CYBER WAR

WEEKLY AWARENESS REPORT

03-23-20

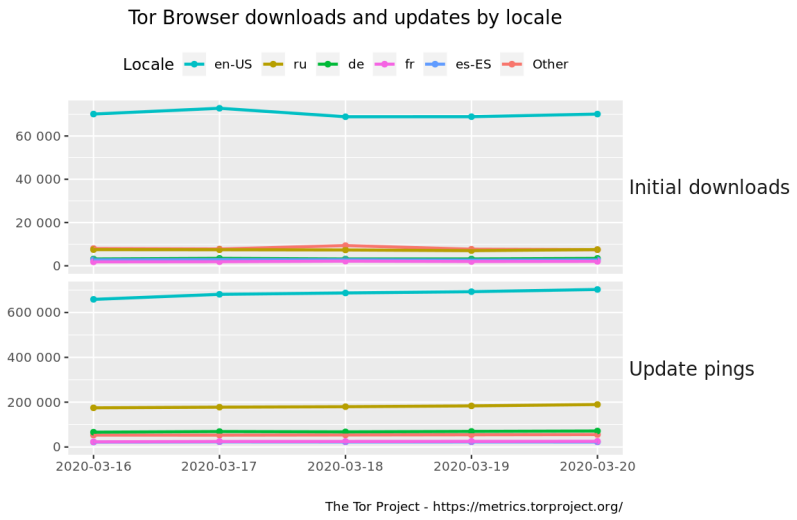
March 23, 2020

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

* CTF: Avengers Arsenal Challenge

The Challenge… Using whatever tool of your choice. Capture all the flags you can, identify and exploit as many vulnerabilities as you can, write a report, and write a walk through on how you found each item within. The findings and final report will then be graded, with the best combo being the winner. Make sure that the report and the walkthrough are two separate documents... Sign up for the CTF Now!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

* Hacker Selling Data Of 538 Million Weibo Users
* UK Coronavirus App Must Respect Privacy Rights
* Pwn2Own Contest Yields 13 Bugs, As Virtual Format Expands Talent Pool
* Inside An Instagram Celebrity Hacking Campaign
* If You Haven't Read It, The Imperial College Report On COVID-19 Is Important
* Google Launches Coronavirus Website In The United States
* Covid-19 Spurs Facial Recognition Tracking, Privacy Fears
* Coronavirus News Being Used To Sneak Malware Past AV Programs
* California Issues Statewide Stay At Home Order To Combat COVID-19
* Windows, Ubuntu, macOS, VirtualBox Fall At Pwn2Own Hacking Contest
* TrickBot Banking Trojan Introduces RDP Brute Forcing Module
* New Mirai Botnet Variant Targets NAS Devices
* Cisco Tackles SD-WAN Root Privilege Vulnerability
* Coronavirus Conspiracies Go Viral On WhatsApp As Crisis Deepens
* WordPress, Apache Struts Attract The Most Bug Exploits
* Android Surveillanceware Operators Jump On The Coronavirus Fear Bandwagon
* With Everyone WFH, VPN Security Has Become Paramount
* VMware Patches Privilege Escalation Vulnerability In Fusion, Horizon
* Coronavirus: Facebook Blames Bug For Incorrectly Marked Spam
* Coronavirus Lockdowns: 24 Hours Of Confusion Around The World
* How Officials Aim To Keep Voters Safe With Coronavirus
* Airlines Are Responding To COVID-19 Travel Bans
* COVID-19: WHO Warns Social Distancing Is Not Enough
* Social Media Giants Warn Of AI Moderation Errors As Coronavirus Empties Offices
* COVID-19: Bay Area Requires All 7 Million Residents To Shelter In Place

Krebs on Security

* Security Breach Disrupts Fintech Firm Finastra
* Zyxel Flaw Powers New Mirai IoT Botnet Strain
* Coronavirus Widens the Money Mule Pool
* The Web's Bot Containment Unit Needs Your Help
* Live Coronavirus Map Used to Spread Malware
* Crafty Web Skimming Domain Spoofs "https"
* Microsoft Patch Tuesday, March 2020 Edition
* FBI Arrests Alleged Owner of Deer.io, a Top Broker of Stolen Accounts
* U.S. Govt. Makes it Harder to Get .Gov Domains
* The Case for Limiting Your Browser Extensions

Dark Reading

* FBI Warns of Fake CDC Emails in COVID-19 Phishing Alert
* 8 Infosec Page-Turners for Days Spent Indoors
* From Zero to Hero: CISO Edition
* 200M Records of US Citizens Leaked in Unprotected Database
* Dark Reading Cybersecurity Crossword Puzzle
* Proof of Concept Released for kr00k Wi-Fi Vulnerability
* Security Ratings Are a Dangerous Fantasy
* Attack Surface, Vulnerabilities Increase as Orgs Respond to COVID-19 Crisis
* Misconfigured Elasticsearch Instance Exposes More Than 5 Billion Records
* DDoS Attack Targets German Food Delivery Service
* VPN Usage Surges as More Nations Shut Down Offices
* New Study Calls Common Risk Figure into Question
* TA505 Targets HR Departments with Poisoned CVs
* Cyber Resilience Benchmarks 2020
* Achieving DevSecOps Requires Cutting Through the Jargon
* Quantifying Cyber Risk: Why You Must & Where to Start
* Skimmer May Have Put NutriBullet Customers' Card Data at Risk for Nearly a Month
* TrickBot Module Takes Aim at Remote Desktops
* Process Injection Tops Attacker Techniques for 2019
* 500,000 Documents Exposed in Open S3 Bucket Incident

The Hacker News

* User Survey 2020 Report Shows Rapid Growth In Apache Pulsar Adoption
* Multiple DDoS Botnets Exploited 0-Day Flaws in LILIN DVR Surveillance Systems
* Mukashi: A New Mirai IoT Botnet Variant Targeting Zyxel NAS Devices
* How CISOs Should Prepare for Coronavirus Related Cybersecurity Threats
* Hackers Created Thousands of Coronavirus (COVID-19) Related Sites As Bait
* Adobe Releases Critical Patches for Acrobat Reader, Photoshop, Bridge, ColdFusion
* TrickBot Now Exploits Infected PCs to Launch RDP Brute Force Attacks
* TrueFire Guitar Tutoring Website Suffers Magecart-style Credit Card Breach
* Researchers Uncover a Nigerian Hacker's Pursuit of his Million Dollar Dream
* Europol Arrests 26 SIM Swapping Fraudsters For Stealing Over $3 Million
* Android Cookie-Stealing Malware Found Hijacking Facebook Accounts
* Critical Patch Released for 'Wormable' SMBv3 Vulnerability - Install It ASAP!
* Beware of 'Coronavirus Maps' - It's a malware infecting PCs to steal passwords
* Use This Ultimate Template to Plan and Monitor Your Cybersecurity Budgets
* Warning - Unpatched Critical 'Wormable' Windows SMBv3 Flaw Disclosed

Security Week

* Vulnerability Exposed Tesla Central Touchscreen to DoS Attacks
* Flaw in Password Managers Allowed Apps to Steal Credentials
* University of Utah Health Discloses Data Breach
* New Mexico Agencies on Edge Amid Rising Ransomware Attacks
* Zero-Day Vulnerabilities in LILIN DVRs Exploited by Several Botnets
* Mozilla to Remove Support for FTP in Firefox
* Unprotected Database Exposed 5 Billion Previously Leaked Records
* Hackers Target UK Fintech Company Finastra
* New Mirai Variant Delivered to Zyxel NAS Devices Via Recently Patched Flaw
* UK Printing Company Exposed Military Documents
* Russian Cyberspies Hacked High-Profile Email Accounts for Phishing
* Russia-Linked Cybercriminals Use Legitimate Tools in Attacks on German Firms
* Oracle VirtualBox, Adobe Reader, Windows Hacked at Pwn2Own 2020
* Android Surveillance Campaign Leverages COVID-19 Crisis
* Drupal Updates CKEditor to Patch XSS Vulnerabilities
* NIST Updates Flagship SP 800-53 Security and Privacy Controls
* Google Patches High-Risk Chrome Flaws, Halts Upcoming Releases
* RDP-Capable TrickBot Targets Telecoms Sectors in U.S. and Hong Kong
* NIST, DHS Publish Guidance on Securing Virtual Meetings, VPNs
* California Man Gets Prison for Hacking Atlanta-Based Company

Infosecurity Magazine

* Allegedly Cash-Strapped OneWeb Launches 34 New Satellites
* Virginia Forms Coronavirus Fraud Taskforce
* CEO Claims More Fake LinkedIn Users Are Claiming to be Employees
* National Gallery Fought Nearly Two Million Email Cyber-Attacks in 2019
* Sextortion Scam Threatens to Infect Victims with #COVID19
* Military Secrets Exposed by UK Printing Company
* Leaked Plans Reveal Mirai-Like Russian IoT Botnet
* Former Waymo Executive Passed Trade Secrets to Uber
* Norwegian Cruise Line Suffers Data Breach
* UAE Drops Cybercrime Charges Against American Who Insulted Vengeful Ex by Email
* Russian APT28 Group Changes Tack to Probe Email Servers
* Over Five Billion Breached Records Leaked

Naked Security

* WhatsApp "Martinelli" hoax is back, warning about "Dance of the Pope"
* Cisco issues urgent fixes for SD-WAN router flaws
* Tour guide/Chinese spy gets four years for SD card dead drops
* Stolen data of company that refused REvil ransom payment now on sale
* Firefox is dropping FTP support
* Monday review - the hot 23 stories of the week
* S2 Ep31: Remote working, malwareless ransomware and EARN IT - Naked Security Podcast
* Trolls ZoomBomb work-from-home videocall with filth
* Exchange rate service's customer details hacked via AWS
* COVID-19 disruption delays release of Chrome version 81

Quick Heal - Security Simplified

* Fake Coronavirus tracking app exploiting our fear and vulnerable social situation
* Are you secured when dealing with money on your mobile phones?
* CVE-2020-0796 - A "wormable" Remote Code Execution vulnerability in SMB v3
* Can playing video games on the PC cause cyberattacks?
* Mailto Ransomware under the skin of explorer.exe
* Take your browser security to the next level!
* Ouroboros: Following A New Trend In Ransomware League
* A Deep Dive Into Wakeup On Lan (WoL) Implementation of Ryuk
* Hackers are riding on the global panic pertaining to the deadly Coronavirus
* Unable to Shut down or Restart Windows 7 systems?

Threat Post

* Fake Coronavirus 'Vaccine' Website Busted in DoJ Takedown
* Revamped HawkEye Keylogger Swoops in on Coronavirus Fears
* Defying Covid-19's Pall: Pwn2Own Goes Virtual
* News Wrap, Coronavirus Edition: WFH Security Woes, Pwn2Own
* Covid-19 Spurs Facial Recognition Tracking, Privacy Fears
* New Mirai Variant 'Mukashi' Targets Zyxel NAS Devices
* Coronavirus Poll Results: Cyberattacks Ramp Up, WFH Prep Uneven
* Cisco Warns of High-Severity SD-WAN Flaws
* Cloud Misconfig Mistakes Show Need For DevSecOps
* WordPress, Apache Struts Attract the Most Bug Exploits

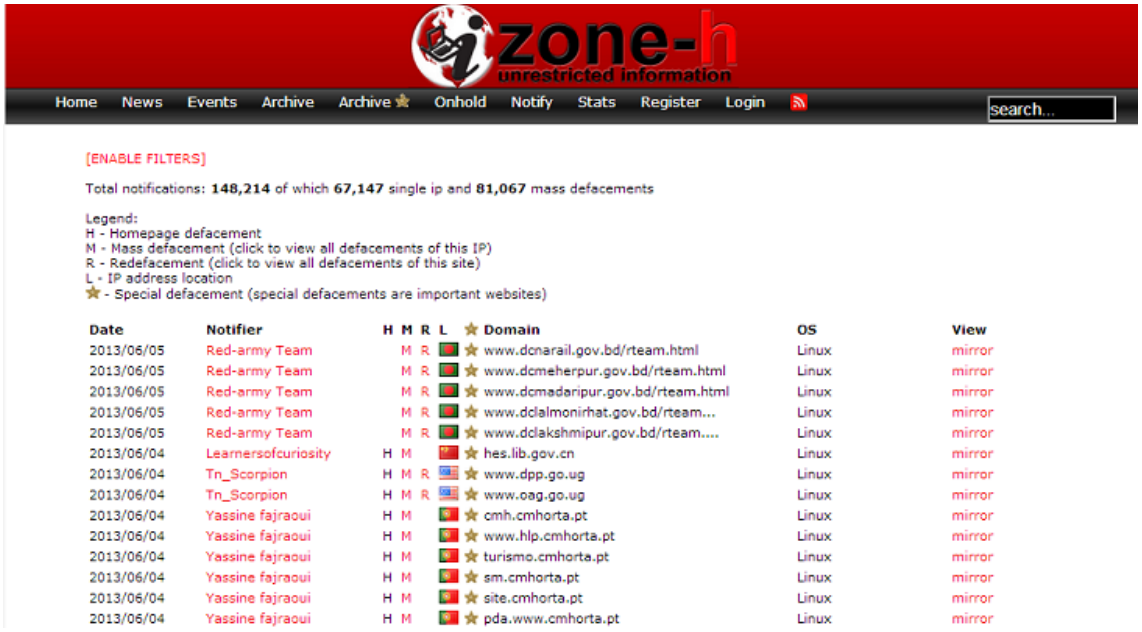
The Hacker Corner

Conferences

* Cancelled Cyber Security Conferences
* 5 Tips To Help You Become A Better Public Speaker
* How To Get Public Cybersecurity Speaking Engagements
* Free Cybersecurity 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
* Apply Now For Your Free 6 Month Speaking Plan
* How To Speak At DEF CON

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

* Mandos Encrypted File System Unattended Reboot Utility 1.8.10
* Hyperion Runtime Encrypter 2.3
* GNU Privacy Guard 2.2.20
* TOR Virtual Network Tunneling Tool 0.4.2.7
* Falco 0.21.0
* OpenSSL Toolkit 1.1.1e
* Lulzbuster 1.3.2
* AIEngine 1.9.2
* Zeek 3.1.1
* Richsploit RichFaces Exploitation Toolkit

Kali Linux Tutorials

* InstaSave : Python Script To Download Images, Videos & Profile Pictures From Instagram
* XSHOCK : Tool To Exploits ShellShock
* Chepy : A Python lib/cli Equivalent Of The Awesome CyberChef Tool
* SShuttle: Where Transparent Proxy Meets VPN Meets SSH
* Lazydocker : The Lazier Way To Manage Everything Docker
* Pypykatz : Mimikatz Implementation In Pure Python
* Token Reverser : Word List Generator To Crack Security Tokens
* ShuffleDNS : Wrapper Around Massdns Written In Go To Enumerate Valid Subdomains Using Active Brutefor
* AWSGen.py : AWS S3 Bucket Name Generator (beta v.)
* Jeopardize : A Low Cost Threat Intelligence&Response Tool

GBHackers Analysis

* 5 Bugs in Cisco SD-WAN Allows Attackers to Inject Arbitrary Commands With Root Privileges
* Why do the Certified Ethical Hacking Course
* Critical RCE Vulnerability in Cisco Protection let Hackers Execute an Arbitrary code Remotely
* Critical Vulnerability in ppp Daemon Let Hackers Remotely Exploit the Linux Systems & Gain Root Acces
* Zero-Day Bug in Verisign & IaaS Services Such as Google, Amazon let Hackers to Register Malicious Dom

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

* Horde 5.2.22 CSV Import Code Execution
* FIBARO System Home Center 5.021 Remote File Inclusion / XSS
* Joomla HDWPlayer 4.2 SQL Injection
* rConfig 3.9.4 Remote Command Injection
* EnovaNet Chateau-Thierry FormaLog WebService02 eChampagne 7.0 Cross Site Scripting / SQL Injection
* CyberArk PSMP 10.9.1 Policy Restriction Bypass
* Google Chrome 80.0.3987.87 Denial Of Service
* ProficySCADA For iOS 5.0.25920 Denial Of Service
* VMware Fusion 11.5.2 Privilege Escalation
* Exagate Sysguard 6001 Cross Site Request Forgery
* Easy File Sharing Web Server 7.2 Local Buffer Overflow
* Broadcom Wi-Fi KR00K Proof Of Concept
* Centreon Poller Authenticated Remote Command Execution
* ZoneAlarm TrueVector Internet Monitor Insecure NTFS Permissions
* Razer Synapse Service 1.0.0 DLL Injection
* Microsoft VSCode Python Extension Code Execution
* VMware Fusion Local Privilege Escalation / Directory Traversal
* Ivanti Workspace Manager Security Bypass
* Microtik SSH Daemon 6.44.3 Denial Of Service
* Netlink GPON Router 1.0.11 Remote Code Execution
* pppd 2.4.8 Buffer Overflow
* NetBackup 7.0 Unquoted Service Path
* UADMIN Botnet SQL Injection
* Rconfig 3.x Chained Remote Code Execution
* ShaderCache Arbitrary File Creation / Privilege Escalation

CXSecurity

* rConfig 3.9.4 search.crud.php Remote Command Injection
* Centreon Poller Authenticated Remote Command Execution
* Broadcom Wi-Fi Devices KR00K Information Disclosure
* pppd 2.4.8 Buffer Overflow
* PHPKB Multi-Language 9 Authenticated Remote Code Execution
* PHPKB Multi-Language 9 Authenticated Directory Traversal
* Zyxel CNM SecuManager 3.1.0 / 3.1.1 Hardcoded Keys / XSS / Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

* [webapps] Joomla! com_hdwplayer 4.2 - 'search.php' SQL Injection
* [webapps] rConfig 3.9.4 - 'search.crud.php' Remote Command Injection
* [webapps] FIBARO System Home Center 5.021 - Remote File Include
* [remote] CyberArk PSMP 10.9.1 - Policy Restriction Bypass
* [dos] Google Chrome 80.0.3987.87 - Heap-Corruption Remote Denial of Service (PoC)
* [dos] ProficySCADA for iOS 5.0.25920 - 'Password' Denial of Service (PoC)
* [local] VMware Fusion 11.5.2 - Privilege Escalation
* [webapps] Exagate Sysguard 6001 - Cross-Site Request Forgery (Add Admin)
* [remote] Broadcom Wi-Fi Devices - 'KR00K Information Disclosure
* [local] VMWare Fusion - Local Privilege Escalation
* [local] Microsoft VSCode Python Extension - Code Execution
* [remote] Microtik SSH Daemon 6.44.3 - Denial of Service (PoC)
* [local] NetBackup 7.0 - 'NetBackup INET Daemon' Unquoted Service Path
* [webapps] Netlink GPON Router 1.0.11 - Remote Code Execution
* [remote] ManageEngine Desktop Central - Java Deserialization (Metasploit)
* [remote] Rconfig 3.x - Chained Remote Code Execution (Metasploit)
* [webapps] PHPKB Multi-Language 9 - 'image-upload.php' Authenticated Remote Code Execution
* [webapps] PHPKB Multi-Language 9 - Authenticated Directory Traversal
* [webapps] PHPKB Multi-Language 9 - Authenticated Remote Code Execution
* [webapps] MiladWorkShop VIP System 1.0 - 'lang' SQL Injection
* [webapps] Enhanced Multimedia Router 3.0.4.27 - Cross-Site Request Forgery (Add Admin)
* [dos] Microsoft Windows 10 (1903/1909) - 'SMBGhost' SMB3.1.1 'SMB2_COMPRESSION_CAPABILITIES' Buffer O
* [webapps] Horde Groupware Webmail Edition 5.2.22 - Remote Code Execution
* [remote] Drobo 5N2 4.1.1 - Remote Command Injection
* [webapps] Centos WebPanel 7 - 'term' SQL Injection

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

* DATATRIBE TOUR WITH DAVE
* 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

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

* DTMF Tones In DIY Projects
* Coronavirus Themed Phishing, Malware, and Ransomware on the Rise - ThreatWire
* Cloud-Free Cameras with a side of Pineapple - Hak5 2612
* Clearview AI Privacy Fails - ThreatWire

The PC Security Channel [TPSC]

* Pwnd Ransomware | PwndLocker
* Raccoon Infostealer Malware
* Sophos vs Malware
* Coronavirus and Phishing

Eli the Computer Guy

* CSS and HTML 5 - Tag Based Class Attributes
* CSS and HTML 5 - nth-of-type Formatting
* CSS and HTML 5 - Table Formatting
* CSS and HTML 5 - DIV Tags and Borders

Security Now

* The SMBGhost Fiasco - Security Now 758
* The Fuzzy Bench - Security Now 757

Troy Hunt

* Cyber-Broken With Scott Helme

Advisories

US-Cert Alerts & bulletins

* Drupal Releases Security Updates
* Cisco Releases Security Updates for SD-WAN Solution Software
* Google Releases Security Updates for Chrome
* Adobe Releases Security Updates for Multiple Products
* VMware Releases Security Updates for Multiple Products
* Microsoft Releases Out-of-Band Security Updates for SMB RCE Vulnerability
* Microsoft Server Message Block RCE Vulnerability
* Unpatched Microsoft Exchange Servers Vulnerable to CVE-2020-0688
* AA20-073A: Enterprise VPN Security
* AA20-049A: Ransomware Impacting Pipeline Operations
* AA20-031A: Detecting Citrix CVE-2019-19781
* Vulnerability Summary for the Week of March 9, 2020
* Vulnerability Summary for the Week of March 2, 2020
* Vulnerability Summary for the Week of February 24, 2020

Symantec - Latest Threats

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

Symantec - Latest Risk

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

Advisories

Symantec - Latest Advisories

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

NCSC - Latest Advisories

Home working: preparing your organisation and staff
How to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (COVID-19) scam emails.
Weekly Threat Report 13th March 2020
The NCSC's weekly threat report is drawn from recent open source reporting.

Zero Day Initiative Advisories

ZDI-CAN-10755: Microsoft
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 'Abdul-Aziz Hariri & Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-10671: 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 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-10668: 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 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-10661: 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 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-10659: Advantech
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-10623: Advantech
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was

reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10622: 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 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10621: Advantech

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10579: 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 'Yu Zhou(@yuzhou6666) of \xe5\xb0\x8f\xe9\xb8\xa1\xe5\xb8\xae' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10441: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10440: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10439: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10436: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10435: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10434: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10433: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10432: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10431: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10430: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10429: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10428: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10427: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10426: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10425: Horde

A CVSS score 6.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Esteban Ruiz (mr_me) of Source Incite' was reported to the affected vendor on: 2020-03-18, 5 days ago. The vendor is given until 2020-07-16 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2020-0942-01

Red Hat Security Advisory 2020-0942-01 - The runC tool is a lightweight, portable implementation of the Open Container Format that provides container runtime. A race condition has been addressed.

Red Hat Security Advisory 2020-0939-01

Red Hat Security Advisory 2020-0939-01 - Red Hat AMQ Streams, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 1.4.0 serves as a replacement for Red Hat AMQ Streams 1.3.0, 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 a code execution vulnerability.

Red Hat Security Advisory 2020-0924-01

Red Hat Security Advisory 2020-0924-01 - The GNU Compiler Collection is a portable compiler suite with support for various programming languages, including C, C++, and Fortran. The devtoolset-8-gcc packages provide the Red Hat Developer Toolset version of GCC, as well as related libraries.

Red Hat Security Advisory 2020-0914-01

Red Hat Security Advisory 2020-0914-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.6.0. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-0920-01

Red Hat Security Advisory 2020-0920-01 - LibVNCServer is a C library that enables you to implement VNC server functionality into own programs. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2020-0913-01

Red Hat Security Advisory 2020-0913-01 - LibVNCServer is a C library that enables you to implement VNC server functionality into own programs. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2020-0912-01

Red Hat Security Advisory 2020-0912-01 - Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages technologies. A file read / inclusion vulnerability was addressed.

Red Hat Security Advisory 2020-0919-01

Red Hat Security Advisory 2020-0919-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.6.0. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-0921-01

Red Hat Security Advisory 2020-0921-01 - LibVNCServer is a C library that enables you to implement VNC server functionality into own programs. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2020-0918-01

Red Hat Security Advisory 2020-0918-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.6.0. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2020-0922-01

Red Hat Security Advisory 2020-0922-01 - 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 7.6.0 serves as a replacement for Red Hat AMQ Broker 7.5.0, 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 cross site scripting, denial of service, and information leakage vulnerabilities.

Gentoo Linux Security Advisory 202003-48

Gentoo Linux Security Advisory 202003-48 - Multiple vulnerabilities have been found in Node.js, worst of which could allow remote attackers to write arbitrary files. Versions less than 12.15.0 are affected.

Gentoo Linux Security Advisory 202003-47

Gentoo Linux Security Advisory 202003-47 - A vulnerability in Exim could allow a remote attacker to execute arbitrary code. Versions less than 4.92.3 are affected.

Avast Secure Browser 76.0.1659.101 Local Privilege Escalation

A local privilege escalation issue was discovered in Avast Secure Browser version 76.0.1659.101. The vulnerability is due to an insecure ACL set by the AvastBrowserUpdate.exe (which is running as NT AUTHORITY\SYSTEM) when AvastSecureBrowser.exe checks for new updates.

Red Hat Security Advisory 2020-0801-01

Red Hat Security Advisory 2020-0801-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0798-01

Red Hat Security Advisory 2020-0798-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0802-01

Red Hat Security Advisory 2020-0802-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0803-01

Red Hat Security Advisory 2020-0803-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0800-01

Red Hat Security Advisory 2020-0800-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0799-01

Red Hat Security Advisory 2020-0799-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0796-01

Red Hat Security Advisory 2020-0796-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. An issue was resolved where /etc/passwd was given incorrect privileges.

Red Hat Security Advisory 2020-0795-01

Red Hat Security Advisory 2020-0795-01 - 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 a cross site scripting vulnerability.

Oce Colorwave 500 CSRF / XSS / Authentication Bypass

Oce Colorwave 500 printer suffers from authentication bypass, cross site request forgery, and cross site scripting vulnerabilities.

Kernel Live Patch Security Notice LSN-0064-1

Paulo Bonzini discovered that the KVM hypervisor implementation in the Linux kernel could improperly let a nested (level 2) guest access the resources of a parent (level 1) guest in certain situations. An attacker could use this to expose sensitive information.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com