# CYBER WAR

WEEKLY AWARENESS REPORT

01-20-20

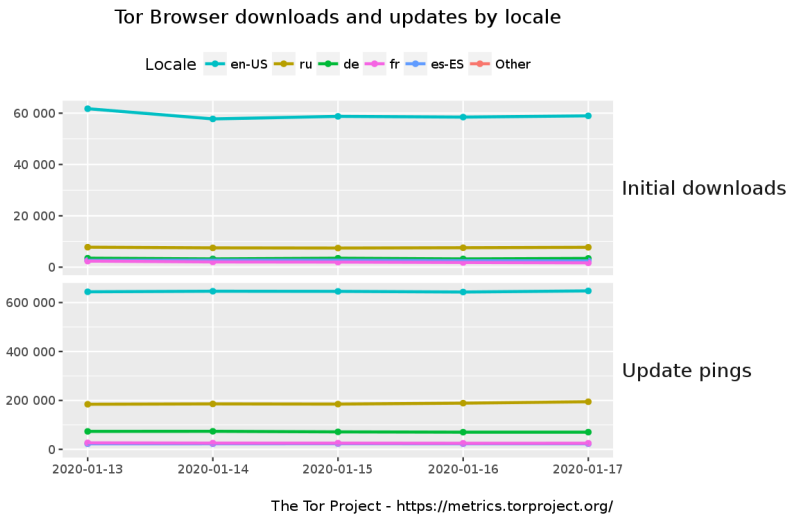
## January 20, 2020

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 Q1for 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**

* 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
* Aussie P&N Bank Suffers Data Breach
* Researchers Find Serious Flaws In WordPress Plugins Used On 400k Sites
* EU Considers Facial Recognition Ban
* JhoneRAT Exploits Cloud To Attack Middle Eastern Countries
* Critical Windows Vuln Used To Rickroll The NSA And Github
* Oracle Just Released A Whopping 334 Security Fixes In Critical Patch Update
* Equifax Settles Class-Action Breach Lawsuit For $380.5 Million
* Intel Patches Six Security Issues
* Satan Ransomware Rebrands As 5ss5c Ransomware
* The NSA Has Discovered A Major Flaw In Windows 10
* FBI Arrests Man Suspected Of Dozens Of Swatting Calls
* Trump Attacks Apple In Push To Weaken Encryption
* Facebook To Notify Users Of Third-Party App Logins
* Remote Access Exploit Affects 200 Million Cable Modems
* Barr Pushes Apple For Help To Unlock Gunman's Phone
* CES Surveillance Hype Worries Privacy Advocates
* Russians Hack Energy Company That Played Major Role In Trump Ukraine Scandal
* Federally Funded Unimax Smartphone Preloaded With Malware
* Texas School District Falls For Email Scam, Hands Over $2.3 Million
* TrickBot Hackers Create New Stealthy Backdoor

**Krebs on Security**

* 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
* The Hidden Cost of Ransomware: Wholesale Password Theft
* Happy 10th Birthday, KrebsOnSecurity.com
* Ransomware at IT Services Provider Synoptek
* Nuclear Bot Author Arrested in Sextortion Case

**Dark Reading**

* Are We Secure Yet? How to Build a 'Post-Breach' Culture
* Mobile Banking Malware Up 50% in First Half of 2019
* FBI Seizes Domain That Sold Info Stolen in Data Breaches
* 7 Ways to Get the Most Out of a Penetration Test
* ADP Users Hit with Phishing Scam Ahead of Tax Season
* Massive Oracle Patch Reverses Company's Trend Toward Fewer Flaws
* With International Tensions Flaring, Cyber-Risk Is Heating Up for All Businesses
* New Attack Campaigns Suggest Emotet Threat Is Far From Over
* Phishing Today, Deepfakes Tomorrow: Training Employees to Spot This Emerging Threat
* CISO Resigns From Pete Buttigieg Presidential Campaign
* NY Fed Reveals Implications of Cyberattack on US Financial System
* Active Directory Needs an Update: Here's Why
* 2017 Data Breach Will Cost Equifax at Least $1.38 Billion
* Google Lets iPhone Users Turn Device into Security Key
* Why Firewalls Aren't Going Anywhere
* New Report Spotlights Changes in Phishing Techniques
* How to Comprehend the Buzz About Honeypots
* ISACs Join Forces to Secure the Travel Industry
* How SD-WAN Helps Achieve Data Security and Threat Protection
* Microsoft Patches Windows Vuln Discovered by the NSA

**The Hacker News**

* 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
* Critical Firefox 0-Day Under Active Attacks - Update Your Browser Now!
* Researchers Demonstrate How to Hack Any TikTok Account by Sending SMS
* 3 Google Play Store Apps Exploit Android Zero-Day Used by NSO Group
* Are You Ready for Microsoft Windows 7 End of Support on 14th January 2020?
* Xiaomi Cameras Connected to Google Nest Expose Video Feeds From Others
* Landry's Restaurant Chain Suffers Payment Card Theft Via PoS Malware

**Security Week**

* Hanna Andersson Data Breach: Hackers Compromise Website of Children's Clothier
* Apple Received Tens of Thousands of Government Requests in H1 2019
* NIST Releases Framework for Privacy Risk Management
* Citrix Releases First Patches for Critical ADC Vulnerability
* Microsoft to Patch Internet Explorer Vulnerability Exploited in Targeted Attacks
* Turkish Hackers Target Greek Government Websites, Stock Exchange
* FBI Takes Down Site Selling Subscriptions to Stolen Data
* Microsoft Introduces Free Source Code Analyzer
* Attacker Installs Backdoor, Blocks Others From Exploiting Citrix ADC Vulnerability
* New Legislation Would Require a Cybersecurity Coordinator in Every State
* Data Security Startup Cyral Emerges From Stealth Mode
* Industry Reactions to Crypto Vulnerability Found by NSA: Feedback Friday
* Hackers Earn $275,000 for Vulnerabilities in U.S. Army Systems
* Expert: Georgia Election Server Showed Signs of Tampering
* Siemens Warns of Security Risks Associated With Use of ActiveX
* U.S. Girds for Cyber Threats From Iran as Military Clash Fears Ebb
* Cloudflare Announces Free Security Services for Political Campaigns
* FBI Plans to Notify States About Local Election Breaches
* Peter Leav Named CEO of McAfee
* Many High-Risk Users Have Bad Security Habits: Google Survey

**Infosecurity Magazine**

* US Could Appoint a Cybersecurity Leader for Each State
* Possessing Ransomware Could Become Illegal in Maryland
* Mitsubishi Electric Discloses Information Leak
* â‚¬114m in Fines Imposed by Euro Authorities Under GDPR
* Travelex Begins Reboot as VPN Bug Persists
* London Councils Lose Nearly 1300 Devices Over Three Years
* Citrix Patches ADC Bug as Attacker Hoards Access
* Fidelis Cybersecurity Acquired by Skyview Capital
* NortonLifeLock Puts Silicon Valley Real Estate Up for Sale
* Teen Charged Over $50m SIM-Swapping Scam on Blockchain Experts
* Oracle Issues Record CPU with 334 Patches
* Equifax Breach Settlement Could Cost Firm Billions

**Naked Security**

* FBI seizes credentials-for-sale site WeLeakInfo.com
* FBI to inform election officials about hacking attempts
* Teen entered 'dark rabbit hole of suicidal content' online
* Facebook and Instagram ban alleged 'brainwashing' service
* Monday review - the hot 27 stories of the week
* 5 tips to avoid spear-phishing attacks
* Oracle's January 2020 update patches 334 security flaws
* Google will now accept your iPhone as an authentication key
* Facial recognition is real-life 'Black Mirror' stuff, Ocasio-Cortez says
* EDRi's guidelines call for more ethical websites

**Quick Heal - Security Simplified**

* 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!!
* Quick Heal Supports Windows 10 November 2019 Update
* This Children's Day, pledge the online security of your kids!
* Think loud! Can the regular delivery boy at your office launch a malware?
* BlueKeep Attacks seen in the wild!

**Threat Post**

* New JhoneRAT Malware Targets Middle East
* Feds Cut Off Access to Billions of Breached Records with Site Takedown
* Mobile Carrier Customer Service Ushers in SIM-Swap Fraud
* Threatpost Poll: Are Published PoC Exploits a Good or Bad Idea?
* News Wrap: PoC Exploits, Cable Haunt and Joker Malware
* FBI Plans to Inform States of Election Breaches
* Critical Cisco Flaws Now Have PoC Exploit
* Google Account Security Keys Launch for iPhone
* Satan Ransomware Reborn to Torment Businesses
* PoC Exploits Published For Microsoft Crypto Bug

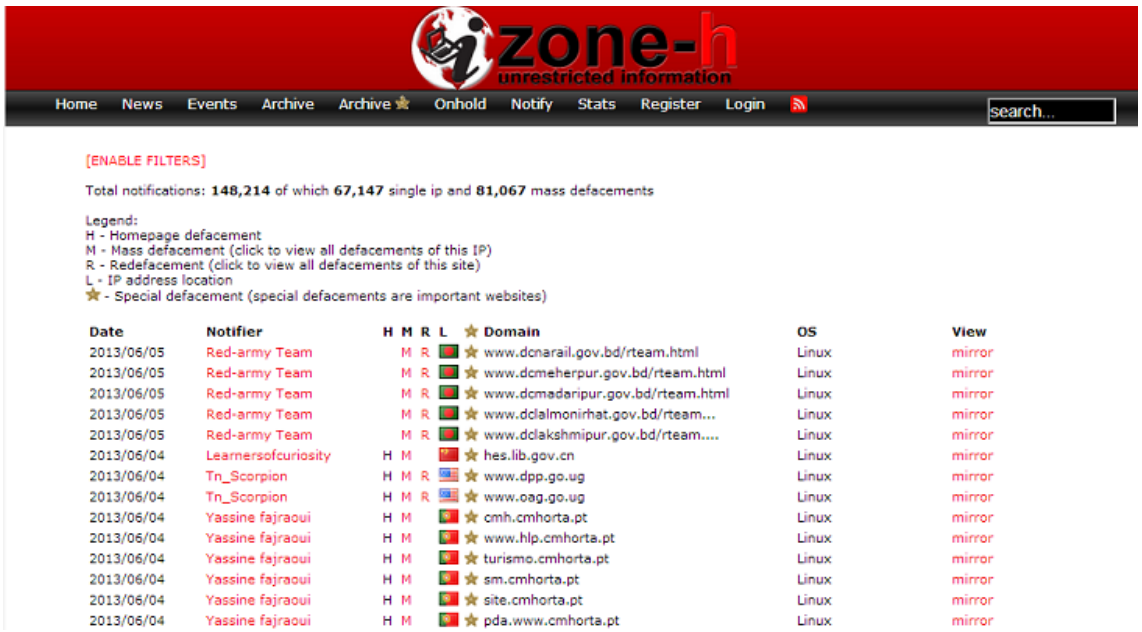
# The Hacker Corner

### 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**

* Maavi Fuzzing Utility
* Wireshark Analyzer 3.2.1
* Packet Fence 9.3.0
* SQLMAP - Automatic SQL Injection Tool 1.4
* Stegano 0.9.8
* Faraday 3.10.0
* GRR 3.4.0.1
* Wireshark Analyzer 3.2.0
* Suricata IDPE 5.0.1
* TestSSL 3.0rc6

**Kali Linux Tutorials**

* Lsassy : Extract Credentials From Lsass Remotel
* Top 3 Best Ways to Track Someone by Cell Phone Number
* LOLBITS : C# Reverse Shell Using BITS As Communication Protocol
* Shell Backdoor List : PHP / ASP Shell Backdoor List
* Hakrawler : Discovery Of Endpoints & Assets Within A Web Application
* GTFO : Search For Unix Binaries To Bypass System Security Restrictions
* SWFPFinder : SWF Potential Parameters Finder
* LaravelN00b : Automated Scan .env Files & Checking Debug Mode In Victim Host
* Andriller : Software Utility With A Collection Of Forensic Tools For Smartphones
* Lava : Large-scale Automated Vulnerability Addition

**GBHackers Analysis**

* 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
* CISA Releases Test Tool for Citrix ADC and Gateway Vulnerability - Sysadmins Can Test Now
* PoC Exploit Code Released for Citrix ACD and Gateway Remote Code Execution Vulnerability

**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

* Centreon 19.04 Remote Code Execution
* Sysax Multi Server 5.50 Denial Of Service
* Advie Framework 2.0.8 Cross Site Scripting
* Easy XML Editor 1.7.8 XML Injection
* Hospital Management System 4.0 Cross Site Scripting
* Microsoft .diagcab Directory Traversal / Code Execution
* Trend Micro Security (Consumer) Arbitrary Code Execution
* Trend Micro Security 2019 Security Bypass Protected Service Tampering
* Common Desktop Environment 2.3.1 Buffer Overflow
* Solaris xlock Information Disclosure
* WordPress Time Capsule 1.21.16 Authentication Bypass
* GTalk Password Finder 2.2.1 Denial Of Service
* WordPress InfiniteWP Client 1.9.4.5 Authentication Bypass
* Torrent FLV Converter 1.51 Build 117 Stack Overflow
* APKF Product Key Finder 2.5.8.0 Denial Of Service
* WordPress Resim ara 1.0 Cross Site Scripting
* Citrix ADC / Gateway Path Traversal
* Jenkins Gitlab Hook 1.4.2 Cross Site Scripting
* CurveBall Microsoft Windows CryptoAPI Spoofing Proof Of Concept
* CurveBall Microsoft Windows CryptoAPI Spoofing Proof Of Concept
* Tautulli 2.1.9 Denial Of Service
* Online Book Store 1.0 Arbitrary File Upload
* SunOS 5.10 Generic_147148-26 Local Privilege Escalation
* WordPress Postie 1.9.40 Cross Site Scripting
* Huawei HG255 Directory Traversal

### CXSecurity

* Tautulli 2.1.9 Denial of Service
* GTalk Password Finder 2.2.1 Denial Of Service
* Torrent FLV Converter 1.51 Build 117 Stack Overflow
* APKF Product Key Finder 2.5.8.0 Denial Of Service
* Huawei HG255 Directory Traversal
* SpotOutlook 1.2.6 Name Denial of Service (PoC)
* Citrix ADC (NetScaler) Directory Traversal / Remote Code Execution

# Proof of Concept (PoC) & Exploits

### Exploit Database

* [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
* [local] Torrent FLV Converter 1.51 Build 117 - Stack Oveflow (SEH partial overwrite)
* [dos] APKF Product Key Finder 2.5.8.0 - 'Name' Denial of Service (PoC)
* [remote] Sagemcom F@ST 3890 (50_10_19-T1) Cable Modem - 'Cable Haunt' Remote Code Execution
* [local] Microsoft Windows 10 (19H1 1901 x64) - 'ws2ifsl.sys' Use After Free Local Privilege Escalatio
* [webapps] Rukovoditel Project Management CRM 2.5.2 - 'filters' SQL Injection
* [local] Microsoft Windows - CryptoAPI (Crypt32.dll) Elliptic Curve Cryptography (ECC) Spoof Code-Sign
* [local] SunOS 5.10 Generic_147148-26 - Local Privilege Escalation
* [webapps] Rukovoditel Project Management CRM 2.5.2 - 'entities_id' SQL Injection
* [webapps] Citrix Application Delivery Controller (ADC) and Gateway 13.0 - Path Traversal
* [webapps] Tautulli 2.1.9 - Denial of Service ( Metasploit )
* [webapps] Online Book Store 1.0 - Arbitrary File Upload
* [webapps] Jenkins Gitlab Hook Plugin 1.4.2 - Reflected Cross-Site Scripting
* [webapps] Rukovoditel Project Management CRM 2.5.2 - 'reports_id' SQL Injection
* [webapps] WordPress Plugin Postie 1.9.40 - Persistent Cross-Site Scripting
* [remote] Barco WePresent - file_transfer.cgi Command Injection (Metasploit)

### 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**

* Jason Mancuso  - Machine Learnings Privacy Problem - DEF CON 27 AI Village
* Angelo Oliveira - Fighting Malware with Deep Learning video - DEF CON 27 AI Village
* Lauren Putvin  - Exploratory Data Analysis Why and How in Python - DEF CON 27 AI Village
* Jesus Solano - Behavioral Biometrics and Context Analytics - DEF CON 27 AI Village

**Hack5**

* 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
* Introducing the O.MG Cable

**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 - How to Self Study Coding
* Programming Intro - Introduction to Programming
* MySQL - HTML Form Validation with PHP (filter_var)
* MySQL - Sanitize Variables with PHP (filter_var)

**Security Now**

* Windows 7 - R. I. P. - Security Now 749
* Our Malware Lexicon - Security Now 748

**Troy Hunt**

* Weekly Update 174

# Advisories

**US-Cert Alerts & bulletins**

* Citrix Adds SD-WAN WANOP, Updated Mitigations to CVE-2019-19781 Advisory
* Microsoft Releases Security Advisory on Internet Explorer Vulnerability
* Google Releases Security Updates for Chrome
* Oracle Releases January 2020 Security Bulletin
* Adobe Releases Security Updates
* VMware Releases Security Update
* Intel Releases Security Updates
* Microsoft Releases January 2020 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 6, 2020
* Vulnerability Summary for the Week of December 30, 2019
* Vulnerability Summary for the Week of December 23, 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**

Secure communication principles
Alpha release of guidance to assess the security of voice, video and messaging services
Secure communications principles: alpha release
Guidance to help you assess the security of voice, video and messaging communication services

**Zero Day Initiative Advisories**

ZDI-CAN-9947: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9941: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9940: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9939: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9938: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9936: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9935: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-10099: VMware

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 'Reno Robert' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-10095: Trend Micro

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: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-10089: 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: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-10088: Trend Micro

A CVSS score 6.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2020-01-17, 3 days ago. The vendor is given until 2020-05-16 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-9973: Trading Technologies

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: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-9972: Trading Technologies

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: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-9971: Trading Technologies

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: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-9970: Trading Technologies

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: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-9607: NEC

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: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-10007: NEC

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 'Sivathmican Sivakumaran of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2020-01-16, 4 days ago. The vendor is given until 2020-05-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-9901: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-15, 5 days ago. The vendor is given until 2020-05-14 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-9898: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-15, 5 days ago. The vendor is given until 2020-05-14 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-9897: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-15, 5 days ago. The vendor is given until 2020-05-14 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-9895: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-15, 5 days ago. The vendor is given until 2020-05-14 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-10116: Microsoft

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'asnine' was reported to the affected vendor on: 2020-01-14, 6 days ago. The vendor is given until 2020-05-13 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-10076: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'anch0vy@theori, kkokkokye@theori' was reported to the affected vendor on: 2020-01-14, 6 days ago. The vendor is given until 2020-05-13 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-9998: 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 'Z0mb1E' was reported to the affected vendor on: 2020-01-10, 10 days ago. The vendor is given until 2020-05-09 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**

Debian Security Advisory 4606-1

Debian Linux Security Advisory 4606-1 - Several vulnerabilities have been discovered in the chromium web browser.

Ubuntu Security Notice USN-4242-1

Ubuntu Security Notice 4242-1 - It was discovered that Sysstat incorrectly handled certain inputs. An attacker could possibly use this issue to cause a crash or execute arbitrary code. This issue only affected Ubuntu 19.04 and Ubuntu 19.10. It was discovered that Sysstat incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. Various other issues were also addressed.

Debian Security Advisory 4604-1

Debian Linux Security Advisory 4604-1 - Multiple issues have been found in cacti, a server monitoring system, potentially resulting in SQL code execution or information disclosure by authenticated users.

Debian Security Advisory 4605-1

Debian Linux Security Advisory 4605-1 - Several vulnerabilities have been discovered in the OpenJDK Java runtime, resulting in denial of service, incorrect implementation of Kerberos GSSAPI and TGS requests or incorrect TLS handshakes.

Debian Security Advisory 4603-1

Debian Linux Security Advisory 4603-1 - Multiple security issues have been found in Thunderbird which could potentially result in the execution of arbitrary code or information disclosure.

Ubuntu Security Notice USN-4225-2

Ubuntu Security Notice 4225-2 - USN-4225-1 fixed vulnerabilities in the Linux kernel for Ubuntu 19.10. This update provides the corresponding updates for the Linux Hardware Enablement kernel from Ubuntu 19.10 for Ubuntu 18.04 LTS. It was discovered that a heap-based buffer overflow existed in the Marvell WiFi-Ex Driver for the Linux kernel. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4241-1

Ubuntu Security Notice 4241-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, conduct cross-site scripting attacks, or execute arbitrary code. It was discovered that NSS incorrectly handled certain memory operations. A remote attacker could potentially exploit this to cause a denial of service, or execute arbitrary code. Various other issues were also addressed.

Ubuntu Security Notice USN-4240-1

Ubuntu Security Notice 4240-1 - It was discovered that Kamailio incorrectly handled a specially crafted file. An attacker could possibly use this issue to cause a denial of service or other unspecified impact.

Red Hat Security Advisory 2020-0134-01

Red Hat Security Advisory 2020-0134-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address security vulnerabilities are now available. The updated versions are .NET Core SDK 3.0.102, .NET Core Runtime 3.0.2, .NET Core SDK 3.1.101 and .NET Core Runtime 3.1.1. Security Fixes: dotnet: Memory Corruption in SignalR. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2020-0132-01

Red Hat Security Advisory 2020-0132-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This release of Red Hat Process Automation Manager 7.6.0 serves as an update to Red Hat Process Automation Manager 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2020-0133-01

Red Hat Security Advisory 2020-0133-01 - Red Hat Decision Manager is an open source decision

management platform that combines business rules management, complex event processing, Decision Model & Notation execution, and Business Optimizer for solving planning problems. It automates business decisions and makes that logic available to the entire business. This release of Red Hat Decision Manager 7.6.0 serves as an update to Red Hat Decision Manager 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2020-0130-01

Red Hat Security Advisory 2020-0130-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation. New versions of .NET Core that address security vulnerabilities are now available. The updated versions are .NET Core SDK 3.0.102 and .NET Core Runtime 3.0.2. Security Fixes: dotnet: Memory Corruption in SignalR. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2020-0124-01

Red Hat Security Advisory 2020-0124-01 - Git is a distributed revision control system with a decentralized architecture. As opposed to centralized version control systems with a client-server model, Git ensures that each working copy of a Git repository is an exact copy with complete revision history. This not only allows the user to work on and contribute to projects without the need to have permission to push the changes to their official repositories, but also makes it possible for the user to work with no network connection. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2020-0122-01

Red Hat Security Advisory 2020-0122-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2020-0128-01

Red Hat Security Advisory 2020-0128-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. Issues addressed include a deserialization vulnerability.

Red Hat Security Advisory 2020-0127-01

Red Hat Security Advisory 2020-0127-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.4.1. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2020-0120-01

Red Hat Security Advisory 2020-0120-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.4.1. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2020-0123-01

Red Hat Security Advisory 2020-0123-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 68.4.1. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-4235-2

Ubuntu Security Notice 4235-2 - USN-4235-1 fixed a vulnerability in nginx. This update provides the corresponding update for Ubuntu 14.04 ESM. Bert JW Regeer and Francisco Oca Gonzalez discovered that nginx incorrectly handled certain error_page configurations. A remote attacker could possibly use this issue to perform HTTP request smuggling attacks and access resources contrary to expectations. Various other issues were also addressed.

Ubuntu Security Notice USN-4221-2

Ubuntu Security Notice 4221-2 - USN-4221-1 fixed a vulnerability in libpcap. This update provides the corresponding update for Ubuntu 12.04 ESM. It was discovered that libpcap did not properly validate PHB headers in some situations. An attacker could use this to cause a denial of service. Various other issues were also addressed.

Ubuntu Security Notice USN-4239-1

Ubuntu Security Notice 4239-1 - It was discovered that PHP incorrectly handled certain files. An attacker could

possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, 16.04 LTS, 18.04 LTS, 19.04 and 19.10. It was discovered that PHP incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. It was discovered that PHP incorrectly handled certain images. An attacker could possibly use this issue to access sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-4237-2

Ubuntu Security Notice 4237-2 - USN-4237-1 fixed several vulnerabilities in SpamAssassin. This update provides the corresponding update for Ubuntu 12.04 ESM and 14.04 ESM. It was discovered that SpamAssassin incorrectly handled certain CF files. If a user or automated system were tricked into using a specially-crafted CF file, a remote attacker could possibly run arbitrary code. Various other issues were also addressed.

Debian Security Advisory 4602-1

Debian Linux Security Advisory 4602-1 - Multiple vulnerabilities have been discovered in the Xen hypervisor, which could result in denial of service, guest-to-host privilege escalation or information leaks.

Red Hat Security Advisory 2020-0111-01

Red Hat Security Advisory 2020-0111-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 68.4.1 ESR. Issues addressed include a bypass vulnerability.

LINUX

CSILinux.com

CYBER SECRETS

INFORMATION WARFARE CENTER

InformationWarfareCenter.com