CYBER WAR

WEEKLY AWARENESS REPORT

01-27-20

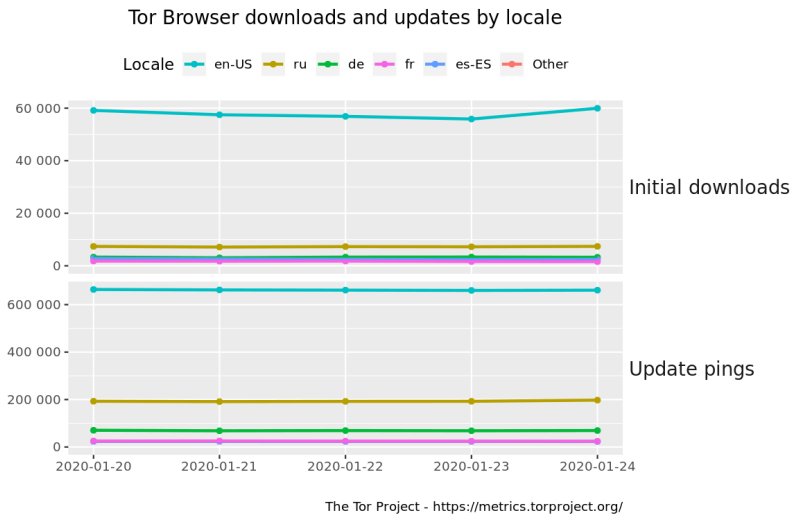
January 27, 2020

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

Symantec ThreatCon Low: Basic network posture

This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms should be used.



Interesting News

* [CSI Linux Forensics Challenge]

Using CSI Linux and the tools included, go through this forensic project and identify all the flags you can. Use Autopsy as your main application. Write a walk through on how you found each item within Autopsy and any other tools within your final report. The findings and final report will then be graded, with the best combo being the winner... [Read the Cyber Intelligence Report 2020 Q1]for more details.

* * We have an active Facebook group that discusses topics ranging from computer forensics to ethical hacking and more. Join the [Cyber Secrets Facebook group here]. If you would like to receive the CIR updates by email, [Subscribe!]

Index of Sections

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* Naked Security
* Quick Heal - Security Simplified
* Threat Post

The Hacker Corner:
* Security Conferences
* Zone-H Latest Published Website Defacements

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

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Advisories
* US-Cert (Current Activity-Alerts-Bulletins)
* Symantec's Latest List
* Packet Storm Security's Latest List

Credits

Packet Storm Security

* NYPD Arrests Ninth Methbot Gang Member
* China Locks Down 35M People Over Coronavirus Case
* The Chrome Web Store Is Currently Facing A Wave Of Fraudulent Transactions
* Clearview AI Sued Over Privacy Concerns
* Facebook's Sir Nick Clegg Criticized Over WhatsApp Security
* Mac Users Bombarded By Laughably Unsophisticated Malware
* Hackers Target Unpatched Citrix Servers To Deploy Ransomware
* Fake SWAT Calls Hit Tech Execs
* Amazon Engineer Leaks Encryption Keys To Public GitHub Repo
* Phishing Campaign Leads To UPS Store Data Breach
* Twitter Demands AI Company Stops Collecting Faces
* Suspected Iranian Hackers Target European Energy Companies
* Crown Prince Of Saudi Arabia Accused Of Hacking Jeff Bezos' Phone
* Brazil Prosecutes Greenwald In Attack On Press Freedom
* Data Leak Strikes US Cannabis Users, Sensitive Info Exposed
* Microsoft Discloses Security Breach Of Customer Support Database
* LastPass Stores Passwords So Securely Users Cannot Access Them
* Antivirus Vendors Push Fixes For EFS Ransomware Attack Method
* Ubisoft Sues Operators Of Four DDoS For Hire Services
* Microsoft Zero Day Actively Exploited, Patch Forthcoming
* Mitsubishi Electric Discloses Breach, China Suspected
* Regus Sales Staff Data Exposed After Undercover Job Review
* Hacker Leaks 500,000 Credentials For IoT Devices And More
* GDPR: 160,000 Data Breaches Reported Already, So Expect The Big Fines To Follow
* How Hackers Are Making Millions Legally

Krebs on Security

* Russian Cybercrime Boss Burkov Pleads Guilty
* Does Your Domain Have a Registry Lock?
* Apple Addresses iPhone 11 Location Privacy Concern
* DDoS Mitigation Firm Founder Admits to DDoS
* Patch Tuesday, January 2020 Edition
* Cryptic Rumblings Ahead of First 2020 Patch Tuesday
* Phishing for Apples, Bobbing for Links
* Alleged Member of Neo-Nazi Swatting Group Charged
* Lawmakers Prod FCC to Act on SIM Swapping
* Tricky Phish Angles for Persistence, Not Passwords

Dark Reading

* Greater Focus on Privacy Pays Off for Firms
* How to Get the Most Out of Your Security Metrics
* New Social Engineering Event to Train Business Pros on Human Hacking
* 'CardPlanet' Operator Pleads Guilty in Federal Court
* 7 Steps to IoT Security in 2020
* 5 Resume Basics for a Budding Cybersecurity Career
* Online Employment Scams on the Rise, Says FBI
* The Annoying MacOS Threat That Won't Go Away
* DHS Warns of Increasing Emotet Risk
* NSA Offers Guidance on Mitigating Cloud Flaws
* Deconstructing Web Cache Deception Attacks: They're Bad; Now What?
* Severe Vulnerabilities Discovered in GE Medical Devices
* Ryuk Ransomware Hit Multiple Oil & Gas Facilities, ICS Security Expert Says
* Weathering the Privacy Storm from GDPR to CCPA & PDPA
* To Avoid Disruption, Ransomware Victims Continue to Pay Up
* For Mismanaged SOCs, The Price Is Not Right
* Eight Flaws in MSP Software Highlight Potential Ransomware Vector
* Configuration Error Reveals 250 Million Microsoft Support Records
* Why DPOs and CISOs Must Work Closely Together
* 'We Only Have Two of the Blinky Boxes Left to Go'

The Hacker News

* Interpol Arrests 3 Indonesian Credit Card Hackers for Magecart Attacks
* Russian Pleads Guilty to Running 'CardPlanet' to Sell Stolen Credit Cards
* 250 Million Microsoft Customer Support Records Exposed Online
* Saudi Prince Allegedly Hacked World's Richest Man Jeff Bezos Using WhatsApp
* Download: The State of Security Breach Protection 2020 Survey Results
* BitDam Study Exposes High Miss Rates of Leading Email Security Systems
* Citrix Releases Patches for Critical ADC Vulnerability Under Active Attack
* Evaluating Your Security Controls? Be Sure to Ask the Right Questions
* Microsoft Warns of Unpatched IE Browser Zero-Day That's Under Active Attacks
* Broadening the Scope: A Comprehensive View of Pen Testing
* Use iPhone as Physical Security Key to Protect Your Google Accounts
* Update Windows 10 Immediately to Patch a Flaw Discovered by the NSA
* Adobe Releases First 2020 Patch Tuesday Software Updates
* Download Ultimate 'Security for Management' Presentation Template
* PoC Exploits Released for Citrix ADC and Gateway RCE Vulnerability

Security Week

* German Privacy Watchdog Investigates Clothing Retailer H&M
* Three Magecart Hackers Arrested in Indonesia
* Lessons Learned From 2016, but U.S. Faces New Election Threats
* World Economic Forum on Securing the Aviation Industry in the Age of Convergence
* NSA Shares Guidance on Mitigating Cloud Vulnerabilities
* Huawei and Supply Chain Security - The Great Geopolitical Debate
* Trend Micro OfficeScan Flaw Apparently Exploited in Mitsubishi Electric Hack
* PoC Exploits Created for Recently Patched 'BlueGate' Windows Server Flaws
* Trump, Johnson Talk Security Ahead of Huawei Decision
* Cisco Webex Vulnerability Exploited to Join Meetings Without a Password
* Questions Linger Over Investigation Into Jeff Bezos' Hacking
* Greece: Government Websites Hit by Cyberattack
* 2020 Rings in a New Era of Cyber Attacks - and it's Getting Personal
* Microsoft Releases Azure Security Benchmark
* Bipartisan Bill Aims to Reform NSA Surveillance of Americans
* Privacy Firm Finds Unsecured Cannabis Patient Information
* The More Authentication Methods, the Merrier
* UK 'to Decide on Huawei 5G Next Week'
* Citrix Releases More Patches for Exploited Flaw, Tool to Detect Compromise
* Researchers Earn $280,000 for Hacking Industrial Systems at Pwn2Own Miami

Infosecurity Magazine

* US Rolls Out New Bill to Reform NSA Surveillance
* Major Canadian Military Contractor Compromised in Ransomware Attack
* US Space Industry to Launch Cybersecurity Portal
* Royal Yachting Association Resets Passwords After Breach
* Chrome and Firefox Clamp Down on Suspicious Behavior
* Citrix Flaw Exploited by Ransomware Attackers
* Russian Pleads Guilty to Running Online Criminal Marketplace
* US Issues Cybersecurity Warnings Over Flawed Medical Devices
* London Police Adopt Facial Recognition Technology as Europe Considers Five-Year Ban
* #BSidesLeeds: Credential Stuffing Often Seen as "Volume" Cybercrime
* #BSidesLeeds: Cyber is Running the World, More Innovation to Come
* European Energy Firm Targeted by RAT Linked to Iran

Naked Security

* Cardplanet mastermind pleads guilty to credit card fraud
* Tinder to get panic button, catfish-fighting facial recognition
* Instagram CEO's homes were targetted by SWATters
* New York wants to ban taxpayer-funded ransomware payments
* Monday review - the hot 21 stories of the week
* Google finds privacy holes in Safari's ITP anti-tracking system
* Protestors petition equity firm over .org buyout
* 9th Methbot suspect arrested in massive clickfraud ring
* Privacy watchdog throws wider net to protect children online
* Looking for silver linings in the CVE-2020-0601 crypto vulnerability

Quick Heal - Security Simplified

* New wave of Mal-Spam campaign attaching Disk Imaging Files
* Ako Ransomware targeting businesses using RaaS
* First Node.js-based Ransomware : Nodera
* Windows 7 reaches End of Life (EOL) - Are you ready for the risks or would you rather upgrade your OS
* STOP (Djvu) Ransomware: Ransom For Your Shady Habits!
* Security resolutions for 2020 to stay safe online!
* Skills that can help kids deal with cybersecurity challenges NOW & LATER
* Top Cyber-security trends affecting Windows users during 2019
* Cybercrime not limited to Metro cities - Wake up call for Smaller cities of India!
* Pegasus like spyware could be snooping on you right now!!

Threat Post

* N.Y. Could Ban Cities from Paying Ransomware Attackers
* Mandatory IoT Security in the Offing with U.K. Proposal
* ThreatList: Ransomware Costs Double in Q4, Sodinokibi Dominates
* Cisco Webex Flaw Lets Unauthenticated Users Join Private Online Meetings
* New Bill Proposes NSA Surveillance Reforms
* Fake Smart Factory Honeypot Highlights New Attack Threats
* Critical, Unpatched 'MDhex' Bugs Threaten Hospital Devices
* U.S. Gov Agency Targeted With Malware-Laced Emails
* Shlayer, No. 1 Threat for Mac, Targets YouTube, Wikipedia
* Cisco Warns of Critical Network Security Tool Flaw

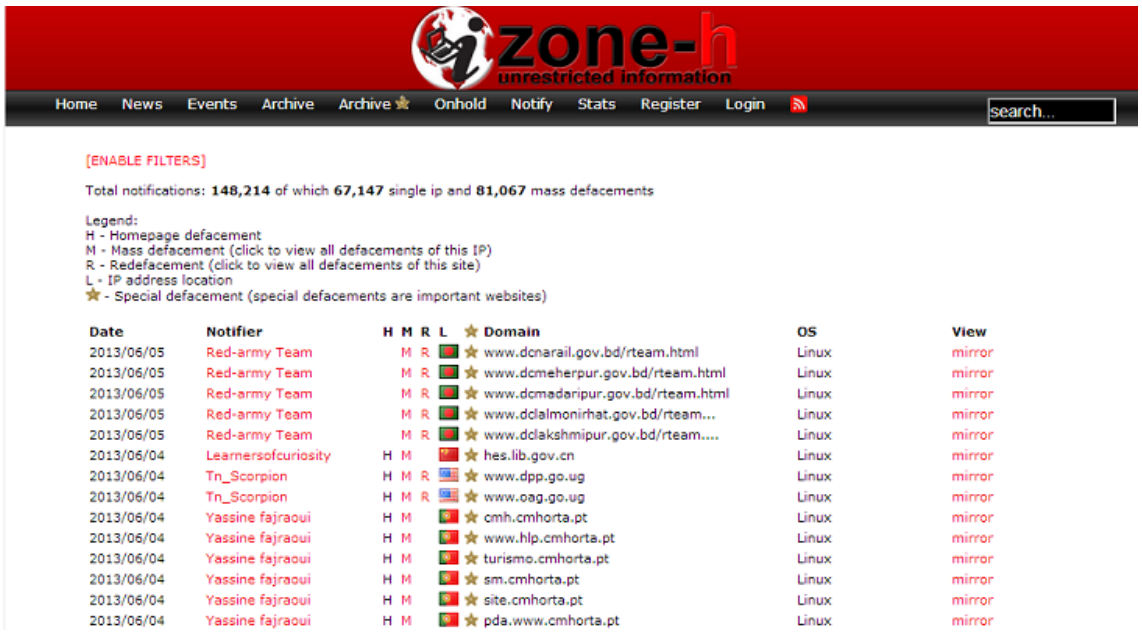
The Hacker Corner

Conferences

* EC Council Training Courses 2020
* Advertising Landing Page Copy/Form
* Apply: FREE 6 Month InfoSec Speaking Plan
* Apply: FREE 30 Day InfoSec Speaking Plan
* How To Speak At DEF CON
* Join Our LinkedIn Group
* Upcoming Cybersecurity Conferences in the United States & Canada
* Upcoming Cybersecurity Conferences in Europe
* 29 Amazing TED Cybersecurity Talks (2008 - 2020)
* 7 Proven Ideas for Your InfoSec Conference Delegate Acquisition Strategy

Latest Website Defacements

Unfortunately, at the time of this report, the resource was not availible.
You can access this resourse here: http://www.zone-h.org/rss/specialdefacements



Tools & Techniques

Packet Storm Security Tools Links

* TestSSL 3.0
* Lulzbuster 1.0.0
* Falco 0.19.0
* Logwatch 7.5.3
* Zed Attack Proxy 2.9.0 Cross Platform Package
* WebSploit Framework 4.0.1
* Maavi Fuzzing Utility
* Wireshark Analyzer 3.2.1
* Packet Fence 9.3.0
* SQLMAP - Automatic SQL Injection Tool 1.4

Kali Linux Tutorials

* HerShell : Multiplatform Reverse Shell Generator
* Check-LocalAdminHash : PowerShell Tool To Authenticate Multiple Hosts Over WMI Or SMB
* SharpStat : C# Utility That Uses WMI To Run CMD
* KsDumper : Dumping Processes Using The Power Of Kernel Space
* Yarasafe : SAFE Embeddings To Match Functions In Yara
* How to Protect Yourself Against Common Password Attacks
* AlertResponder : Automatic Security Alert Response Framework By AWS Serverless Application Model
* TAS : A Tiny Framework For Easily Manipulate The TTY & Create Fake Binaries
* Corsy : CORS Misconfiguration Scanner
* TeleGram-Scraper : Telegram Group Scraper Tool

GBHackers Analysis

* CWE Top 25 (2019) - List of Top 25 Most Dangerous Software Weakness that Developers Need to Focus
* Citrix Released Permanent Fixes for the Actively Exploited CVE-2019-19781 Flaw in ADC 11.1 and 12.0
* JhoneRAT - Hackers Launching New Cloud-based Python RAT to Steal Data From Google Drive, Twitter & G
* Proof-of-Concept Exploits Released for The Microsoft-NSA Crypto vulnerability - CVE-2020-0601
* Urgent !! Windows User Urged to Patch A Critical Crypto Vulnerability on Windows 10, Clients & Server

CSI Linux

A Linux Distro focusing on Online Investigations and Incident Response. Download here.
Help grow the distribution by giving feedback and suggestions.

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Realtek SDK Information Disclosure / Code Execution
* Ricoh Printer Driver Local Privilege Escalation
* OLK Web Store 2020 Cross Site Request Forgery
* Webtareas 2.0 SQL Injection
* TP-Link TP-SG105E 1.0.0 Unauthenticated Remote Reboot
* Genexis Platinum-4410 2.1 Authentication Bypass
* qdPM 9.1 Remote Code Execution
* Umbraco CMS 8.2.2 Cross Site Request Forgery
* Pachev FTP Server 1.0 Path Traversal
* BOOTP Turbo 2.0 Denial Of Service
* D-Link DIR-859 Unauthenticated Remote Command Execution
* Reliable Datagram Sockets (RDS) rds_atomic_free_op Privilege Escalation
* ZOHO ManageEngine ServiceDeskPlus 11.0 Build 11007 Cross Site Scripting
* Employee Leaves Management System 2.0 Cross Site Request Forgery
* Citrix XenMobile Server 10.8 XML Injection
* XNU vm_map_copy Insufficient Fix
* KeePass 2.44 Denial Of Service
* ECTouch ECShop 2.7.3 SQL Injection
* Park Ticketing Management System 1.0 Cross Site Scripting
* Microsoft Windows Theme API File Parsing
* ManageEngine Network Configuration Manager 12.2 SQL Injection
* Microsoft Windows Media Center .wmv Security Bypass / Code Execution
* Neowise CarbonFTP 1.4 Insecure Proprietary Password Encryption
* WordPress WP Fanzone 3.1 SQL Injection
* Centreon 19.04 Remote Code Execution

CXSecurity

* Sysax Multi Server 5.50 Denial of Service
* qdPM 9.1 Remote Code Execution
* BOOTP Turbo 2.0 Denial Of Service
* Reliable Datagram Sockets (RDS) rds_atomic_free_op Privilege Escalation
* Microsoft Windows 10 (19H1 1901 x64) ws2ifsl.sys Use After Free Local Privilege Escalation (kASLR kCF
* Tautulli 2.1.9 Denial of Service
* GTalk Password Finder 2.2.1 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

* [local] Torrent 3GP Converter 1.51 - Stack Overflow (SEH)
* [dos] Remote Desktop Gateway - 'BlueGate' Denial of Service (PoC)
* [local] Ricoh Printer Drivers - Local Privilege Escalation
* [webapps] Genexis Platinum-4410 2.1 - Authentication Bypass
* [webapps] OLK Web Store 2020 - Cross-Site Request Forgery
* [webapps] Webtareas 2.0 - 'id' SQL Injection
* [webapps] TP-Link TP-SG105E 1.0.0 - Unauthenticated Remote Reboot
* [local] Reliable Datagram Sockets (RDS) - rds_atomic_free_op NULL pointer dereference Privilege Escal
* [remote] Pachev FTP Server 1.0 - Path Traversal
* [dos] BOOTP Turbo 2.0 - Denial of Service (SEH)(PoC)
* [webapps] qdPM 9.1 - Remote Code Execution
* [dos] KeePass 2.44 - Denial of Service (PoC)
* [webapps] Citrix XenMobile Server 10.8 - XML External Entity Injection
* [local] NEOWISE CARBONFTP 1.4 - Weak Password Encryption
* [webapps] ManageEngine Network Configuration Manager 12.2 - 'apiKey' SQL Injection
* [webapps] Centreon 19.04 - Authenticated Remote Code Execution (Metasploit)
* [dos] Sysax Multi Server 5.50 - Denial of Service (PoC)
* [webapps] Adive Framework 2.0.8 - Persistent Cross-Site Scripting
* [local] Easy XML Editor 1.7.8 - XML External Entity Injection
* [local] Plantronics Hub 3.13.2 - SpokesUpdateService Privilege Escalation (Metasploit)
* [local] Trend Micro Maximum Security 2019 - Privilege Escalation
* [dos] GTalk Password Finder 2.2.1 - 'Key' Denial of Service (PoC)
* [webapps] Wordpress Time Capsule Plugin 1.21.16 - Authentication Bypass
* [local] Trend Micro Maximum Security 2019 - Arbitrary Code Execution
* [webapps] Wordpress Plugin InfiniteWP Client 1.9.4.5 - Authentication Bypass

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.

Cyber Security Video Channels

Black Hat

* evm: ALLSTAR: New Challenge Problems for Static Analysis
* Patrick Wardle: Making the Old, New: repurposing macOS malware
* Maddie Stone: Whatsup with WhatsApp: A Detailed Walk Through of Reverse Engineering CVE-2019-3568
* Mike Bell: Extending Ghidra: from Script to Plugins and Beyond

Defcon Conference

* Bridge Attack Double edged Sword in MobileSec - Zidong Han - DEF CON China 1
* Breaking the back end! - Gregory Pickett - DEF CON China 1
* Creating the DEFCON China 1.0 Badge - Joe Grand - DEF CON China 1
* Hacking Driverless Vehicles - Zoz - DEF CON China 1

Hack5

* Citrix Patches Major Vulnerability; Windows Patches NSA Reported Bug - ThreatWire
* SHA-1 Is Terrible, Cable Modems Haunted By Flaw, SIM Swapping Gets Worse - ThreatWire
* Cheap DIY WiFi Cameras & Cloud Free Home Automation
* O.MG DemonSeed EDU - Ep5 - Payloads & Bit Banging

The PC Security Channel [TPSC]

* Soviet Ransomware destroys Capitalist Windows
* Ransomware vs Ransomware Grand Finale
* NSA discloses major security flaw in Windows 10
* Kaspersky Security Cloud Review | Test vs Malware

Eli the Computer Guy

* Programming Intro - Wireframing Intro
* Programming Intro - How to Find a Coding Job
* Programming Intro - Best Programming Language
* Programming Intro - How to Self Study Coding

Security Now

* The Crypto CurveBall - Security Now 750
* Windows 7 - R. I. P. - Security Now 749

Troy Hunt

* Weekly Update 175

Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates
* NSA Releases Guidance on Mitigating Cloud Vulnerabilities
* Citrix Releases Security Updates for SD-WAN WANOP
* Cisco Releases Security Updates
* Increased Emotet Malware Activity
* IC3 Issues Alert on Employment Scams
* Reminder: Safeguard Websites from Cyberattacks
* Samba Releases Security Updates
* AA20-020A: Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANO
* AA20-014A: Critical Vulnerabilities in Microsoft Windows Operating Systems
* AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability
* Vulnerability Summary for the Week of January 13, 2020
* Vulnerability Summary for the Week of January 6, 2020
* Vulnerability Summary for the Week of December 30, 2019

Symantec - Latest Threats

ISB.Downloader!gen297: Risk Level: Very Low. Type: Trojan.
SONAR.SuspDrop!g26: Risk Level: Very Low. Type: Trojan, Virus, Worm.
SONAR.SuspDrop!g27: Risk Level: Very Low. Type: Trojan, Virus, Worm.
SONAR.SuspDrop!g28: Risk Level: Very Low. Type: Trojan, Virus, Worm.
SONAR.SuspLaunch!g110: Risk Level: Very Low. Type: Trojan, Virus, Worm.
SONAR.SuspReg!gen23: Risk Level: Very Low. Type: Trojan, Virus, Worm.
Heur.Malcode!gen3: Risk Level: Very Low. Type: Trojan.
ISB.Downloader!gen349: Risk Level: Very Low. Type: Trojan.
ISB.Downloader!gen344: Risk Level: Very Low. Type: Trojan.

Symantec - Latest Risk

PUA.SafelyOnline: Type: Potentially Unwanted App.
Adware.4SharedDesktop: Type: Adware.
Hacktool.Sharpdpapi: Hacktool.Foxplace: ActiveContent.DI.1: Type: Other.
Hacktool.Sharphound: Hacktool.Safetykatz : PUA.Avrising: Type: Potentially Unwanted App.
Hacktool.ProcHack : PUA.FileConvTab: Type: Potentially Unwanted App.
PUA.Redpher: Type: Potentially Unwanted App.
Remacc.Remadmin: Type: Other.
Adware.TMAagent: Type: Adware.
Hacktool.Filensfer:

Advisories

Symantec - Latest Advisories

Unfortunately, at the time of this report, Symantec advisories was not availible.

NCSC - Latest Advisories

Launch of the Academic Centres of Excellence in Cyber Security Education
New programme from the NCSC recognises cyber security excellence in higher education and opens with a call for applications.
Introducing new NCSC Mobile Device Guidance
Keeping your organisation's mobile devices secure just got a little bit easier.

Zero Day Initiative Advisories

ZDI-CAN-9743: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9742: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9740: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9736: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9735: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9732: CentOS Web Panel
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous'

was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9731: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9716: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9714: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9713: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9709: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9707: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9259: CentOS Web Panel

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-10120: Fuji 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 'kimiya' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-10119: Fuji 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 'kimiya' was reported to the affected vendor on: 2020-01-23, 4 days ago. The vendor is given until 2020-05-22 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-9884: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Z0mb1E' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-9883: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Z0mb1E' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-9882: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Z0mb1E' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-9484: Adobe

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 'Steven Seeley (mr_me) of Source Incite' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-10124: 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: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-10082: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'chung96vn - Security Researcher of VinCSS (Member of Vingroup)' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-10074: Docker

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 '0-duke' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-10073: Trend Micro

A CVSS score 8.6 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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-10037: Microsoft

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jakub Palaczynski' was reported to the affected vendor on: 2020-01-21, 6 days ago. The vendor is given until 2020-05-20 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

WebKitGTK+ / WPE WebKit Code Execution

WebKitGTK+ and WPE WebKit suffer from multiple memory handling vulnerabilities that can result in arbitrary code execution. Versions affected include WebKitGTK before 2.26.3 and WPE WebKit before 2.26.3.

Red Hat Security Advisory 2020-0222-01

Red Hat Security Advisory 2020-0222-01 - The Ghostscript suite contains utilities for rendering PostScript and PDF documents. Ghostscript translates PostScript code to common bitmap formats so that the code can be displayed or printed.

Ubuntu Security Notice USN-4230-2

Ubuntu Security Notice 4230-2 - USN-4230-1 fixed a vulnerability in ClamAV. This update provides the corresponding update for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. It was discovered that ClamAV incorrectly handled certain MIME messages. A remote attacker could possibly use this issue to cause ClamAV to crash, resulting in a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4233-2

Ubuntu Security Notice 4233-2 - USN-4233-1 disabled SHA1 being used for digital signature operations in GnuTLS. In certain network environments, certificates using SHA1 may still be in use. This update adds the %VERIFY_ALLOW_BROKEN and %VERIFY_ALLOW_SIGN_WITH_SHA1 priority strings that can be used to temporarily re-enable SHA1 until certificates can be replaced with a stronger algorithm. Various other issues were also addressed.

Red Hat Security Advisory 2020-0215-01

Red Hat Security Advisory 2020-0215-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Red Hat Security Advisory 2020-0218-01

Red Hat Security Advisory 2020-0218-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Red Hat Security Advisory 2020-0216-01

Red Hat Security Advisory 2020-0216-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Red Hat Security Advisory 2020-0217-01

Red Hat Security Advisory 2020-0217-01 - Ansible is a simple model-driven configuration management, multi-node deployment, and remote-task execution system. Ansible works over SSH and does not require any software or daemons to be installed on remote nodes. Extension modules can be written in any language and are transferred to managed machines automatically.

Ubuntu Security Notice USN-4247-3

Ubuntu Security Notice 4247-3 - USN-4247-1 fixed several vulnerabilities in python-apt. This update provides the corresponding updates for Ubuntu 12.04 ESM and Ubuntu 14.04 ESM. It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. Various other issues were also addressed.

Red Hat Security Advisory 2020-0214-01

Red Hat Security Advisory 2020-0214-01 - Chromium is an open-source web browser, powered by WebKit. This update upgrades Chromium to version 79.0.3945.130. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-4249-1

Ubuntu Security Notice 4249-1 - It was discovered that e2fsprogs incorrectly handled certain ext4 partitions. An attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-4247-2

Ubuntu Security Notice 4247-2 - USN-4247-1 fixed vulnerabilities in python-apt. The updated packages caused a regression when attempting to upgrade to a new Ubuntu release. This update fixes the problem. It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. It was discovered that python-apt could install packages from untrusted repositories, contrary to expectations. Various other issues were also addressed.

Red Hat Security Advisory 2020-0204-01

Red Hat Security Advisory 2020-0204-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include denial of service, heap overflow, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-4246-1

Ubuntu Security Notice 4246-1 - It was discovered that zlib incorrectly handled pointer arithmetic. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that zlib incorrectly handled vectors involving left shifts of negative integers. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4248-1

Ubuntu Security Notice 4248-1 - It was discovered that GraphicsMagick incorrectly handled certain image files. An attacker could possibly use this issue to cause a denial of service or other unspecified impact.

Ubuntu Security Notice USN-4247-1

Ubuntu Security Notice 4247-1 - It was discovered that python-apt would still use MD5 hashes to validate certain downloaded packages. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages. It was discovered that python-apt could install packages from untrusted repositories, contrary to expectations.

Red Hat Security Advisory 2020-0203-01

Red Hat Security Advisory 2020-0203-01 - The libarchive programming library can create and read several different streaming archive formats, including GNU tar, cpio, and ISO 9660 CD-ROM images. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several popular desktop file managers. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2020-0202-01

Red Hat Security Advisory 2020-0202-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2020-0201-01

Red Hat Security Advisory 2020-0201-01 - Python-reportlab is a library used for generation of PDF documents. A code injection vulnerability has been addressed.

Red Hat Security Advisory 2020-0199-01

Red Hat Security Advisory 2020-0199-01 - OpenSLP is an open source implementation of the Service Location Protocol which is an Internet Engineering Task Force standards track protocol and provides a framework to allow networking applications to discover the existence, location, and configuration of networked services in enterprise networks. Issues addressed include buffer overflow and code execution vulnerabilities.

Debian Security Advisory 4608-1

Debian Linux Security Advisory 4608-1 - Multiple integer overflows have been discovered in the libtiff library and the included tools.

Red Hat Security Advisory 2020-0172-01

Red Hat Security Advisory 2020-0172-01 - Open vSwitch provides standard network bridging functions and

support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2020-0171-01

Red Hat Security Advisory 2020-0171-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2020-0196-01

Red Hat Security Advisory 2020-0196-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include a deserialization vulnerability.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com