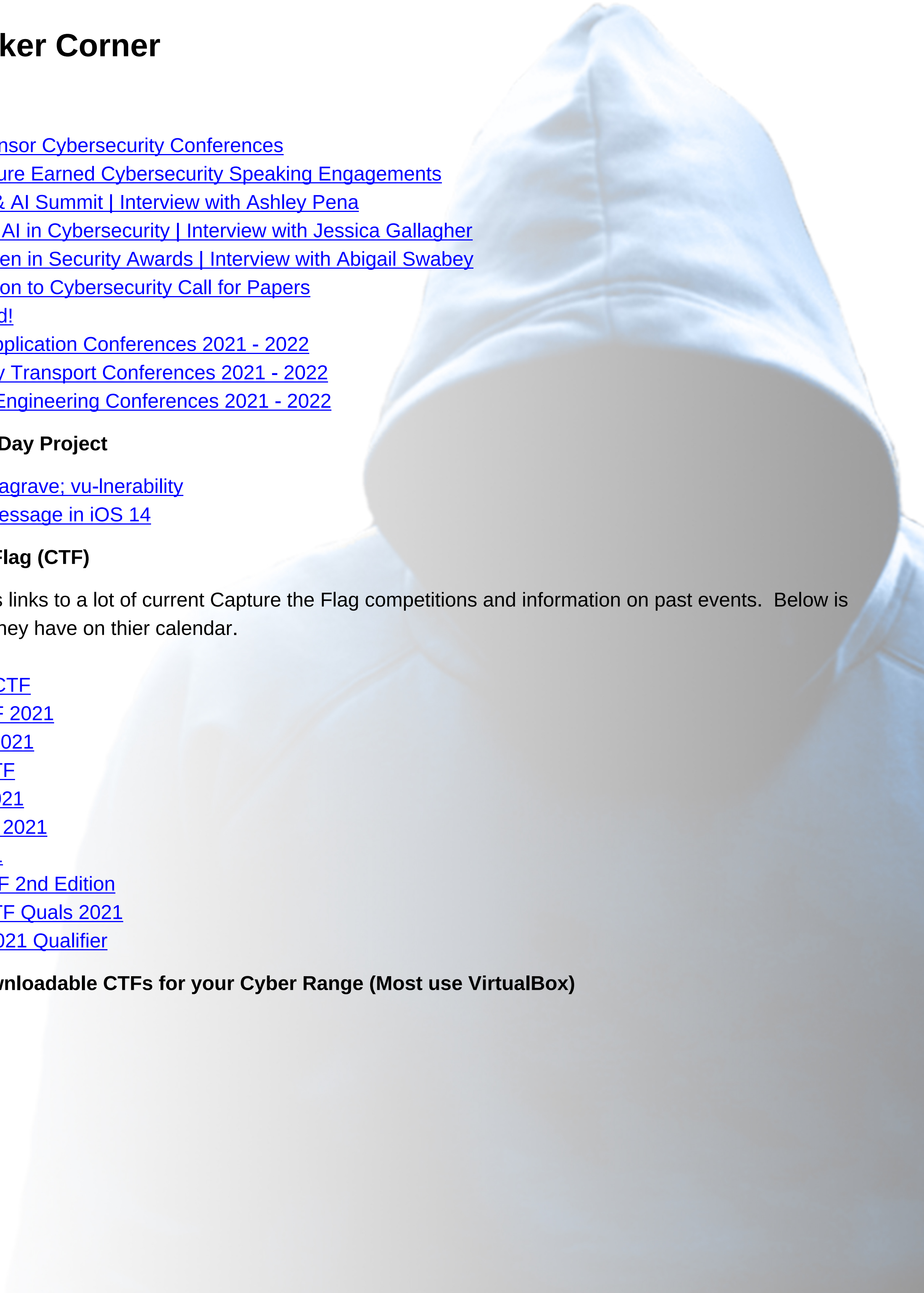
* Cybersecurity Insurance Pros and Cons: Is it the Best Policy?
* Cloud Native Tools Series Part 1: Go Beyond Traditional Security
* Moving Threat Identification From Reactive to Predictive and Preventative
* Remote Work Trends: How Cloud Computing Security Changed
* 5 Ways Companies Can Protect Personally Identifiable Information
* How Doxing Affects Gen Z
* Does a Strong Privacy Program Make for a Stronger Security Program?
* Link Previews Could Threaten Your Digital Security and Privacy
* School's Out for Ransomware
* How to Shut Down Business Units Safely

InfoWorld

* Java 17 proposal would enhance PRNGs
* Homebrew 3 brings Apple Silicon support
* How to use implicit and explicit operators in C#
* Hidden figures: 7 Black programmers you should know
* 7 best practices for remote development teams
* The future of work: Coming sooner than you think
* GitHub increases developer's cut of GitHub Marketplace sales
* You're doing cloud-based AI and machine learning wrong
* Visual Studio Code 1.53 brings customizable search mode
* Got the Python basics down? Read this book next

C4ISRNET - Media for the Intelligence Age Military

* British military's space campaign picks up steam with 'Skynet' upgrade
* Russia-Iran cooperation poses challenges for US cyber strategy, global norms
* French military orders first sigint suite to work across all services
* For CAE the future means expansion in cyber, space and more defense acquisitions
* Politics should not determine location for US Space Command
* Pentagon urged to work with industry on 5G network development
* Cyber denial of service is cyber attack
* In year two, the Space Force is focused on international partnerships
* A reshuffling of House subcommittees to boost oversight of military tech
* The Space Force considers a new mission: tactical satellite imagery



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.

* SecureBug CTF
* Tenable CTF 2021
* Union CTF 2021
* darkCON CTF
* Aero CTF 2021
* zer0pts CTF 2021
* UTCTF 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

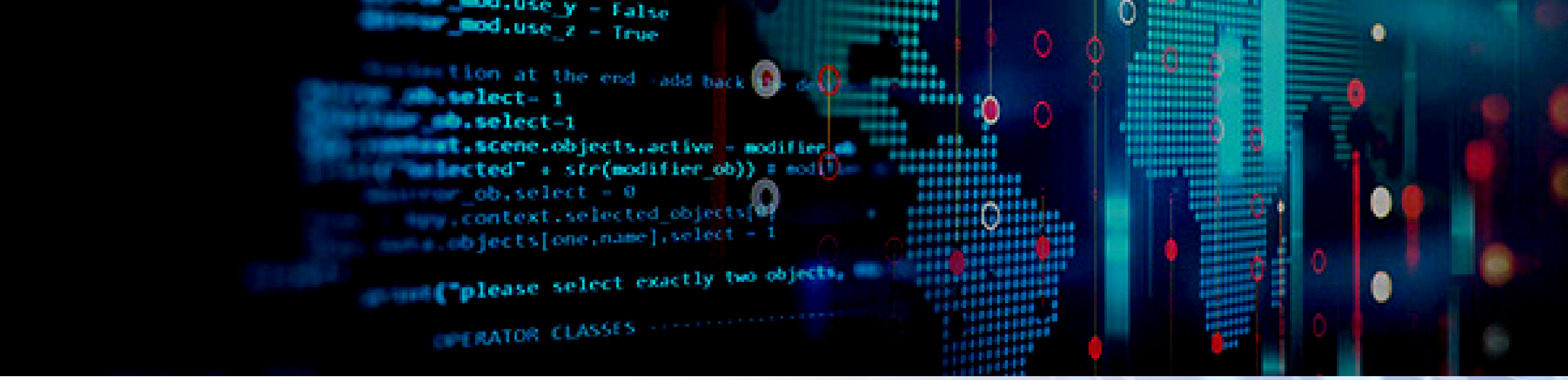
* AIDE 0.17.2
* TOR Virtual Network Tunneling Tool 0.4.4.7
* Clam AntiVirus Toolkit 0.103.1
* Mandos Encrypted File System Unattended Reboot Utility 1.8.14
* SQLMAP - Automatic SQL Injection Tool 1.5.2
* Wireshark Analyzer 3.4.3
* AIDE 0.17.1
* Sifter 11.5
* AIDE 0.17
* Logwatch 7.5.5

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 169: Apple Forensics: Magic Keystrokes - Single User Mode key
* Episode 168: Apple Forensics: Magic Keystrokes - alt/option key
* Episode 167: Digital Forensics & Knot Tying
* Episode 166: Collecting Machine Config on Mac - Part 3

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

* Unlimited LTE Hotspot on PC via Phone or USB modem! -GlytchTips
* Emotet Botnet Sinkholed, Apple Adds App Tracking Opt-In - ThreatWire
* Li-Ion FPV Drone Showdown! w/Glytch & Darren

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* MORGAN WALLEN CANCELLED for stupidity
* SJW's CANCELLING EXTREMIST PODCASTS
* COVID RESTRICTIONS FOR FOUR MORE YEARS
* GOOGLE FAILING with Record Revenue

Security Now

* NAT Slipstreaming 2.0 - SUDO Was Pseudo Secure, BigNox Supply-Chain Attack, iMessage in a Sandbox
* Comparative Smartphone Security - Browser Password Managers, Adobe Flash Repercussions, SolarWinds

Troy Hunt

* Weekly Update 229

Intel Techniques: The Privacy, Security, & OSINT Show

* 205-Five Shows In One
* 204-Radio Frequency Monitoring

Proof of Concept (PoC) & Exploits

Packet Storm Security

* SmartFoxServer 2X 2.17.0 Remote Code Execution
* Unibox 2.4 CSRF / Remote Code Execution
* SmartFoxServer 2X 2.17.0 Credential Disclosure
* Unibox Cross Site Request Forgery
* SmartFoxServer 2X 2.17.0 God Mode Console WebSocket Cross Site Scripting
* Millewin 13.39.028 Unquoted Service Path / Insecure Permissions
* Backdoor.Win32.Wollf.15 Missing Authentication
* Alt-N MDaemon Webmail 20.0.0 Cross Site Scripting
* Trojan-Spy.Win32.WinSpy.vwl Insecure Permissions
* Trojan-Spy.Win32.WebCenter.a Information Disclosure
* WordPress Supsystic Backup 2.3.9 Local File Inclusion
* Trojan-Spy.Win32.SpyEyes.awow Insecure Permissions
* Trojan.Win32.Delf.uq Insecure Permissions
* Email-Worm.Win32.Sircam.eb Insecure Permissions
* WordPress Supsystic Contact Form 1.7.5 XSS / SQL Injection
* Trojan.Win32.Cospet.abg Insecure Permissions
* Trojan.Win32.Comei.pgo Insecure Permissions
* Trojan-Spy.Win32.SpyEyes.auwl Insecure Permissions
* WordPress Supsystic Data Tables Generator 1.9.96 XSS / SQL Injection
* Trojan-Spy.Win32.SpyEyes.auqj Insecure Permissions
* Trojan.Win32.Gentee.h Insecure Permissions
* YetiShare File Hosting Script 5.1.0 Server-Side Request Forgery
* Microsoft Internet Explorer 11 Use-After-Free
* WordPress Supsystic Digital Publications 1.6.9 XSS / DoS / Traversal
* WordPress Supsystic Membership 1.4.7 SQL Injection

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

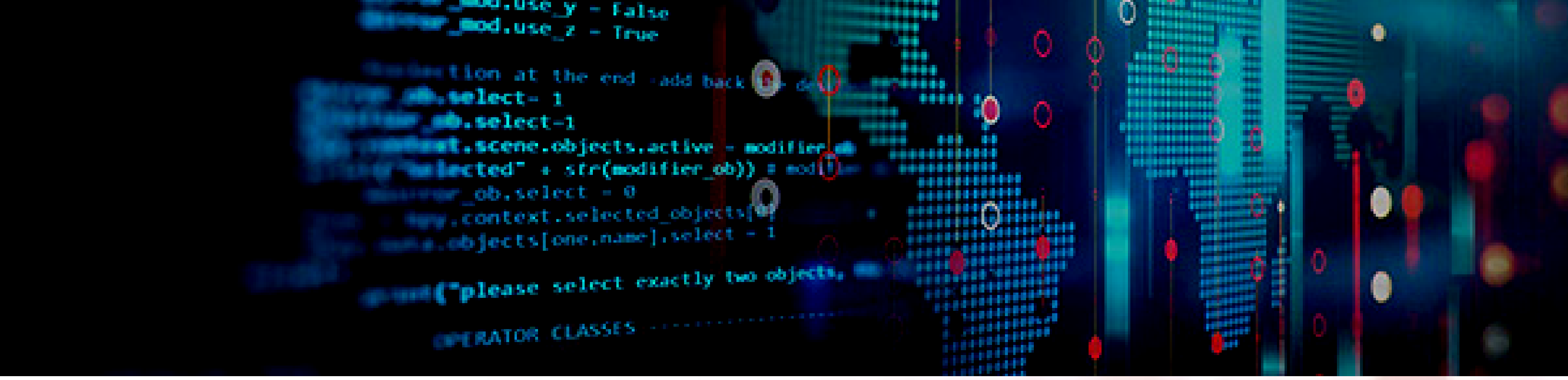
* [webapps] WordPress Plugin Supsystic Backup 2.3.9 - Local File Inclusion
* [webapps] WordPress Plugin Supsystic Contact Form 1.7.5 - Multiple Vulnerabilities
* [webapps] WordPress Plugin Supsystic Data Tables Generator 1.9.96 - Multiple Vulnerabilities
* [webapps] WordPress Plugin Supsystic Digital 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)
* [webapps] Alt-N MDaemon webmail 20.0.0 - 'Contact name' Stored Cross Site Scripting (XSS)
* [local] AMD Fuel Service - 'Fuel.service' Unquote Service Path
* [webapps] YetiShare File Hosting Script 5.1.0 - 'url' Server-Side Request Forgery
* [webapps] WordPress Plugin Supsystic Pricing Table 1.8.7 - Multiple Vulnerabilities
* [webapps] WordPress Plugin Supsystic Ultimate Maps 1.1.12 - 'sidx' SQL injection
* [webapps] WordPress Plugin Welcart e-Commerce 2.0.0 - 'search[order_column][0]' SQL injection
* [local] Millewin 13.39.146.1 - Local Privilege Escalation
* [webapps] Jenzabar 9.2.2 - 'query' Reflected XSS.
* [webapps] SmartFoxServer 2X 2.17.0 - God Mode Console WebSocket XSS
* [local] SmartFoxServer 2X 2.17.0 - Credentials Disclosure
* [local] SmartFoxServer 2X 2.17.0 - God Mode Console Remote Code Execution
* [webapps] SEO Panel 4.6.0 - Remote Code Execution (2)
* [webapps] PhreeBooks 5.2.3 ERP - Remote Code Execution (2)
* [webapps] LiteSpeed Web Server Enterprise 5.4.11 - Command Injection (Authenticated)
* [local] Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege Escalation (2)
* [local] Sudo 1.9.5p1 - 'Baron Samedit ' Heap-Based Buffer Overflow Privilege Escalation (1)
* [webapps] Car Rental Project 2.0 - Arbitrary File Upload to Remote Code Execution

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
```

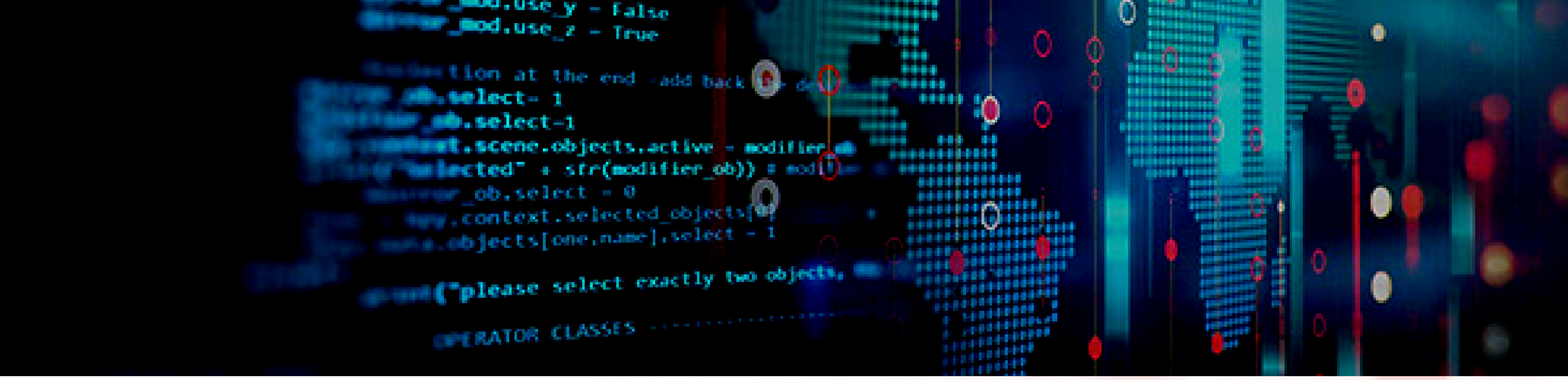
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://9dejulio.gob.ar
https://9dejulio.gob.ar notified by K4TSUY4-GH05T
http://lcbkp.gov.pk
http://lcbkp.gov.pk notified by H45H_C47
https://pa-lumajang.go.id/styo.php
https://pa-lumajang.go.id/styo.php notified by Cubjrnet7
http://perpustakaan.pn-bireuen.go.id/0x48.txt
http://perpustakaan.pn-bireuen.go.id/0x48.txt notified by FRK48
http://loncopue.gob.ar
http://loncopue.gob.ar notified by K4TSUY4-GH05T
https://www.elections.gov.bz/Sans.php
https://www.elections.gov.bz/Sans.php notified by 1K4lL_*
http://www.pn-bengkalis.go.id/1.txt
http://www.pn-bengkalis.go.id/1.txt notified by Mr.Rm19
https://dinsos.pandeglangkab.go.id
https://dinsos.pandeglangkab.go.id notified by Riyan1337
http://ppid.pandeglangkab.go.id
http://ppid.pandeglangkab.go.id notified by Riyan1337
http://www.tumbonbanduea.go.th/index.php
http://www.tumbonbanduea.go.th/index.php notified by Imkey7
https://www.angt.go.th/Mr_Sakib.php
https://www.angt.go.th/Mr_Sakib.php notified by Royal Battler BD
https://www.nonglong.go.th/-.txt
https://www.nonglong.go.th/-.txt notified by Imkey7
https://www.pa-fakfak.go.id/Sans.php
https://www.pa-fakfak.go.id/Sans.php notified by 1K4lL_*
http://pn-fakfak.go.id/Sans.php
http://pn-fakfak.go.id/Sans.php notified by 1K4lL_*
http://www.luh.gov.sc/ma.html
http://www.luh.gov.sc/ma.html notified by Moroccan Revolution
http://www.ict.gov.sc/ma.html
http://www.ict.gov.sc/ma.html notified by Moroccan Revolution
http://sicoex.minco.gov.ao/ma.html
http://sicoex.minco.gov.ao/ma.html notified by Moroccan Revolution


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

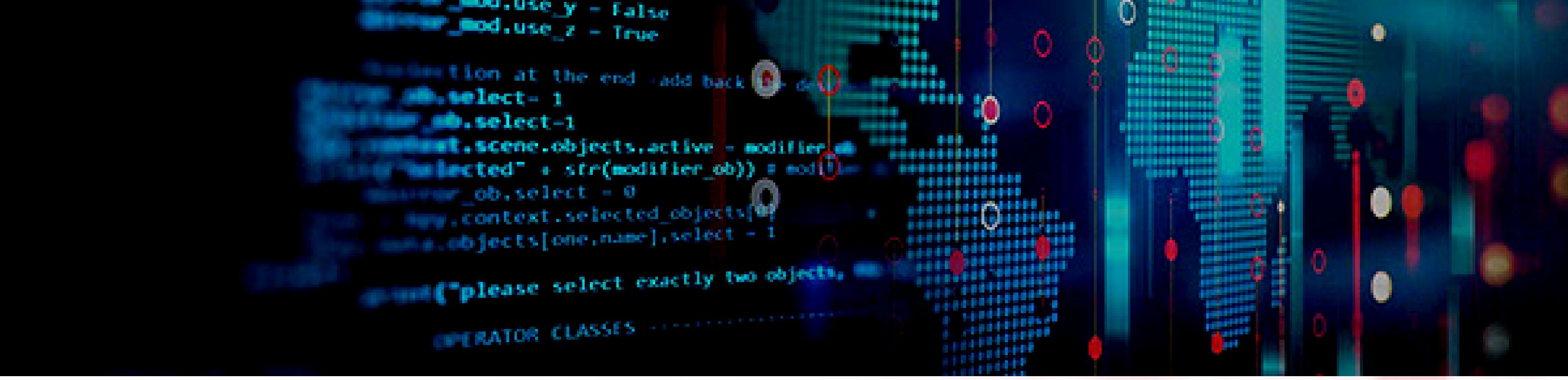
Dark Web News

Darknet Live

[The Darknetlive PGP Key Has Been Rotated]
The time has come for rotation of this site's PGP key. This post serves as a public announcement of the rotation. (via darknetlive.com)
[Fraudster Forfeited 1,700 Bitcoin but Not the Password...]
A fraudster is refusing to give police the decryption key to his Bitcoin wallet worth more than $60 million. (via darknetlive.com)
[Alleged Wallstreet Market Vendor to Stand Trial This Month]
Three German men will be standing trial for allegedly selling a wide variety of drugs on WallStreet Market. (via darknetlive.com)
[XMR.to, a Popular Monero Exchange, is Shutting Down]
The popular Monero to Bitcoin exchange, XMR.to, is shutting down as a result of increasingly invasive money laundering laws and regulations. (via darknetlive.com)

Dark Web Link

[Wallstreet Market Vendor Will Face Trial This Month]
Three alleged German men are about to face trial for selling a wide variety of drugs on a now-defunct dark web marketplace, Wallstreet Market. The indictment had accused those three men of earning over 211,000 euros via at least 2,756 transactions on the darknet market. The accused trio belonged from Germany, North Rhine-Westphalia and Herford. [...] The post Wallstreet Market Vendor Will Face Trial This Month appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Stolen Mail: Man Arrested And Received 500+ Charges]
The discovery of the stolen mail from Louisiana, Texas and Arizona residents and the businesses around eight months earlier had propelled what the authorities say has turned into a disturbing dark web investigation. A Louisiana man is facing hundreds of charges related to child pornography and a couple of charges relating to animal sexual abuse. [...] The post Stolen Mail: Man Arrested And Received 500+ Charges appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
[Child Sexual Abuse: Man Shares Media On The Dark Web]
Daniel Joseph Hunter, a 41-years-old office worker, who still lived with his parents, had been sending child sexual abuse images and videos using the dark web from his bedroom. The AFP officers had arrested the accused from his workplace in Sydney's CBD. They say that they have been tipped off, which led to the arrest. [...] The post Child Sexual Abuse: Man Shares Media On The Dark Web appeared first on Dark Web Link | Deep web Onion Links | Darknet News.


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

Trend Micro Anti-Malware Blog

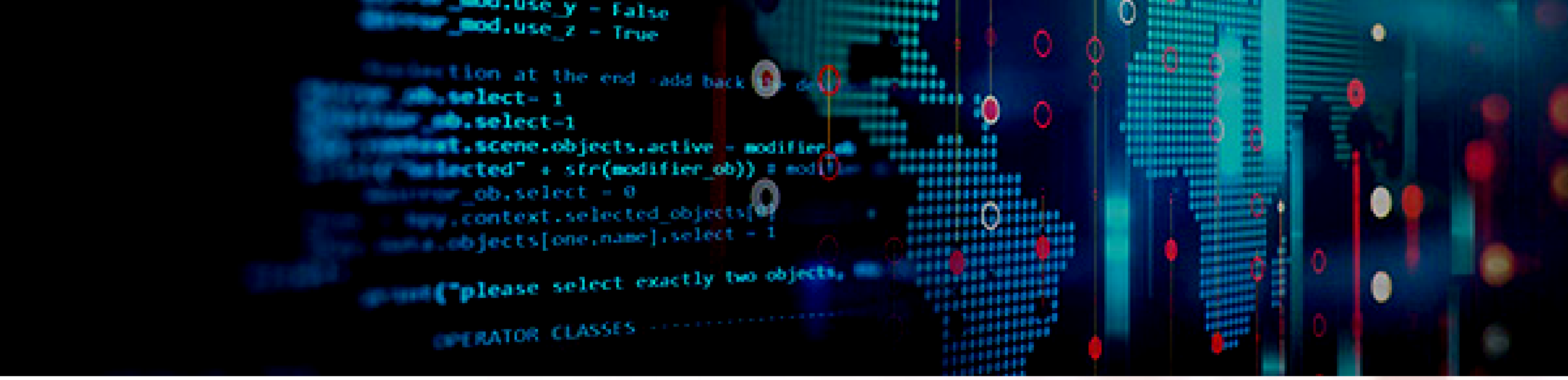
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing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

* 2020 Mobile App Threat Landscape: New Threats Arise, But the Ecosystem Got Safer
* LogoKit: Simple, Effective, and Deceptive
* Attacks on the Capitol Showed the Pitfalls of Having a Narrow View of the Internet
* New Analysis Puts Magecart Interconnectivity into Focus
* RiskIQ's New JARM Feature Supercharges Incident Response
* Skimming a Little Off the Top: 'Meyhod' Skimmer Hits Hair Loss Specialists
* SolarWinds Orion Hack: Know if You're Affected and Defend Your Attack Surface
* Implement FireEye's List of CVEs and Detections with RiskIQ Attack Surface Intelligence
* 'Shadow Academy' Targets 20 Universities Worldwide
* How Do Consumers View Spending and Safety for Online Shopping this Holiday Season? We Took a Look.

FireEye

* 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)
* Addressing the OT-IT Risk and Asset Inventory Gap
* Rapid7 Acquires Leading Kubernetes Security Provider, Alcide
* Metasploit Wrap-Up
* NICER Protocol Deep Dive: Internet Exposure of HTTP and HTTPS
* Upcoming Rapid7 Webcast: How Far Does Your VRM Strategy Go?
* State-Sponsored Threat Actors Target Security Researchers



Advisories

US-Cert Alerts & bulletins

* Mozilla Releases Security Updates for Firefox and Firefox ESR
* Google Releases Security Updates for Chrome
* NCIJTF Releases Ransomware Factsheet
* Cisco Releases Security Updates
* Google Releases Security Updates for Chrome
* Zero-Day Vulnerability in SonicWall SMA 100 Series Version 10.x Products
* Apple Releases Security Updates
* Sudo Heap-Based Buffer Overflow Vulnerability - CVE-2021-3156
* AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
* AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and
* Vulnerability Summary for the Week of February 1, 2021
* Vulnerability Summary for the Week of January 25, 2021

Zero Day Initiative Advisories

ZDI-CAN-13146: Microsoft
A CVSS score 6.6 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12948: Microsoft
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12791: Parallels
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'grigoritchy' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12659: 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: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-13053: Microsoft
A CVSS score 6.6 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is

given until 2021-06-08 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-12654: 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: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12949: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12633: 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: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12925: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'JeongOh Kyea (@kkokkokye) of THEORI' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12790: Parallels

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'grigoritchy' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-13082: Parallels

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L) severity vulnerability discovered by 'renorobert' was reported to the affected vendor on: 2021-02-08, 0 days ago. The vendor is given until 2021-06-08 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-12128: Fortinet

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 'Csaba Fitzl (@theevilbit) of Offensive Security' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12450: Adobe

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 'rookuu' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12142: Samsung

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 'Ye Zhang' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12590: Schneider Electric

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12589: Schneider Electric

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: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12761: Oracle

A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'DongJun Shin' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12586: Schneider Electric

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12604: Schneider Electric

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12997: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin of Trend Micro Mobile Security Research Team' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13014: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin of Trend Micro Mobile Security Research Team' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13013: Apple

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 'Mickey Jin of Trend Micro Mobile Security Research Team' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-12832: VMware

A CVSS score 6.5 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-13118: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mickey Jin of Trend Micro Mobile Security Research Team' was reported to the affected vendor on: 2021-02-03, 5 days ago. The vendor is given until 2021-06-03 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2021-0310-01
Red Hat Security Advisory 2021-0310-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.6.16.

Ubuntu Security Notice USN-4724-1
Ubuntu Security Notice 4724-1 - It was discovered that OpenLDAP incorrectly handled Certificate Exact Assertion processing. A remote attacker could possibly use this issue to cause OpenLDAP to crash, resulting in a denial of service. It was discovered that OpenLDAP incorrectly handled saslAuthzTo processing. A remote attacker could use this issue to cause OpenLDAP to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4723-1
Ubuntu Security Notice 4723-1 - It was discovered that PEAR incorrectly handled symbolic links in archives. A remote attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-4725-1
Ubuntu Security Notice 4725-1 - It was discovered that QEMU incorrectly handled memory in iSCSI emulation. An attacker inside the guest could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. Alexander Bulekov discovered that QEMU incorrectly handled Intel e1000e emulation. An attacker inside the guest could use this issue to cause QEMU to crash, resulting in a denial of service. Various other issues were also addressed.

Red Hat Security Advisory 2021-0433-01
Red Hat Security Advisory 2021-0433-01 - Red Hat Data Grid is a distributed, in-memory data store. This release of Red Hat Data Grid 8.1.1 serves as a replacement for Red Hat Data Grid 8.1.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, deserialization, and memory leak vulnerabilities.

Red Hat Security Advisory 2021-0295-01
Red Hat Security Advisory 2021-0295-01 - This release of Red Hat build of Thorntail 2.7.3 includes security updates, bug fixes, and enhancements. For more information, see the release notes listed in the References section. Issues addressed include information leakage and memory leak vulnerabilities.

Ubuntu Security Notice USN-4721-1
Ubuntu Security Notice 4721-1 - Simon McVittieg discovered that flatpak-portal service allowed sandboxed applications to execute arbitrary code on the host system. A malicious user could create a Flatpak application that set environment variables, trusted by the Flatpak "run" command, and use it to execute arbitrary code outside the sandbox.

Ubuntu Security Notice USN-4722-1
Ubuntu Security Notice 4722-1 - It was discovered that ReadyMedia allowed subscription requests with a delivery URL on a different network segment than the fully qualified event-subscription URL. An attacker could use this to hijack smart devices and cause denial of service attacks. It was discovered that ReadyMedia allowed remote code execution. A remote attacker could send a malicious UPnP HTTP request to the service using HTTP chunked encoding and cause a denial of service.

Red Hat Security Advisory 2021-0421-01
Red Hat Security Advisory 2021-0421-01 - 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 2021-0420-01
Red Hat Security Advisory 2021-0420-01 - Quay 3.4.0 release. Issues addressed include HTTP request smuggling, buffer overflow, information leakage, integer overflow, out of bounds read, and out of bounds write vulnerabilities.

Red Hat Security Advisory 2021-0417-01

Red Hat Security Advisory 2021-0417-01 - AMQ Broker is a high-performance messaging implementation based on ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms. This release of Red Hat AMQ Broker 7.8.1 serves as a replacement for Red Hat AMQ Broker 7.8.0, and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2021-0411-01

Red Hat Security Advisory 2021-0411-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux.

Red Hat Security Advisory 2021-0401-01

Red Hat Security Advisory 2021-0401-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2021-0397-01

Red Hat Security Advisory 2021-0397-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 78.7.0. Issues addressed include an information leakage vulnerability.

Ubuntu Security Notice USN-4720-1

Ubuntu Security Notice 4720-1 - Itai Greenhut discovered that Apport incorrectly parsed certain files in the /proc filesystem. A local attacker could use this issue to escalate privileges and run arbitrary code. Itai Greenhut discovered that Apport incorrectly handled opening certain special files. A local attacker could possibly use this issue to cause Apport to hang, resulting in a denial of service.

Ubuntu Security Notice USN-4719-1

Ubuntu Security Notice 4719-1 - The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.46 version of the Mozilla certificate authority bundle.

Ubuntu Security Notice USN-4720-2

Ubuntu Security Notice 4720-2 - USN-4720-1 fixed several vulnerabilities in Apport. This update provides the corresponding update for Ubuntu 14.04 ESM. Itai Greenhut discovered that Apport incorrectly parsed certain files in the /proc filesystem. A local attacker could use this issue to escalate privileges and run arbitrary code. Various other issues were also addressed.

Red Hat Security Advisory 2021-0395-01

Red Hat Security Advisory 2021-0395-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a buffer overflow vulnerability.

Ubuntu Security Notice USN-4718-1

Ubuntu Security Notice 4718-1 - It was discovered that fastd incorrectly handled certain packets. An attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2021-0281-01

Red Hat Security Advisory 2021-0281-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

Red Hat Security Advisory 2021-0282-01

Red Hat Security Advisory 2021-0282-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include an XML injection vulnerability.

Oracle Privilege Escalation / Denial Of Service / Code Execution

The Oracle CPU dated 2020 Jan 14 included patches for various issues related to database links and gateways ("Oracle Heterogeneous Services"). Two vulnerabilities in particular might lead to privilege escalation, denial of service, or code execution attacks against Oracle databases.

Red Hat Security Advisory 2021-0384-01

Red Hat Security Advisory 2021-0384-01 - Red Hat Fuse provides a small-footprint, flexible, open source enterprise service bus and integration platform. Red Hat A-MQ is a standards compliant messaging system that is tailored for use in mission critical applications. This patch is an update to Red Hat Fuse 6.3 and Red Hat A-MQ 6.3. It includes bug fixes, which are documented in the patch notes accompanying the package on the download page. Issues addressed include bypass, code execution, and deserialization vulnerabilities.

Red Hat Security Advisory 2021-0383-01

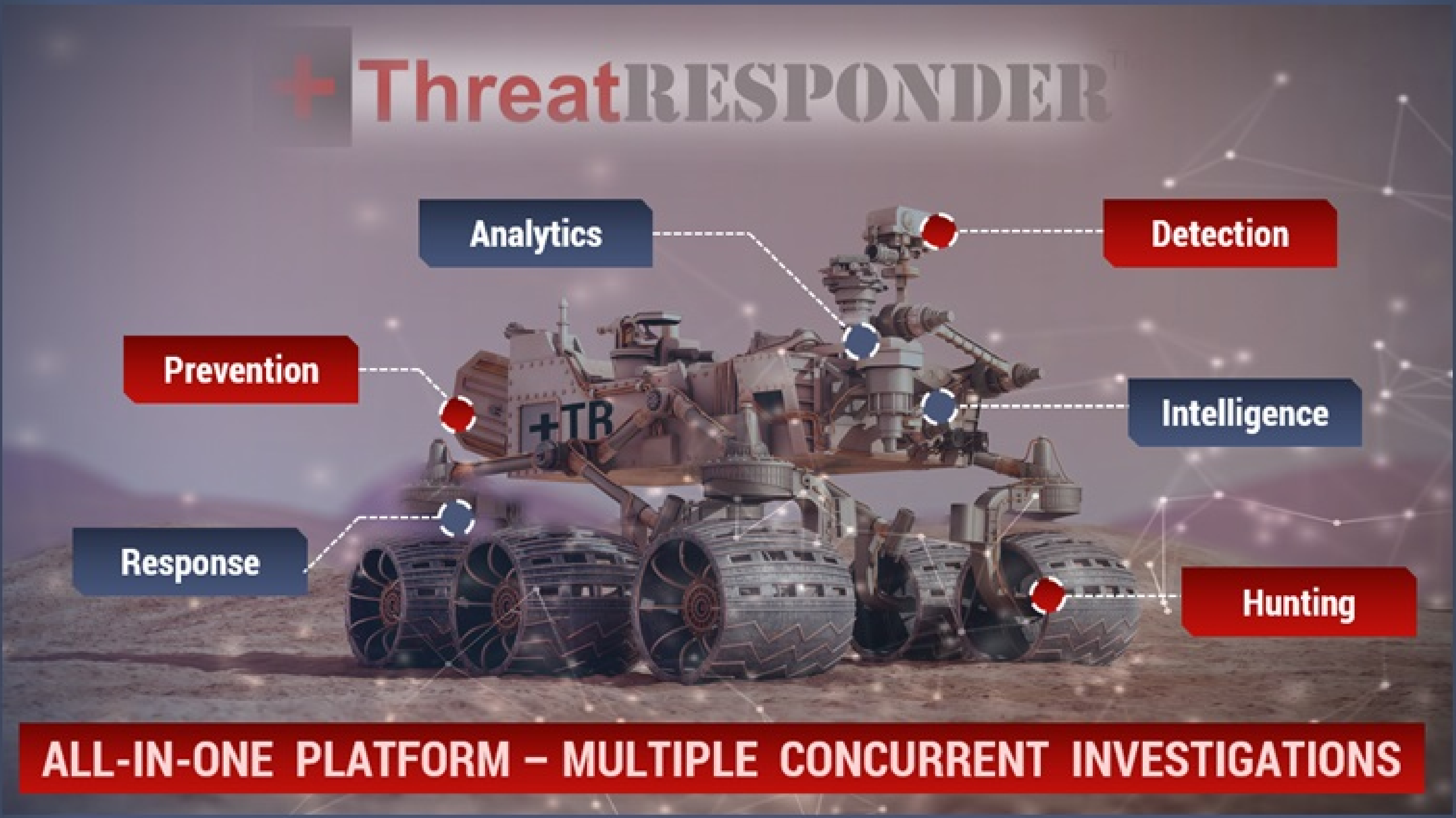
Red Hat Security Advisory 2021-0383-01 - The ovirt-engine package provides the Red Hat Virtualization Manager, a centralized management platform that allows system administrators to view and manage virtual machines. The Manager provides a comprehensive range of features including search capabilities, resource management, live migrations, and virtual infrastructure provisioning. The Manager is a JBoss Application Server application that provides several interfaces through which the virtual environment can be accessed and interacted with, including an Administration Portal, a VM Portal, and a Representational State Transfer Application Programming Interface.

Are You…

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

Do DFIR Investigations Better

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



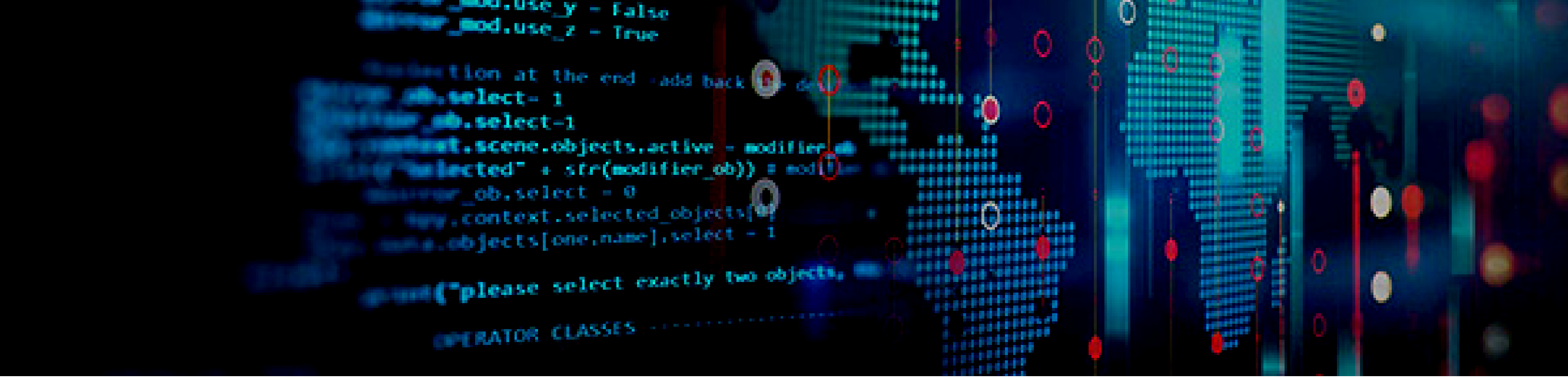
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com



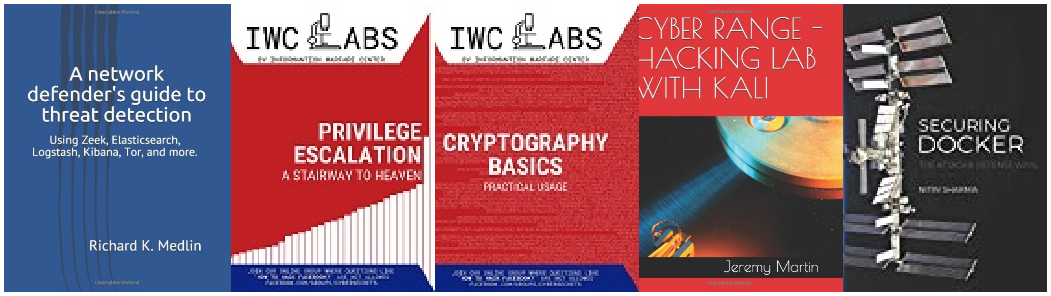
The Cyber Secrets publications on Amazon

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

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

CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
CYBER SECRETS
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
SOCRANGE
LINUX
CYBER SECRETS
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
CYBER SECRETS
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
CYBER SECRETS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

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