Feb-13-23

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

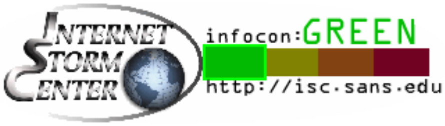
netSecurity®

CYBER WEEKLY AWARENESS REPORT

February 13, 2023

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

Summary



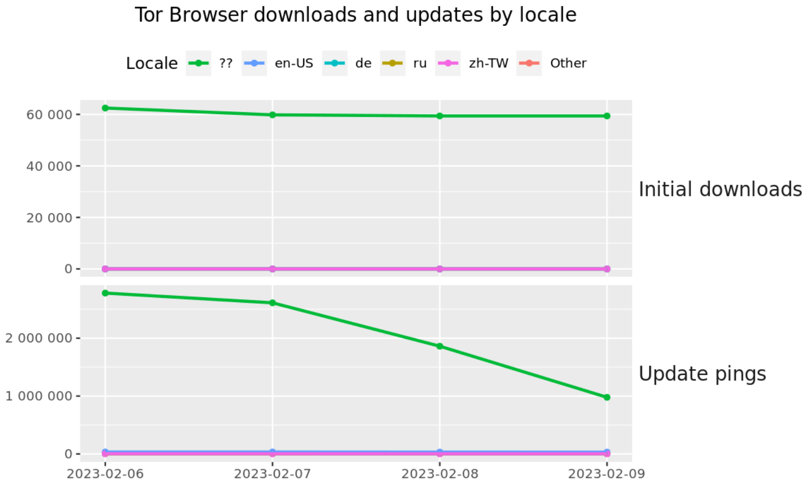
Internet Storm Center Infocon Status

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

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

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



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * 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

* Valve Waited 15 Months To Patch High Severity Flaw. A Hacker Pounced.
* Musk Seems To Think His Own Employees Are Shadowbanning Him
* Novel Phishing Campaign Takes Screenshots Before Payload Delivery
* Australian Government Bans Chinese CCTV Tech
* Google's Bard AI Bot Mistake Wipes $100 Billion Off Shares
* Uncle Sam Wants To Strip The IoS Out Of IoT With Light Crypto
* Codebreakers Decipher Mary, Queen Of Scots' Secret Letters 436 Years After Her Execution
* Auto Dealers Are Prime Targets For Hackers, Warn Researchers
* Netflix Extends Crackdown On Password Sharing To More Countries
* U.S., Britain Impose Sanctions On Russia's Trickbot Hacking Gang
* Hackers Are Selling A Service That Bypasses ChatGPT Restrictions On Malware
* Mysterious Leak Of Booking.com Data Being Used For Scams
* Mysterious Russian Satellites Are Now Breaking Apart In Low Earth Orbit
* Suspect In Finnish Psychotherapy Blackmail Hack Arrested
* Scammers Steal $4 Million In Crypto During Face-To-Face Meeting
* Top Android Phones From China Are Packed With Spyware, Research Finds
* Google Launches ChatGPT Rival Bard
* Lawsuit Blast GoodRx, Meta Over Egregious Privacy Practices
* QNAP Backtracks On Scope Of Critical NAS Bug
* Here's A List Of Proxy IPs To Help Block KillNet's DDoS Bots
* Dutch Police Read Messages Of Encrypted Messenger Exclu
* School Laptop Auction Devolves Into Extortion Allegation
* Iran Crew Stole Charlie Hebdo Database, Says Microsoft
* No Evidence Global Ransomware Hack Was By State Entity, Italy Says
* Former Ubiquiti Dev Pleads Guilty In Data Theft And Extortion Case

Krebs on Security

* U.S., U.K. Sanction 7 Men Tied to Trickbot Hacking Group
* KrebsOnSecurity in Upcoming Hulu Series on Ashley Madison Breach
* Finland's Most-Wanted Hacker Nabbed in France
* Experian Glitch Exposing Credit Files Lasted 47 Days
* Administrator of RSOCKS Proxy Botnet Pleads Guilty
* New T-Mobile Breach Affects 37 Million Accounts
* Thinking of Hiring or Running a Booter Service? Think Again.
* Microsoft Patch Tuesday, January 2023 Edition
* Identity Thieves Bypassed Experian Security to View Credit Reports
* Happy 13th Birthday, KrebsOnSecurity!

LATEST NEWS

Dark Reading

* Reddit Hack Shows Limits of MFA, Strengths of Security Training
* Trickbot Members Sanctioned for Pandemic-Era Ransomware Hits
* Integreon Launches Cyber Incident Response Offering with Development of AI-Based Review and Integrati
* MagicWeb Mystery Highlights Nobelium Attacker's Sophistication
* Malicious Game Mods Target Dota 2 Game Users
* Attacker Allure: A Look at the Super Bowl's Operational Cyber-Risks
* Addressing the Elephant in the Room: Getting Developers & Security Teams to Work Together
* Google Cloud Connects Chronicle to Health ISAC Feed
* Reddit Breached With Stolen Employee Credentials
* NewsPenguin Goes Phishing for Maritime & Military Secrets
* Avast Threat Report: Consumers Plagued With Refund Fraud, Tech Support Scams, and Adware
* 4 Ways to Handle AI Decision-Making in Cybersecurity
* 7 Critical Cloud Threats Facing the Enterprise in 2023
* SynSaber Releases ICS CVE Retrospective: 3 Years of CISA Advisories
* Kaspersky Finds Growing Number of Parents Experiencing Ransomware Attacks on Children's Schools
* Cryptographers Decode Secret Letters of Mary, Queen of Scots
* Phishing Surges Ahead, as ChatGPT & AI Loom
* NIST Picks IoT Standard for Small Electronics Cybersecurity
* In Perfect Harmony: Cybersecurity Regulation Harmonization
* Twitter Implements API Paywall, but Will That Solve Its Enormous Bot Crisis?

The Hacker News

* Honeypot-Factory: The Use of Deception in ICS/OT Environments
* Chinese Tonto Team Hackers' Second Attempt to Target Cybersecurity Firm Group-IB Fails
* Hackers Targeting U.S. and German Firms Monitor Victims' Desktops with Screenshotter
* New ESXiArgs Ransomware Variant Emerges After CISA Releases Decryptor Tool
* Enigma, Vector, and TgToxic: The New Threats to Cryptocurrency Users
* CISA Warns of Active Attacks Exploiting Fortra MFT, TerraMaster NAS, and Intel Driver Flaws
* Researchers Uncover Obfuscated Malicious Code in PyPI Python Packages
* North Korean Hackers Targeting Healthcare with Ransomware to Fund its Operations
* 3 Overlooked Cybersecurity Breaches
* U.K. and U.S. Sanction 7 Russians for TrickBot, Ryuk, and Conti Ransomware Attacks
* Reddit Suffers Security Breach Exposing Internal Documents and Source Code
* Critical Infrastructure at Risk from New Vulnerabilities Found in Wireless IIoT Devices
* Webinar: Learn How to Comply with New Cyber Insurance Identity Security Requirements
* NewsPenguin Threat Actor Emerges with Malicious Campaign Targeting Pakistani Entities
* A Hackers Pot of Gold: Your MSP's Data

LATEST NEWS

Security Week

* Play Ransomware Group Claims Attack on A10 Networks
* Cybersecurity M&A Roundup: 40 Deals Announced in January 2023
* SecurityWeek Cyber Insights 2023 Series
* US Blacklists 6 Chinese Entities Over Balloon Program
* Microsoft OneNote Abuse for Malware Delivery Surges
* Siemens Drives Rise in ICS Vulnerabilities Discovered in 2022: Report
* NIST Picks Ascon Algorithms to Protect Data on IoT, Small Electronic Devices
* Security Awareness Training Startup Riot Raises $12 Million
* Military Organizations in Pakistan Targeted With Sophisticated Espionage Tool
* US, South Korea: Ransomware Attacks Fund North Korea's Cyber Operations

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Spear Phishing Attacks Increase 127% as Use of Impersonation Skyrockets
* U.K. Citizens See 82% Increase in Advanced Fee Scams in the Last Year
* Hackers Work Around ChatGPT Malicious Content Restrictions to Create Phishing Email Content
* Be Wary of Survey Scams
* [HEADS UP] If You're a Fan of 'The Last of Us' You May be Targeted for These Campaigns
* Do Not Fall Victim to Cyber Attacks - Find Out What the Latest Hiscox Report Reveals!
* [Scam Of The Week] The Turkey-Syria Earthquake
* CyberheistNews Vol 13 #06 [Eye Opener] Russian and Iranian Spear Phishing Campaigns Are Running Rampa
* Thinking Critically About Your Online Behavior
* How Artificial Intelligence Can Make or Break Cybersecurity

ISC2.org Blog

* LATEST CYBERTHREATS AND ADVISORIES - FEBRUARY 10, 2023
* (ISC)&sup2; Puts Members at the Center of Our Cybersecurity Content in 2023
* PREDICTIONS 2023, PART 2: WHAT WILL THE NEW YEAR BRING FOR THE INFOSEC COMMUNITY?
* Calling All CISSP-ISSMP and CISSP Certification Holders
* Analysis: CircleCI attackers stole session cookie to bypass MFA

HackRead

* Iranian State TV Hacked During President's Speech on Revolution Day
* Geo Targetly URL Shortener Abused in Phishing Scam
* Reddit Hacked After Employee Bites on Phishing Scam
* Bard AI Causes Google Losses of $100 Billion
* Weee! Grocery Service Hacked, 1.1m Accounts Leaked
* SaaS Security Best Practices: Safeguard Consumer Data
* Tor Network Hit By a Series of Ongoing DDoS Attacks

Koddos

* Iranian State TV Hacked During President's Speech on Revolution Day
* Geo Targetly URL Shortener Abused in Phishing Scam
* Reddit Hacked After Employee Bites on Phishing Scam
* Bard AI Causes Google Losses of $100 Billion
* Weee! Grocery Service Hacked, 1.1m Accounts Leaked
* SaaS Security Best Practices: Safeguard Consumer Data
* Tor Network Hit By a Series of Ongoing DDoS Attacks

LATEST NEWS

Naked Security

* Reddit admits it was hacked and data stolen, says "Don't panic"
* S3 Ep121: Can you get hacked and then prosecuted for it? [Audio + Text]
* OpenSSL fixes High Severity data-stealing bug - patch now!
* VMWare user? Worried about "ESXi ransomware"? Check your patches now!
* Tracers in the Dark: The Global Hunt for the Crime Lords of Crypto
* Finnish psychotherapy extortion suspect arrested in France
* OpenSSH fixes double-free memory bug that's pokable over the network
* S3 Ep120: When dud crypto simply won't let go [Audio + Text]
* Password-stealing "vulnerability" reported in KeePass - bug or feature?
* GitHub code-signing certificates stolen (but will be revoked this week)

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

Null-Byte

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

LATEST NEWS

IBM Security Intelligence

* Six Common Ways That Malware Strains Get Their Names
* What is a Pentester, and Can They Prevent Data Breaches?
* Cybersecurity in the Next-Generation Space Age, Pt. 1: Introduction to New Space
* What CISOs Should Know About Hacking in 2023
* How to Spot a Nefarious Cryptocurrency Platform
* Why Crowdsourced Security is Devastating to Threat Actors
* Bridging the 3.4 Million Workforce Gap in Cybersecurity
* The Evolution of Antivirus Software to Face Modern Threats
* How Do Threat Hunters Keep Organizations Safe?
* Contain Breaches and Gain Visibility With Microsegmentation

InfoWorld

* Gatsby, Netlify, and the gravitational pull of general-purpose platforms
* Zero-shot learning and the foundations of generative AI
* 10 reasons to worry about generative AI
* Android 14 preview for developers arrives
* 3 reasons not to repatriate cloud-based apps and data sets
* GitHub lays off 10% of workforce, plans to go fully remote to cut costs
* Deno 1.30 backs built-in Node.js modules
* Intro to Remix: A leader in full-stack evolution
* The best new features in ASP.NET Core 7
* DataStax launches Astra Block to support Web3 applications

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

The Hacker Corner

Conferences

* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* Exploiting null-dereferences in the Linux kernel
* DER Entitlements: The (Brief) Return of the Psychic Paper

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.

* Incognito 4.0
* 0xL4ughCTF 2023
* HackTM CTF Quals 2023
* pbctf 2023
* VU CYBERTHON 2023
* Trellix HAX 2023
* Cyber-Bytes 2023
* CTF After Dark - Winter 2023
* KalmarCTF 2023
* hxp CTF 2022

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

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

Tools & Techniques

Packet Storm Security Tools Links

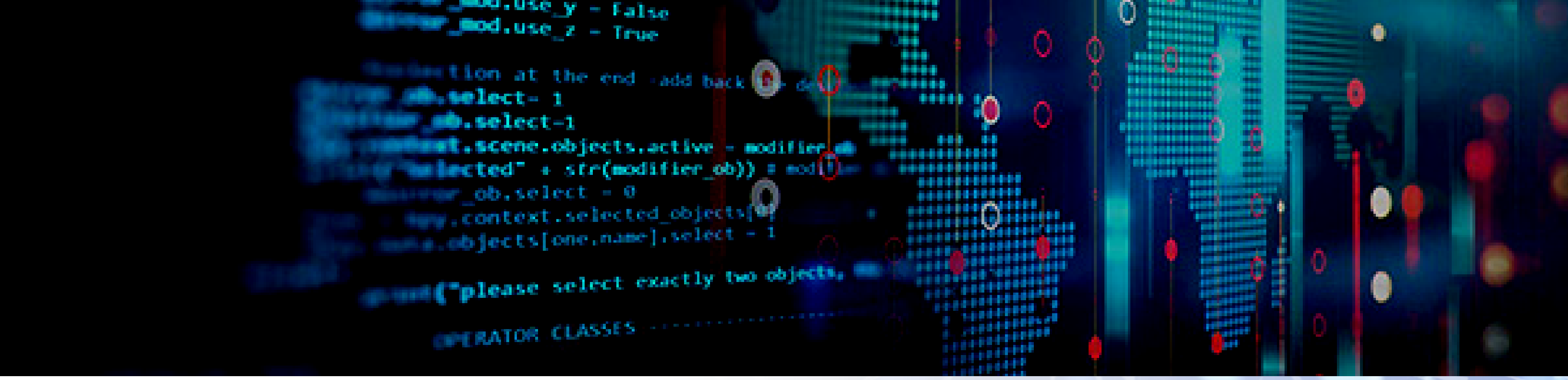
* Mandos Encrypted File System Unattended Reboot Utility 1.8.16
* OpenSSL Toolkit 3.0.8
* OpenSSL Toolkit 1.1.1t
* AIDE 0.18
* Falco 0.34.0
* NDC Protocol Fuzzer
* GNUnet P2P Framework 0.19.3
* Zeek 5.0.6
* OpenSSH 9.2p1
* Suricata IDPE 6.0.10

Kali Linux Tutorials

* YATAS : A Simple Tool To Audit Your AWS Infrastructure For Misconfiguration
* AceLdr : Cobalt Strike UDRL For Memory Scanner Evasion
* REST-Attacker : A Proof-Of-Concept For The Feasibility Of Testing
* Why Data Breach Protection Must Include Physical Security
* Types Of Security Breaches: Physical And Digital
* DotDumper : An Automatic Unpacker & Logger For DotNet Framework
* Security Cameras: Bridging The Gap Between Physical And Digital Cybersecurity
* ExchangeFinder : Find Microsoft Exchange Instance For A Given Domain And Identify The Exact Version
* Villain : Windows And Linux Backdoor Generator And Multi-Session Handler
* PXEThief : Extract Passwords From The Operating System Deployment Functionality

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input


_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)) # modif
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown (STAR) | Live Stream
* SANS Threat Analysis Rundown
* The Truth about Ransomware: Its not Complicated!
* Think DFIRently: What is Digital Forensics & Incident Response (DFIR)?

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

* Learn Polymorphic Powershell Payload Techniques! [PAYLOAD]
* Microsoft Verified Publisher System Abused For Data Exfiltration - ThreatWire
* Staged and non-staged payloads for the USB Rubber Ducky [PAYLOAD]

The PC Security Channel [TPSC]

* New Discord Ransomware
* Elon Musk Cryptoscams

Eli the Computer Guy

* STARTUP LIFE... kinda sucks... ;)
* eBeggar Wednesday on Thursday
* FAT SHAMMING at Amusement Park - "Average" US Male waist is 40+ inches...
* MORE TECH LAYOFFS - jack dorsey screwing block employees...

Security Now

* How ESXi Fell - EU Internet Surveillance, QNAP returns, .DEV is always HTTPS
* Data Operand Independent Timing - Old Android apps, Kevin Rose, iOS 6.3 and FIDO, Hive hacked

Troy Hunt

* Weekly Update 334

Intel Techniques: The Privacy, Security, & OSINT Show

* 289-Combo Lists & Extreme Privacy Series
* 288-Privacy, Security, & OSINT Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* ChiKoi 1.0 Directory Traversal
* ChiKoi 1.0 Cross Site Scripting
* Monitorr 1.7.6 Shell Upload
* Windows Kernel Registry Virtualization Incompatibility
* Windows Kernel Virtualizable Hive Key Deletion
* WEBY 1.2.5 Cross Site Request Forgery
* Windows Kernsl SID Table Poisoning
* Windows Kernel Key Replication Issues
* SOUND4 LinkAndShare Transmitter 1.1.2 Format String Stack Buffer Overflow
* Zoho ManageEngine Endpoint Central / MSP 10.1.2228.10 Remote Code Execution
* Fortra GoAnywhere MFT Unsafe Deserialization Remote Code Execution
* Windows Kernel Dangling Registry Link Node Use-After-Free
* CKSource CKEditor5 35.4.0 Cross Site Scripting
* ManageEngine ADSelfService Plus Unauthenticated SAML Remote Code Execution
* Nagios XI 5.7.5 Remote Code Execution
* Zoho ManageEngine ServiceDesk Plus 14003 Remote Code Execution
* 101news By Mayuri K 1.0 SQL Injection
* Material Dashboard 2 SQL Injection
* Apache Tomcat On Ubuntu Log Init Privilege Escalation
* Android Binder VMA Management Security Issues
* Windows Kernel Registry Virtualization Memory Corruption
* Lenovo Diagnostics Driver Memory Access
* macOS Dirty Cow Arbitrary File Write Local Privilege Escalation
* F5 Big-IP Create Administrative User
* Oracle Database 12.1.0.2 Spatial Component Privilege Escalation

CXSecurity

* Wordpress Multiple themes - Unauthenticated Arbitrary File Upload
* Fortra GoAnywhere MFT Unsafe Deserialization Remote Code Execution
* ManageEngine ADSelfService Plus Unauthenticated SAML Remote Code Execution
* Lenovo Diagnostics Driver Memory Access
* macOS Dirty Cow Arbitrary File Write Local Privilege Escalation
* F5 Big-IP Create Administrative User
* Apache Tomcat On Ubuntu Log Init Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

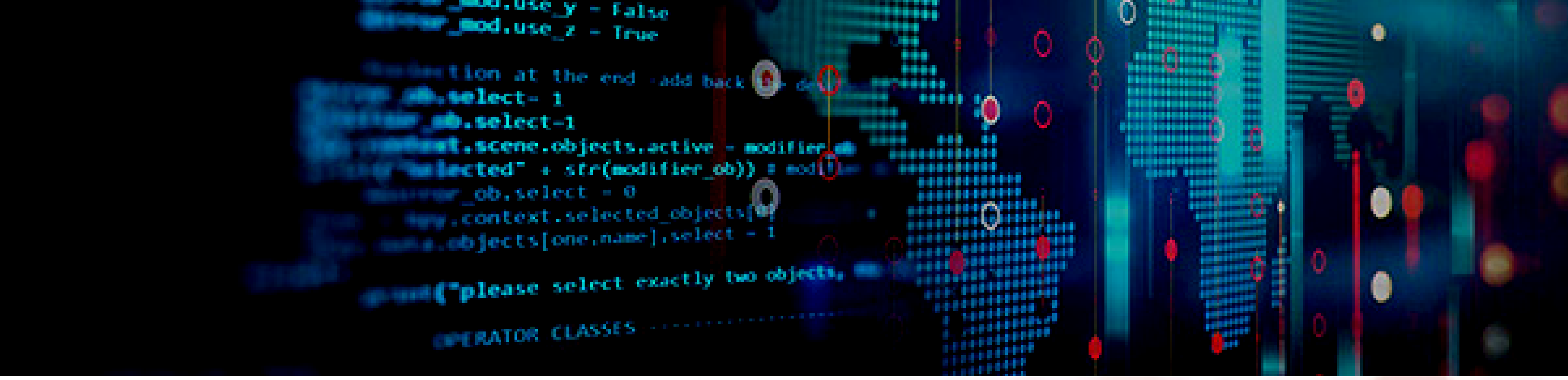
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [webapps] Open Web Analytics 1.7.3 - Remote Code Execution
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - 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
```

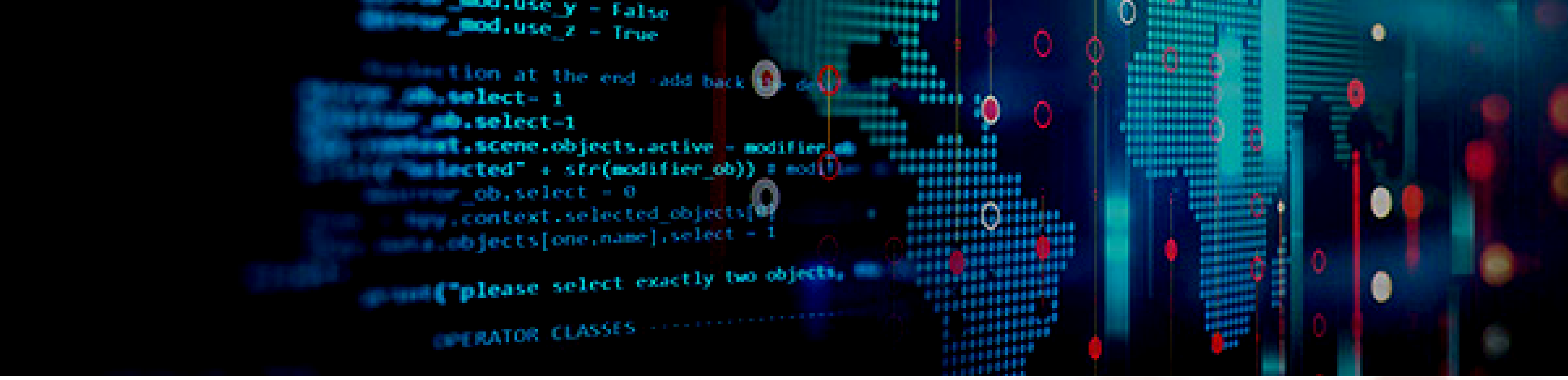
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
.scene.objects.active = modifier_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

Latest Hacked Websites

Published on Zone-h.org

http://munitalavera.gob.pe/-.html
http://munitalavera.gob.pe/-.html notified by Indonesia Attacker
https://pn-kotabaru.go.id/chi.php
https://pn-kotabaru.go.id/chi.php notified by Indonesia Attacker
https://www.hcm.gov.mz
https://www.hcm.gov.mz notified by TEAM_INSANE_PK
https://simbniger.cilss.int/1915.html
https://simbniger.cilss.int/1915.html notified by D4LGH4CK_TM
https://cc-beaujolaisvaldesaone.fr
https://cc-beaujolaisvaldesaone.fr notified by Cyb3r_Sw0rd
https://cc-agd.fr
https://cc-agd.fr notified by Cyb3r_Sw0rd
http://www.munitayacaja.gob.pe/a.htm
http://www.munitayacaja.gob.pe/a.htm notified by Mr. BDKR28
https://intra.cerrolargo.rs.gov.br/xx.html
https://intra.cerrolargo.rs.gov.br/xx.html notified by xstro0
https://jdih2.kkp.go.id/xx.html
https://jdih2.kkp.go.id/xx.html notified by xstro0
http://udsangsawang.go.th/xstro0.jpg
http://udsangsawang.go.th/xstro0.jpg notified by xstro0
https://www.immigration.gov.so/images/Trending/1674015065_xx.jpg
https://www.immigration.gov.so/images/Trending/1674015065_xx.jpg notified by xstro0
http://idokavre.p3.gov.np/xx.html
http://idokavre.p3.gov.np/xx.html notified by xstro0
https://gestion.puntodigital.gob.ar/glpi/xx.html
https://gestion.puntodigital.gob.ar/glpi/xx.html notified by xstro0
http://www.elandreporting.munshiganjlg.gov.bd/img/xx.html
http://www.elandreporting.munshiganjlg.gov.bd/img/xx.html notified by xstro0
http://aplicativo.onda.gob.do/ARCH/xx.html_1675403289.html
http://aplicativo.onda.gob.do/ARCH/xx.html_1675403289.html notified by xstro0
http://careers.owwa.gov.ph/events/allan10.jpg
http://careers.owwa.gov.ph/events/allan10.jpg notified by allan10k
http://etu.owwa.gov.ph/events/allan10.jpg
http://etu.owwa.gov.ph/events/allan10.jpg notified by allan10k

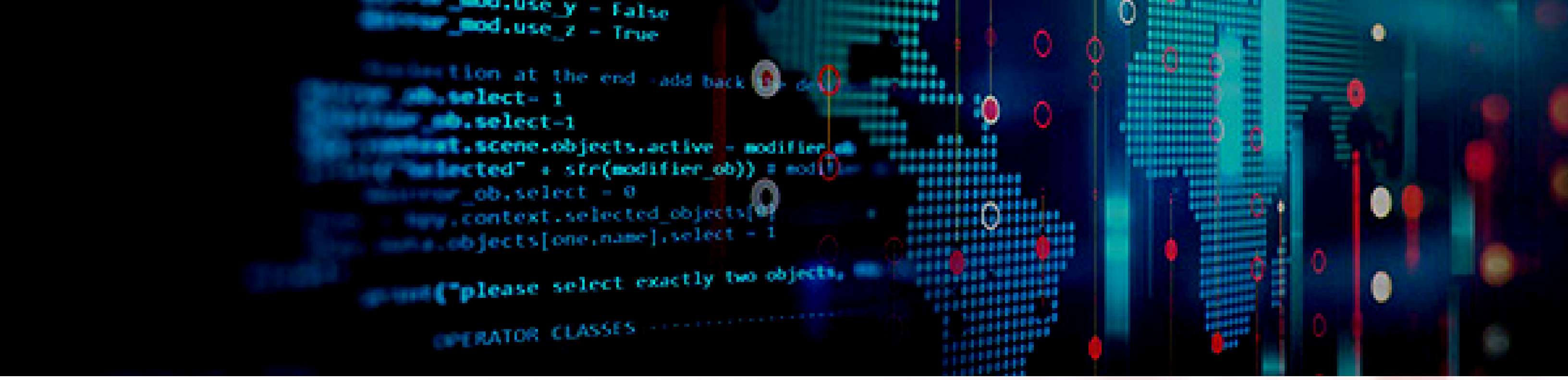

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Dark Web News

Darknet Live

[Tor is slow right now. Here is what is happening](#)
[UK Woman Attempted to Hire a Hitman on the Dark Web](#)
[The Hitchhiker's Guide to Monero](#)
[NJ Man Attempted to Hire a Hitman on the Dark Web](#)

Dark Web Link


_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

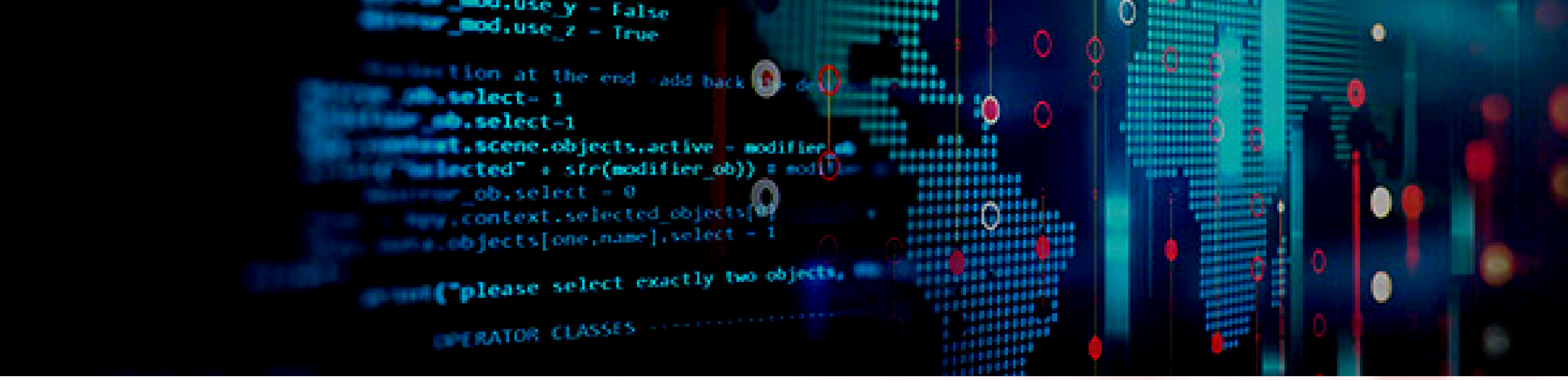
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-Up
* Nearly 19,000 ESXi Servers Still Vulnerable to CVE-2021-21974
* Evasion Techniques Uncovered: An Analysis of APT Methods
* Year In Review: Rapid7 InsightIDR
* Rapid7 Recognized on Bloomberg Gender Equality Index, Continues Commitments to Support DEI
* CVE-2022-21587: Rapid7 Observed Exploitation of Oracle E-Business Suite Vulnerability
* Multiple DMS XSS (CVE-2022-47412 through CVE-20222-47419)
* CVE-2023-22501: Critical Broken Authentication Flaw in Jira Service Management Products
* Ransomware Campaign Compromising VMware ESXi Servers
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* #StopRansomware - Ransomware Attacks on Critical Infrastructure Fund DPRK Espionage Activities
* CISA Releases Six Industrial Control Systems Advisories
* OpenSSL Releases Security Advisory
* CISA and FBI Release ESXiArgs Ransomware Recovery Guidance
* CISA Releases ESXiArgs Ransomware Recovery Script
* CISA Releases One Industrial Control Systems Advisory
* CISA Releases Six Industrial Control Systems Advisories
* AA23-040A: #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber A
* AA23-039A: ESXiArgs Ransomware Virtual Machine Recovery Guidance
* Vulnerability Summary for the Week of January 30, 2023
* Vulnerability Summary for the Week of January 23, 2023

Zero Day Initiative Advisories

ZDI-CAN-20346: 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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20356: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-19747: Rockwell Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20109: Rockwell Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-19749: Rockwell Automation
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Simon Janz

(@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20339: 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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20305: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20296: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20307: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20337: 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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20297: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20345: 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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20334: 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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20299: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20300: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20302: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20298: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20304: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20306: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20301: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20308: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-02-10, 3 days ago. The vendor is given until 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-20361: Adobe

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: 2023-02-09, 4 days ago. The vendor is given until 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-20311: Adobe

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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2023-02-09, 4 days ago. The vendor is given until 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-20365: Adobe

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: 2023-02-09, 4 days ago. The vendor is given until 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-5862-1

Ubuntu Security Notice 5862-1 - It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Pawan Kumar Gupta, Alyssa Milburn, Amit Peled, Shani Rehana, Nir Shildan and Ariel Sabba discovered that some Intel processors with Enhanced Indirect Branch Restricted Speculation did not properly handle RET instructions after a VM exits. A local attacker could potentially use this to expose sensitive information.

Ubuntu Security Notice USN-5861-1

Ubuntu Security Notice 5861-1 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. Tam&aacute;s Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5860-1

Ubuntu Security Notice 5860-1 - Kyle Zeng discovered that the sysctl implementation in the Linux kernel contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service or execute arbitrary code. Tam&aacute;s Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5863-1

Ubuntu Security Notice 5863-1 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. Tam&aacute;s Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5848-1

Ubuntu Security Notice 5848-1 - David Leadbeater discovered that less was not properly handling escape sequences when displaying raw control characters. A maliciously formed OSC 8 hyperlink could possibly be used by an attacker to cause a denial of service.

Ubuntu Security Notice USN-5858-1

Ubuntu Security Notice 5858-1 - Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the Netronome Ethernet driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5859-1

Ubuntu Security Notice 5859-1 - Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the Netronome Ethernet driver in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5857-1

Ubuntu Security Notice 5857-1 - Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5856-1

Ubuntu Security Notice 5856-1 - Davide Ornaghi discovered that the netfilter subsystem in the Linux kernel did not properly handle VLAN headers in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Hu Jiahui discovered that multiple race conditions existed in the Advanced Linux Sound Architecture framework, leading to use-after-free vulnerabilities. A local attacker could use these to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5855-1

Ubuntu Security Notice 5855-1 - It was discovered that ImageMagick incorrectly handled certain PNG images. If a user or automated system were tricked into opening a specially crafted PNG file, an attacker could use this issue to cause ImageMagick to stop responding, resulting in a denial of service, or possibly obtain the contents of arbitrary files by including them into images.

Red Hat Security Advisory 2023-0713-01

Red Hat Security Advisory 2023-0713-01 - Red Hat Data Grid is an in-memory, distributed, NoSQL datastore solution. Data Grid 8.4.1 replaces Data Grid 8.4.0 and includes bug fixes and enhancements. Issues addressed include denial of service and deserialization vulnerabilities.

Red Hat Security Advisory 2023-0573-01

Red Hat Security Advisory 2023-0573-01 - 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 4.9.55. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2023-0708-01

Red Hat Security Advisory 2023-0708-01 - Red Hat OpenShift Serverless Client kn 1.27.0 provides a CLI to interact with Red Hat OpenShift Serverless 1.27.0. The kn CLI is delivered as an RPM package for installation on RHEL platforms, and as binaries for non-Linux platforms.

Red Hat Security Advisory 2023-0709-01

Red Hat Security Advisory 2023-0709-01 - Version 1.27.0 of the OpenShift Serverless Operator is supported on Red Hat OpenShift Container Platform versions 4.8, 4.9, 4.10, 4.11 and 4.12. This release includes security and bug fixes, and enhancements.

Red Hat Security Advisory 2023-0634-01

Red Hat Security Advisory 2023-0634-01 - Logging Subsystem 5.6.1 - Red Hat OpenShift. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5853-1

Ubuntu Security Notice 5853-1 - It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service or possibly execute arbitrary code. It was discovered that a use-after-free vulnerability existed in the Bluetooth stack in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5854-1

Ubuntu Security Notice 5854-1 - It was discovered that an out-of-bounds write vulnerability existed in the Video for Linux 2 implementation in the Linux kernel. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Pawan Kumar Gupta, Alyssa Milburn, Amit Peled, Shani Rehana, Nir Shildan and Ariel Sabba discovered that some Intel processors with Enhanced Indirect Branch Restricted Speculation did not properly handle RET instructions after a VM exits. A local attacker could potentially use this to expose sensitive information.

Ubuntu Security Notice USN-5850-1

Ubuntu Security Notice 5850-1 - It was discovered that the Bluetooth HCI implementation in the Linux kernel did not properly deallocate memory in some situations. An attacker could possibly use this cause a denial of service. It was discovered that the Broadcom FullMAC USB WiFi driver in the Linux kernel did not properly perform bounds checking in some situations. A physically proximate attacker could use this to craft a malicious USB device that when inserted, could cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5851-1

Ubuntu Security Notice 5851-1 - It was discovered that a memory leak existed in the Unix domain socket implementation of the Linux kernel. A local attacker could use this to cause a denial of service. It was discovered that the Bluetooth HCI implementation in the Linux kernel did not properly deallocate memory in some situations. An attacker could possibly use this cause a denial of service.

Ubuntu Security Notice USN-5852-1

Ubuntu Security Notice 5852-1 - It was discovered that OpenStack Swift incorrectly handled certain XML files. A remote authenticated user could possibly use this issue to obtain arbitrary file contents containing sensitive information from the server.

Ubuntu Security Notice USN-5835-5

Ubuntu Security Notice 5835-5 - USN-5835-3 fixed vulnerabilities in Nova. This update provides the corresponding updates for Ubuntu 18.04 LTS. Guillaume Espanel, Pierre Libeau, Arnaud Morin, and Damien Rannou discovered that Nova incorrectly handled VMDK image processing. An authenticated attacker could possibly supply a specially crafted VMDK flat image and obtain arbitrary files from the server containing sensitive information.

Ubuntu Security Notice USN-5835-4

Ubuntu Security Notice 5835-4 - USN-5835-1 fixed vulnerabilities in Cinder. This update provides the corresponding updates for Ubuntu 18.04 LTS. In addition, a regression was fixed for Ubuntu 20.04 LTS. Guillaume Espanel, Pierre Libeau, Arnaud Morin, and Damien Rannou discovered that Cinder incorrectly handled VMDK image processing. An authenticated attacker could possibly supply a specially crafted VMDK flat image and obtain arbitrary files from the server containing sensitive information.

Red Hat Security Advisory 2023-0691-01

Red Hat Security Advisory 2023-0691-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2023-0685-01

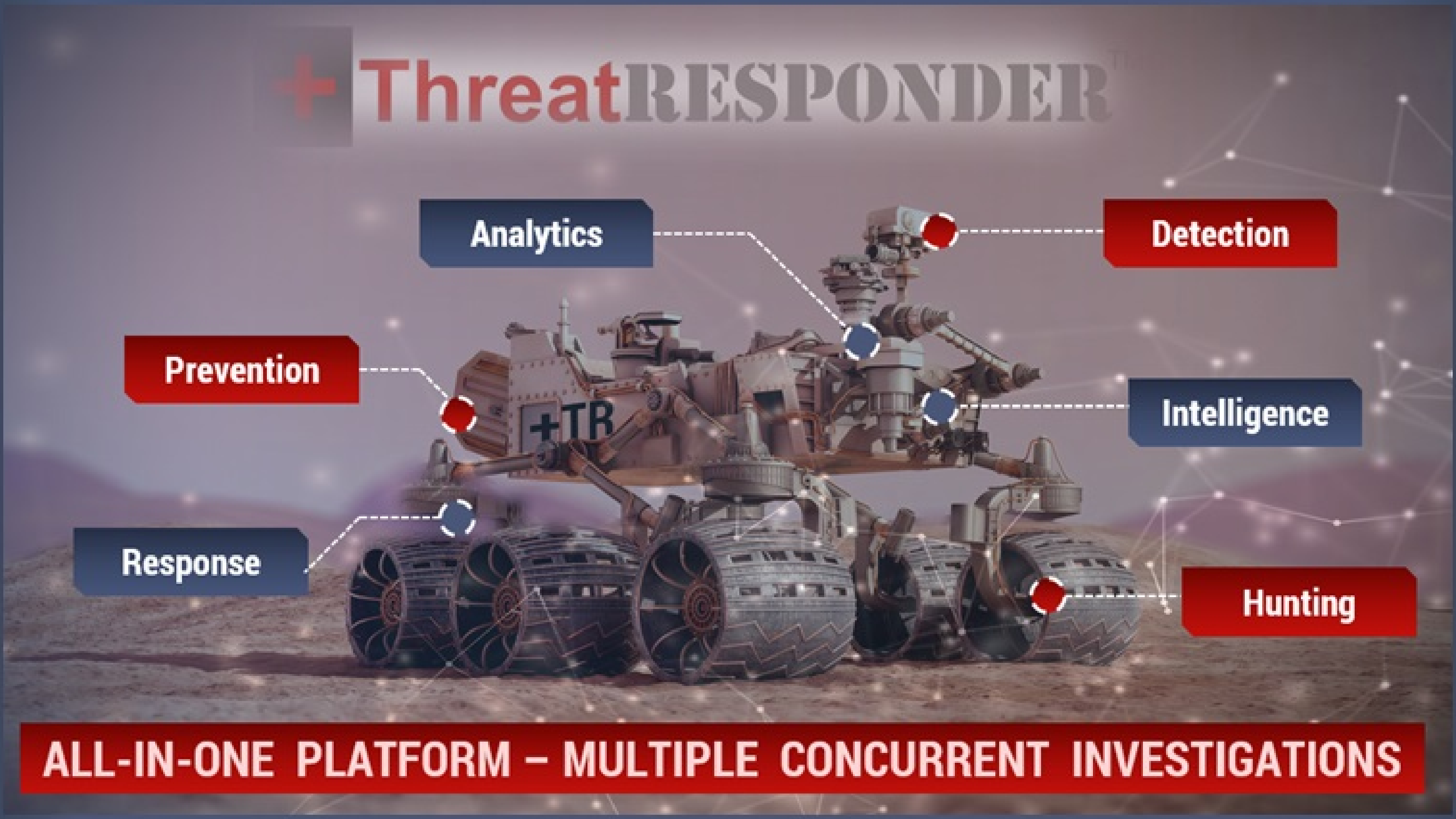
Red Hat Security Advisory 2023-0685-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include an out of bounds read vulnerability.

Are You...

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

Do DFIR Investigations Better

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



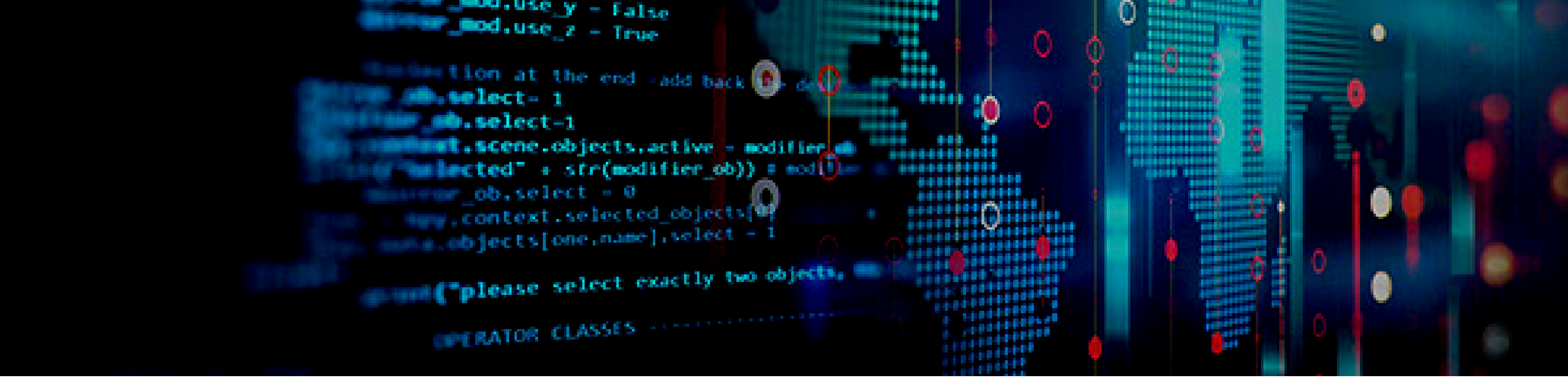
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com



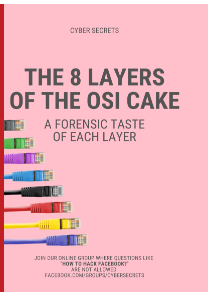
The Cyber Secrets publications on Amazon

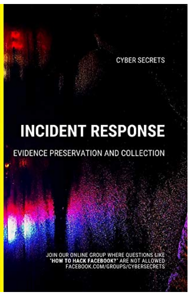
The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

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.

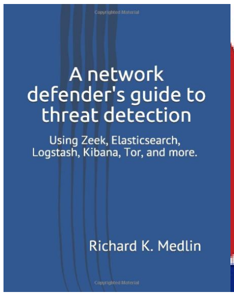
CYBER Secrets
Information Warfare Center
What's Inside?
SCADA/ICS:
Triton... The Russia-Linked Cyber ICS WMD
Advanced Persistent Threats:
The Cyber Kill Chain
Dark Web News
Tools & Tips:
Education Center
Confidentiality, Integrity, Availability
Technical Walkthroughs
Securing Data at Rest and Data in Transit
Anonymity on the Internet
Digital Forensics and Incident Response:
- Zeek (Bro) IDS - Installation & Configuration
Bug Hunting and Exploitation:
- VulnServer: TRUN Buffer Overflow
Visit our YouTube Channel
Threat Intelligence & Training
The Cyber Intelligence Report is an Information Warfare Center publication focusing on Real-World cyber threats and digital defenses. Included is analysis, basic whitepapers, and technical walkthroughs that will range from attack vectors to the incident response.

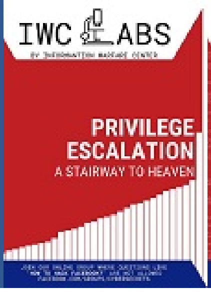
CYBER SECRETS
RED TEAMING
AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
SOCRANGE
LINUX
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"HOW TO HACK FACEBOOK?"
ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

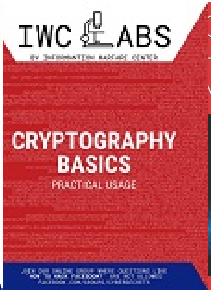


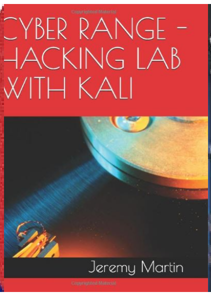

CYBER SECRETS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE
"HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

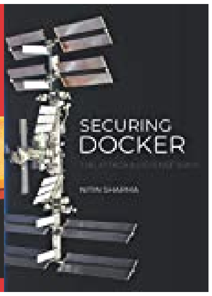
Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin









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