Sun City Computer Club

Cyber Security SIG

December 17, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

SolarWinds

- Breaking News
- Supply chain attack
- Military, Fortune 500, White House, universities, Pentagon, State department, Treasury, Microsoft, … a lot
- FireEye hack
- Orion platform
- CISA rare emergency directive
- Orion needs exclusion from security suite scan
- Reading, sending, ALTERING communications
- To be continued

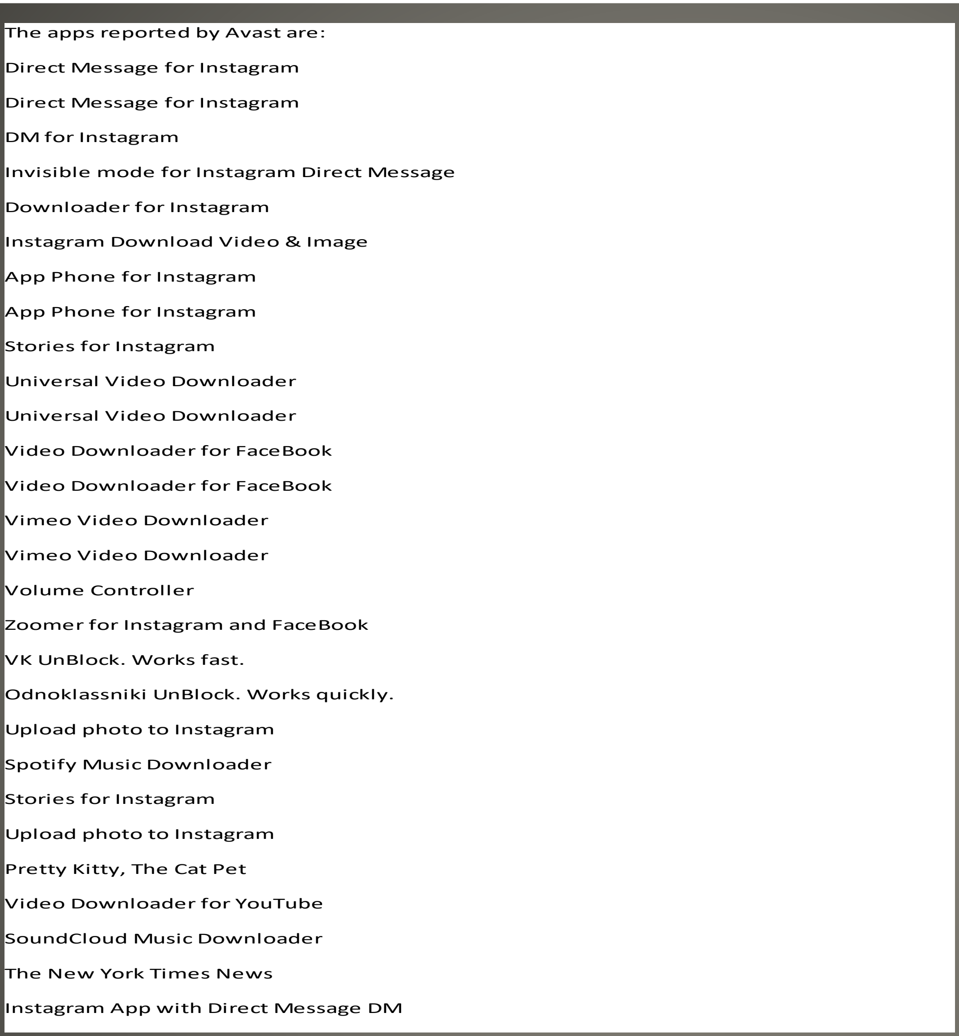
Current Issues

- Faraday cage
- eMail forwarding rules exploits
- Covid cold chain exploits
- DHS purchase of phone location data immigration
- Google authenticator
  Export accounts   Import accounts
  KEEP paper record
- IRS PI PIN (Personal Identity PIN)
- FireEye Red team tools stolen
- Firefox DoH public comment
- WordPress vulnerability to redirect to e-commerce stores
- FTC request data collection practices
- Flash end-of-support
- Firefox 84.0
- D-Link VPN   DSR family firmware 3.14 & 3.17
- We will reverse charges to your account
- 17,447 US-CERT vulnerabilities
- ToR Helpful <-> Harmful

- WSJ John Ratcliff China
  rob, replicate, replace
  51% ownership
  No divide between government and industry
- Adrozek
  Criminal they want your credentials
  infect all major browsers
  MACs might be more vulnerable
  30,000 per day
  Update Windows Defender signatures ; full scan
  Periodic check of browsers
  Periodic re-install of browsers
  Keep security suite signatures up-to-date

https://sccccyber.blogspot.com/2020/12/adrozek.html

Browser Extensions



The apps reported by Avast are:

Direct Message for Instagram

Direct Message for Instagram

DM for Instagram

Invisible mode for Instagram Direct Message

Downloader for Instagram

Instagram Download Video & Image

App Phone for Instagram

App Phone for Instagram

Stories for Instagram

Universal Video Downloader

Universal Video Downloader

Video Downloader for FaceBook

Video Downloader for FaceBook

Vimeo Video Downloader

Vimeo Video Downloader

Volume Controller

Zoomer for Instagram and FaceBook

VK UnBlock. Works fast.

Odnoklassniki UnBlock. Works quickly.

Upload photo to Instagram

Spotify Music Downloader

Stories for Instagram

Upload photo to Instagram

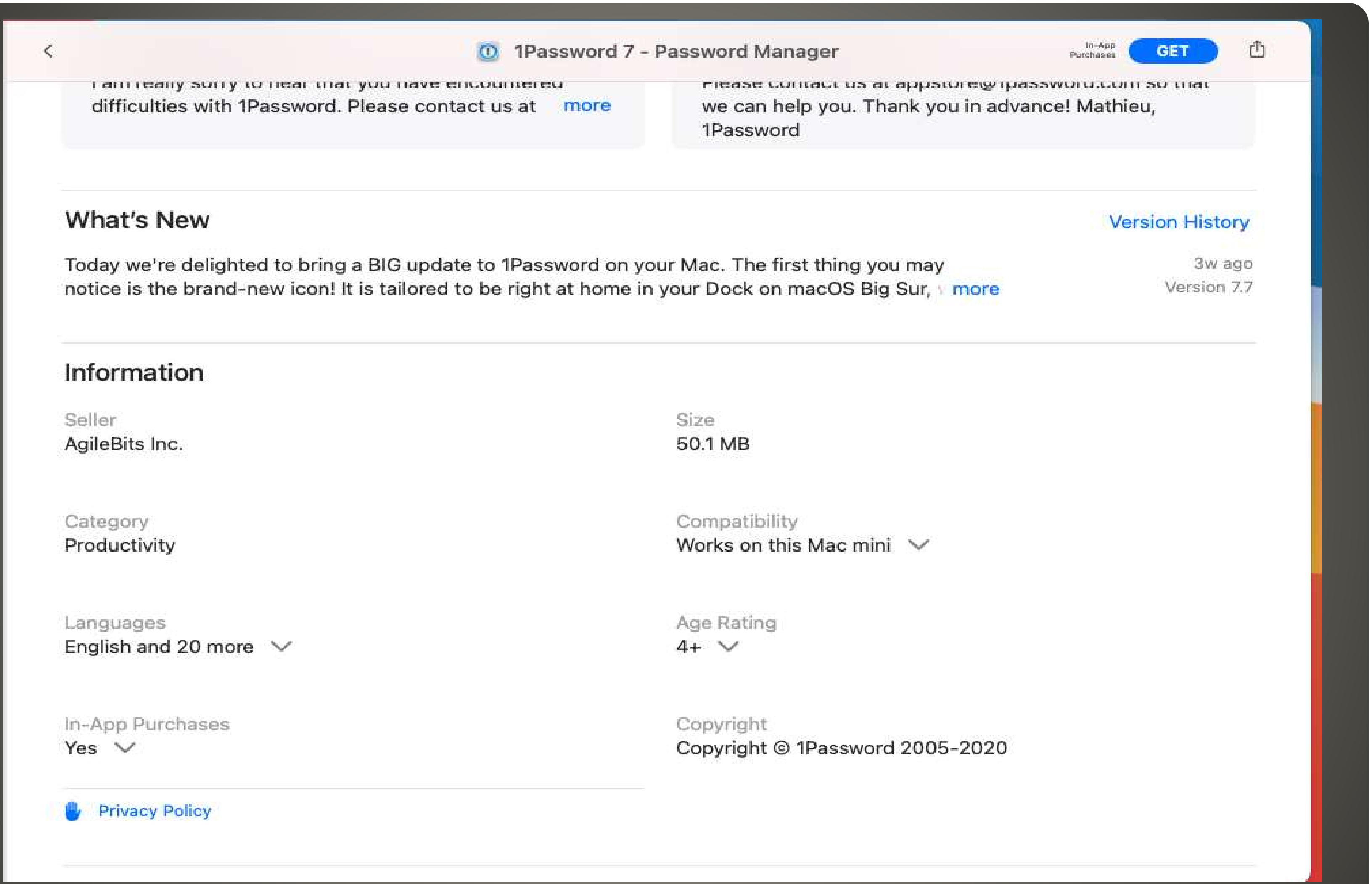
Pretty Kitty, The Cat Pet

Video Downloader for YouTube

SoundCloud Music Downloader

The New York Times News

Instagram App with Direct Message DM



I am really sorry to hear that you have encountered difficulties with 1Password. Please contact us at more

Please contact us at appstore@1password.com so that we can help you. Thank you in advance! Mathieu, 1Password

What's New

Version History

Today we're delighted to bring a BIG update to 1Password on your Mac. The first thing you may notice is the brand-new icon! It is tailored to be right at home in your Dock on macOS Big Sur, more

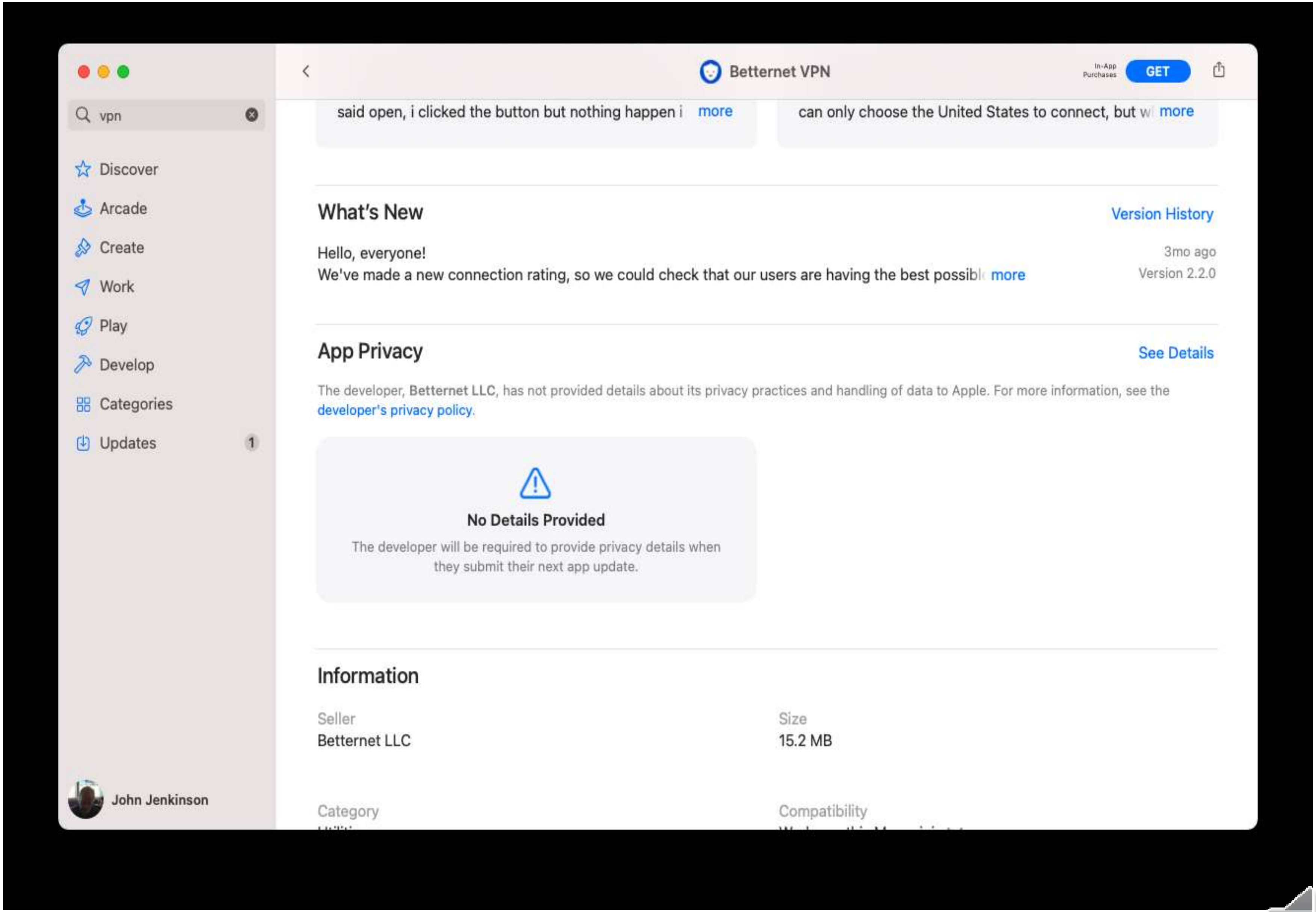
3w ago
Version 7.7

Information

Seller AgileBits Inc.	Size 50.1 MB
Category Productivity	Compatibility Works on this Mac mini
Languages English and 20 more	Age Rating 4+
In-App Purchases Yes	Copyright Copyright © 1Password 2005-2020

Privacy Policy

Apple store privacy



said open, i clicked the button but nothing happen i

can only choose the United States to connect, but w

What's New

Hello, everyone!
We've made a new connection rating, so we could check that our users are having the best possibl

3mo ago
Version 2.2.0

App Privacy

The developer, **Betternet LLC**, has not provided details about its privacy practices and handling of data to Apple. For more information, see the developer's privacy policy.

No Details Provided

The developer will be required to provide privacy details when they submit their next app update.

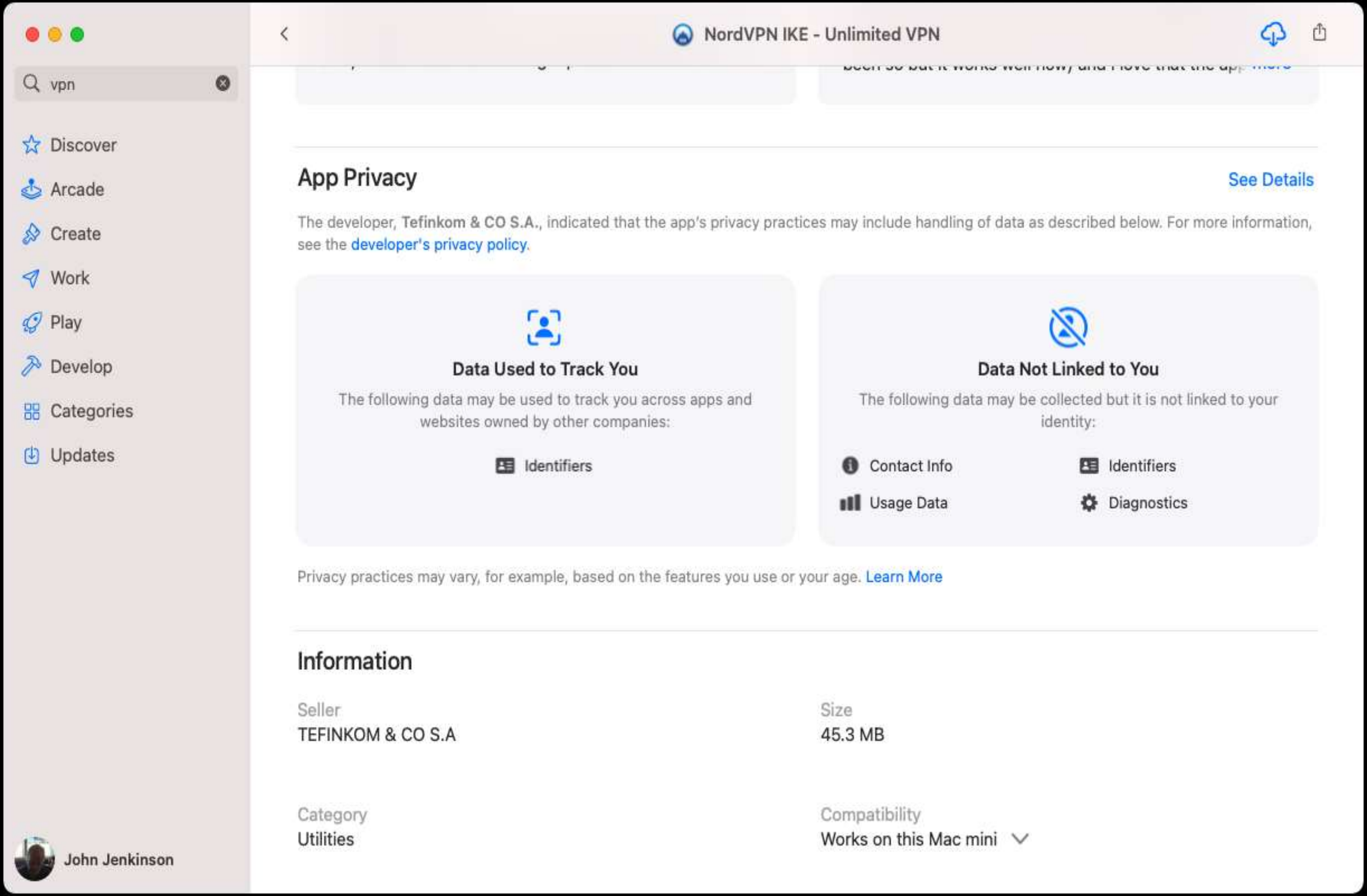
Information

Seller
Betternet LLC

Size
15.2 MB

Category

Compatibility



App Privacy

See Details

The developer, **Tefinkom & CO S.A.**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Identifiers

Data Not Linked to You

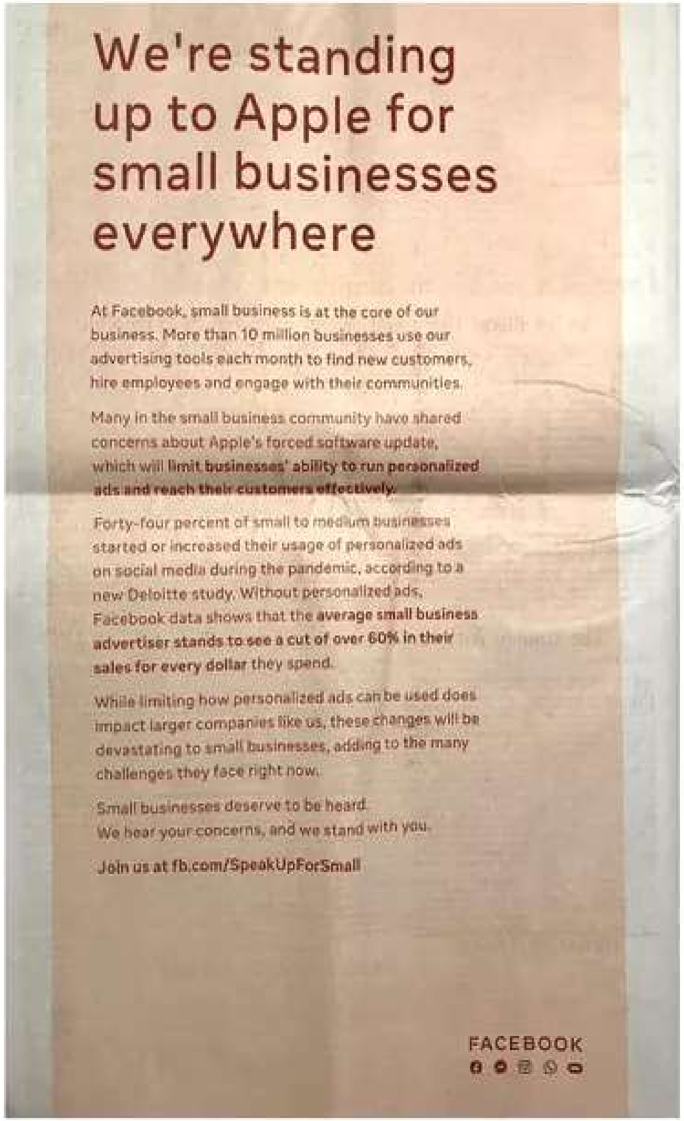
The following data may be collected but it is not linked to your identity:

- Contact Info
- Identifiers
- Usage Data
- Diagnostics

Privacy practices may vary, for example, based on the features you use or your age. Learn More

Information

Seller TEFINKOM & CO S.A	Size 45.3 MB
Category Utilities	Compatibility Works on this Mac mini



We're standing up to Apple for small businesses everywhere

At Facebook, small business is at the core of our business. More than 10 million businesses use our advertising tools each month to find new customers, hire employees and engage with their communities.

Many in the small business community have shared concerns about Apple's forced software update, which will **limit businesses' ability to run personalized ads and reach their customers effectively.**

Forty-four percent of small to medium businesses started or increased their usage of personalized ads on social media during the pandemic, according to a new Deloitte study. Without personalized ads, Facebook data shows that the **average small business advertiser stands to see a cut of over 60% in their sales for every dollar** they spend.

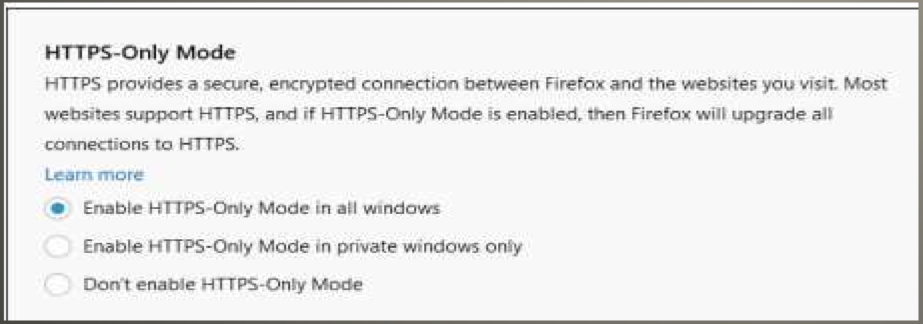
While limiting how personalized ads can be used does impact larger companies like us, these changes will be devastating to small businesses, adding to the many challenges they face right now.

Small businesses deserve to be heard.
We hear your concerns, and we stand with you.

Join us at fb.com/SpeakUpForSmall

FACEBOOK

- US Cybersecurity Information Sharing Act Update ?
- US weather service limit bandwidth
- Microsoft Windows force install 1903
- Raspberry Pi OS update/upgrade
- Laptop dock firmware update
- Firefox https only mode



HTTPS-Only Mode

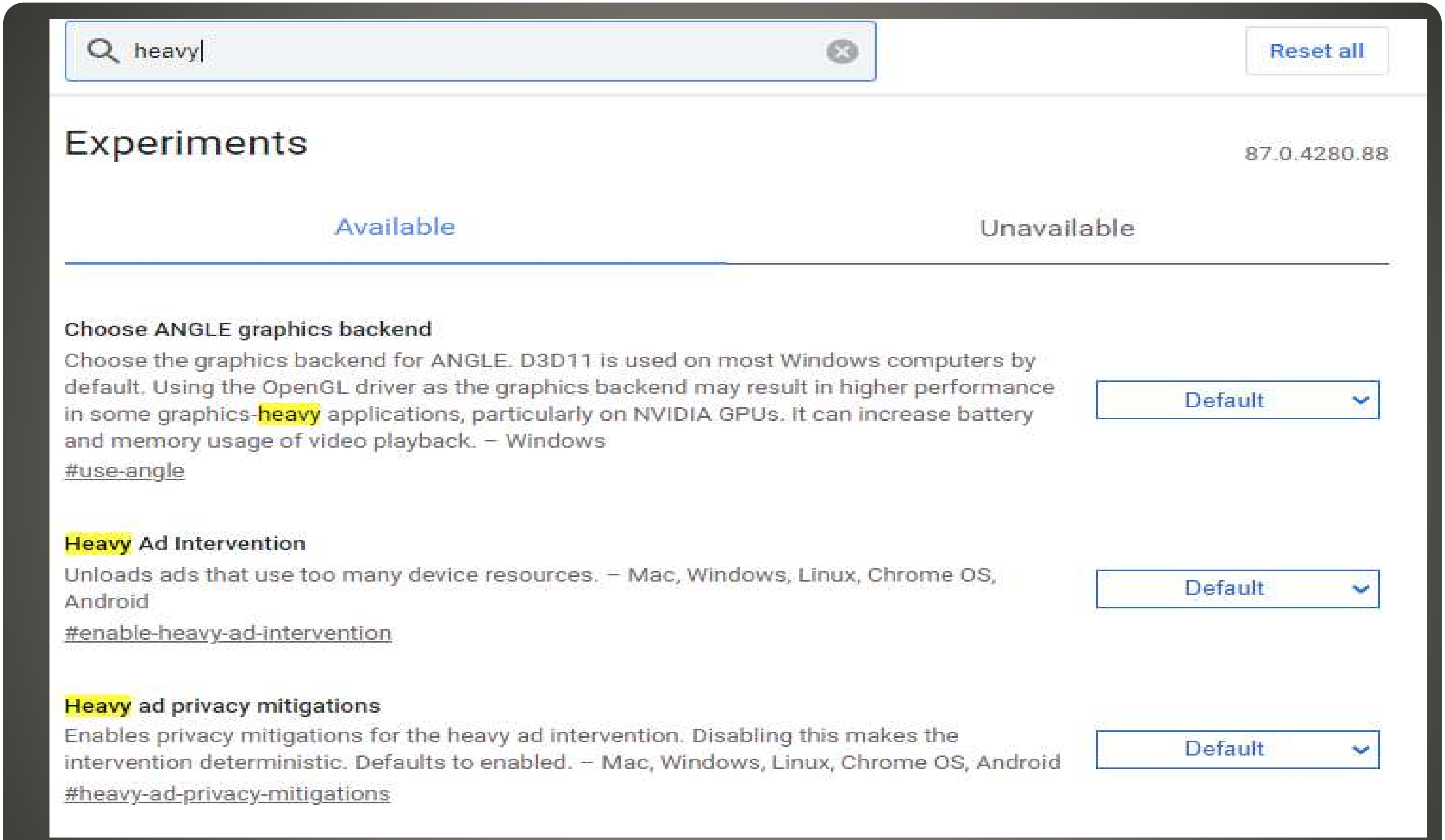
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

Learn more

● Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

○ Don't enable HTTPS-Only Mode



Experiments

87.0.4280.88

Choose ANGLE graphics backend

Choose the graphics backend for ANGLE. D3D11 is used on most Windows computers by default. Using the OpenGL driver as the graphics backend may result in higher performance in some graphics-heavy applications, particularly on NVIDIA GPUs. It can increase battery and memory usage of video playback. – Windows

#use-angle

Default

Heavy Ad Intervention

Unloads ads that use too many device resources. – Mac, Windows, Linux, Chrome OS, Android

#enable-heavy-ad-intervention

Default

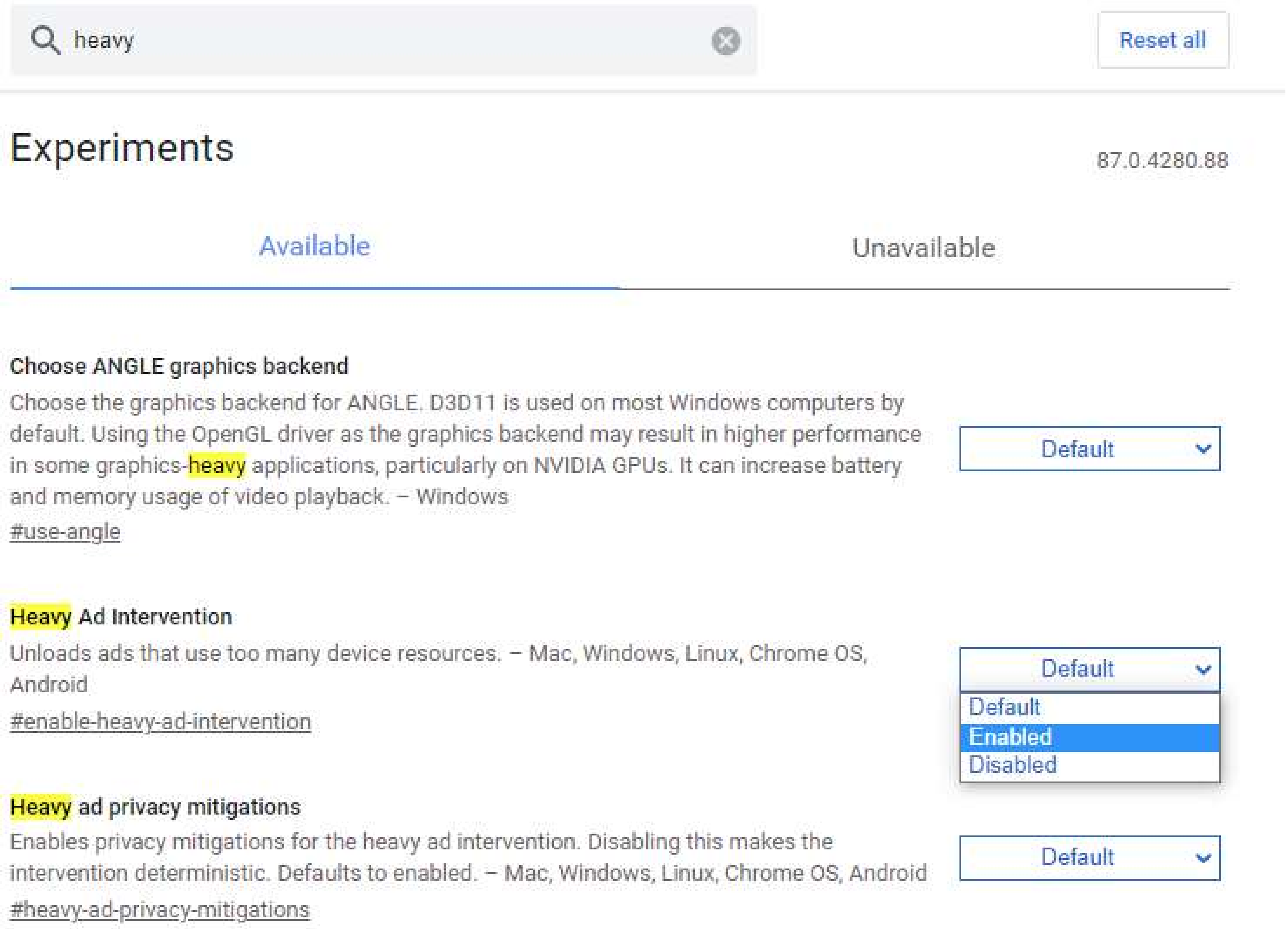
Heavy ad privacy mitigations

Enables privacy mitigations for the heavy ad intervention. Disabling this makes the intervention deterministic. Defaults to enabled. – Mac, Windows, Linux, Chrome OS, Android

#heavy-ad-privacy-mitigations

Default

Chrome Heavy Ad



Experiments

87.0.4280.88

Choose ANGLE graphics backend

Choose the graphics backend for ANGLE. D3D11 is used on most Windows computers by default. Using the OpenGL driver as the graphics backend may result in higher performance in some graphics-heavy applications, particularly on NVIDIA GPUs. It can increase battery and memory usage of video playback. – Windows

#use-angle

Default

Heavy Ad Intervention

Unloads ads that use too many device resources. – Mac, Windows, Linux, Chrome OS, Android

#enable-heavy-ad-intervention

Default

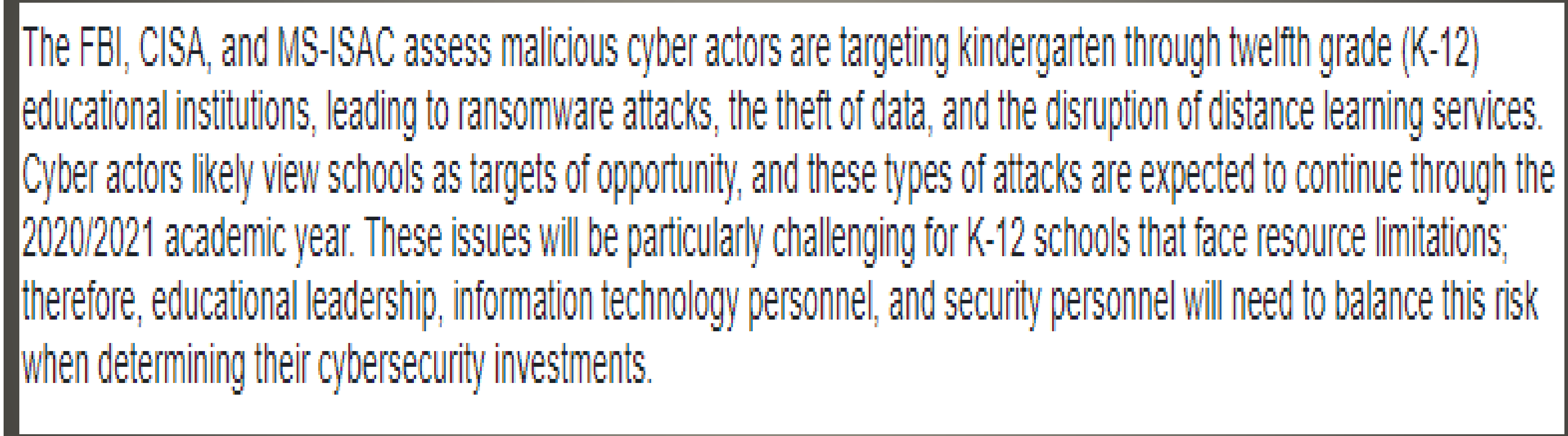
Heavy ad privacy mitigations

Enables privacy mitigations for the heavy ad intervention. Disabling this makes the intervention deterministic. Defaults to enabled. – Mac, Windows, Linux, Chrome OS, Android

#heavy-ad-privacy-mitigations

Default

- Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data | CISA



The FBI, CISA, and MS-ISAC assess malicious cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, the theft of data, and the disruption of distance learning services. Cyber actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year. These issues will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments.

US-CERT 10-Dec-2020

Why K-12?

- Virtual learning strained
- Have not invested in cyber defenses
- Probably not insured   no legal counsel
- Student data more valuable

Disabling browser updates

Disabling file integrity checks

Disabling the Safe Browsing feature

Registering and activating the extension they added in a previous step

Allowing their malicious extension to run in incognito mode

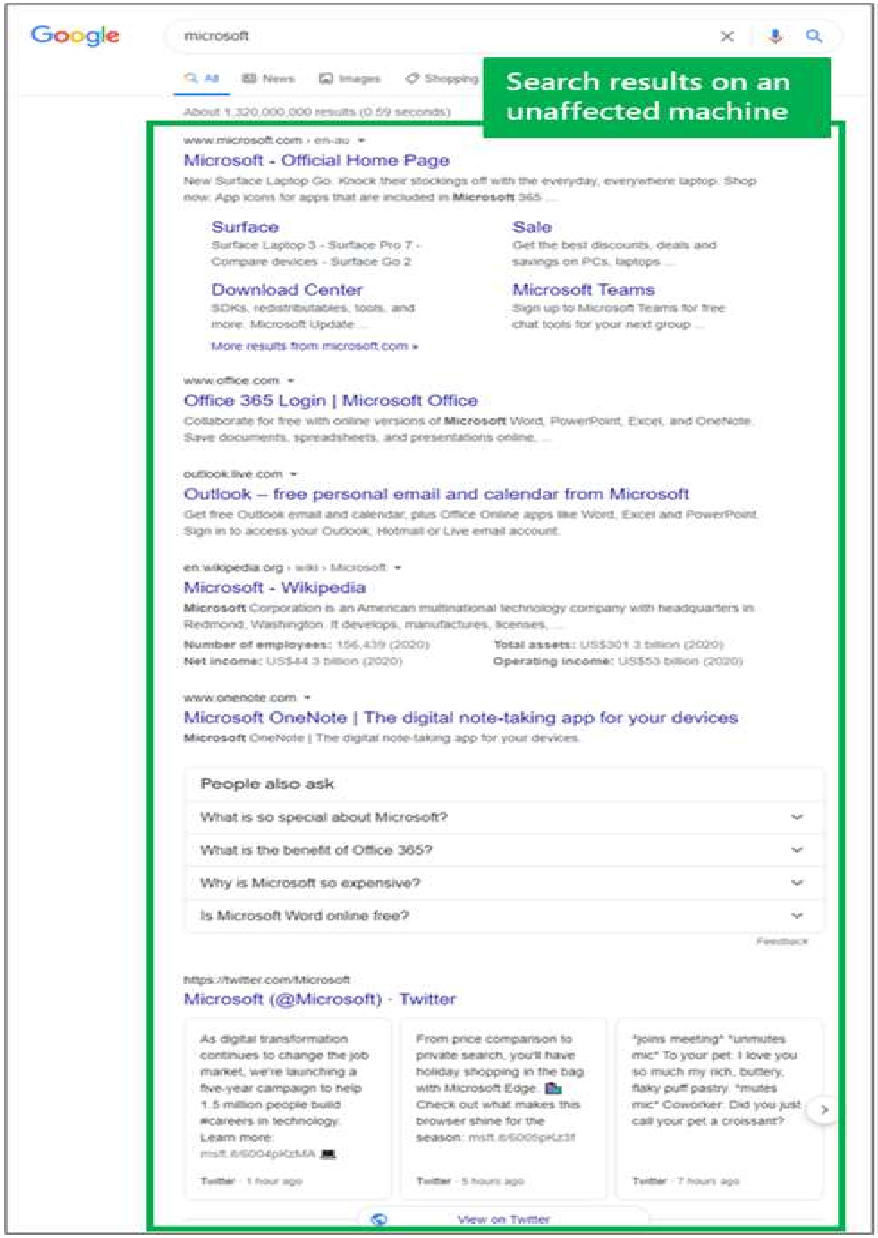
Allowing the extension to run without obtaining the appropriate permissions

Hiding the extension from the toolbar

Modifying the browser's default home page

Modifying the browser's default search engine

Adzrozek 30,000 / day



Google

microsoft

About 1,320,000,000 results (0.59 seconds)

Search results on an unaffected machine

www.microsoft.com › en-au ▾

Microsoft - Official Home Page

New Surface Laptop Go. Knock their stockings off with the everyday, everywhere laptop. Shop now. App icons for apps that are included in **Microsoft** 365 ...

Surface
Surface Laptop 3 - Surface Pro 7 - Compare devices - Surface Go 2

Sale
Get the best discounts, deals and savings on PCs, laptops ...

Download Center
SDKs, redistributables, tools, and more. Microsoft Update ...

Microsoft Teams
Sign up to Microsoft Teams for free chat tools for your next group ...

More results from microsoft.com »

www.office.com ▾

Office 365 Login | Microsoft Office

Collaborate for free with online versions of **Microsoft** Word, PowerPoint, Excel, and OneNote. Save documents, spreadsheets, and presentations online, ...

outlook.live.com ▾

Outlook – free personal email and calendar from Microsoft

Get free Outlook email and calendar, plus Office Online apps like Word, Excel and PowerPoint. Sign in to access your Outlook, Hotmail or Live email account.

en.wikipedia.org › wiki › Microsoft ▾

Microsoft - Wikipedia

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, ...

Number of employees: 156,439 (2020)
Total assets: US$301.3 billion (2020)
Net income: US$44.3 billion (2020)
Operating income: US$53 billion (2020)

www.onenote.com ▾

Microsoft OneNote | The digital note-taking app for your devices

Microsoft OneNote | The digital note-taking app for your devices.

People also ask

What is so special about Microsoft?

What is the benefit of Office 365?

Why is Microsoft so expensive?

Is Microsoft Word online free?

Feedback

https://twitter.com/Microsoft

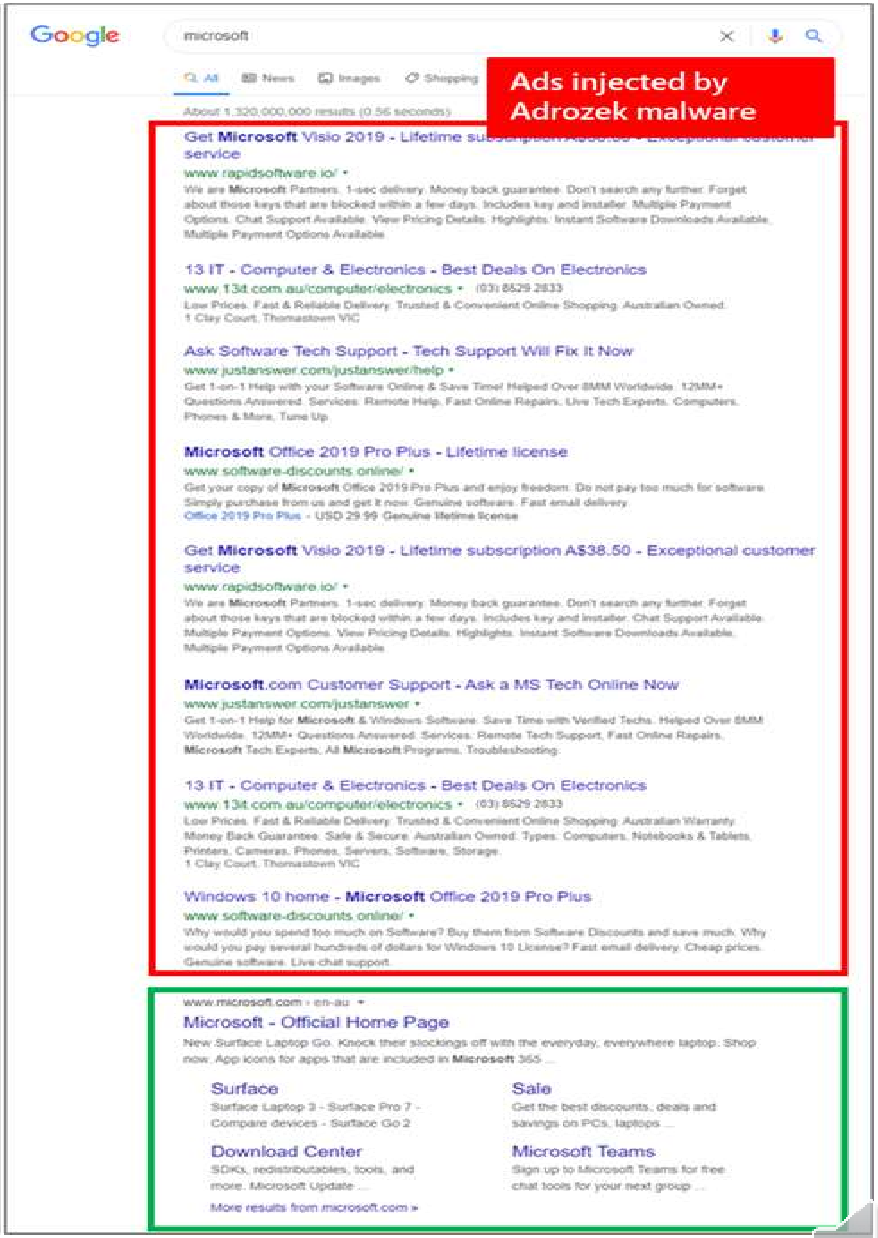
Microsoft (@Microsoft) · Twitter

As digital transformation continues to change the job market, we're launching a five-year campaign to help 1.5 million people build #careers in technology. Learn more: msft.it/6004pKzMA 💻
Twitter · 1 hour ago

From price comparison to private search, you'll have holiday shopping in the bag with Microsoft Edge. 🛍 Check out what makes this browser shine for the season: msft.it/6005pKz3f
Twitter · 5 hours ago

joins meeting *unmutes mic* To your pet: I love you so much my rich, buttery, flaky puff pastry. *mutes mic* Coworker: Did you just call your pet a croissant?
Twitter · 7 hours ago

View on Twitter



Google

microsoft

About 1,320,000,000 results (0.56 seconds)

Ads injected by Adrozek malware

Get **Microsoft** Visio 2019 - Lifetime su
service

www.rapidsoftware.io/ ▾

We are **Microsoft** Partners. 1-sec delivery. Money back guarantee. Don't search any further. Forget about those keys that are blocked within a few days. Includes key and installer. Multiple Payment Options. Chat Support Available. View Pricing Details. Highlights: Instant Software Downloads Available. Multiple Payment Options Available

13 IT - Computer & Electronics - Best Deals On Electronics

www.13it.com.au/computer/electronics ▾ (03) 8529 2833

Low Prices. Fast & Reliable Delivery. Trusted & Convenient Online Shopping. Australian Owned.
1 Clay Court, Thomastown VIC

Ask Software Tech Support - Tech Support Will Fix It Now

www.justanswer.com/justanswer/help ▾

Get 1-on-1 Help with your Software Online & Save Time! Helped Over 8MM Worldwide. 12MM+ Questions Answered. Services: Remote Help, Fast Online Repairs, Live Tech Experts, Computers, Phones & More, Tune Up

Microsoft Office 2019 Pro Plus - Lifetime license

www.software-discounts.online/ ▾

Get your copy of **Microsoft** Office 2019 Pro Plus and enjoy freedom. Do not pay too much for software. Simply purchase from us and get it now. Genuine software. Fast email delivery.
Office 2019 Pro Plus - USD 29.99 Genuine lifetime license

Get **Microsoft** Visio 2019 - Lifetime subscription A$38.50 - Exceptional customer service

www.rapidsoftware.io/ ▾

We are **Microsoft** Partners. 1-sec delivery. Money back guarantee. Don't search any further. Forget about those keys that are blocked within a few days. Includes key and installer. Chat Support Available. Multiple Payment Options. View Pricing Details. Highlights: Instant Software Downloads Available. Multiple Payment Options Available

Microsoft.com Customer Support - Ask a MS Tech Online Now

www.justanswer.com/justanswer ▾

Get 1-on-1 Help for **Microsoft** & Windows Software. Save Time with Verified Techs. Helped Over 8MM Worldwide. 12MM+ Questions Answered. Services: Remote Tech Support, Fast Online Repairs, **Microsoft** Tech Experts, All **Microsoft** Programs, Troubleshooting.

13 IT - Computer & Electronics - Best Deals On Electronics

www.13it.com.au/computer/electronics ▾ (03) 8529 2833

Low Prices. Fast & Reliable Delivery. Trusted & Convenient Online Shopping. Australian Warranty. Money Back Guarantee. Safe & Secure. Australian Owned. Types: Computers, Notebooks & Tablets, Printers, Cameras, Phones, Servers, Software, Storage.
1 Clay Court, Thomastown VIC

Windows 10 home - **Microsoft** Office 2019 Pro Plus

www.software-discounts.online/ ▾

Why would you spend too much on Software? Buy them from Software Discounts and save much. Why would you pay several hundreds of dollars for Windows 10 License? Fast email delivery. Cheap prices. Genuine software. Live chat support

www.microsoft.com › en-au ▾

Microsoft - Official Home Page

New Surface Laptop Go. Knock their stockings off with the everyday, everywhere laptop. Shop now. App icons for apps that are included in **Microsoft** 365 ...

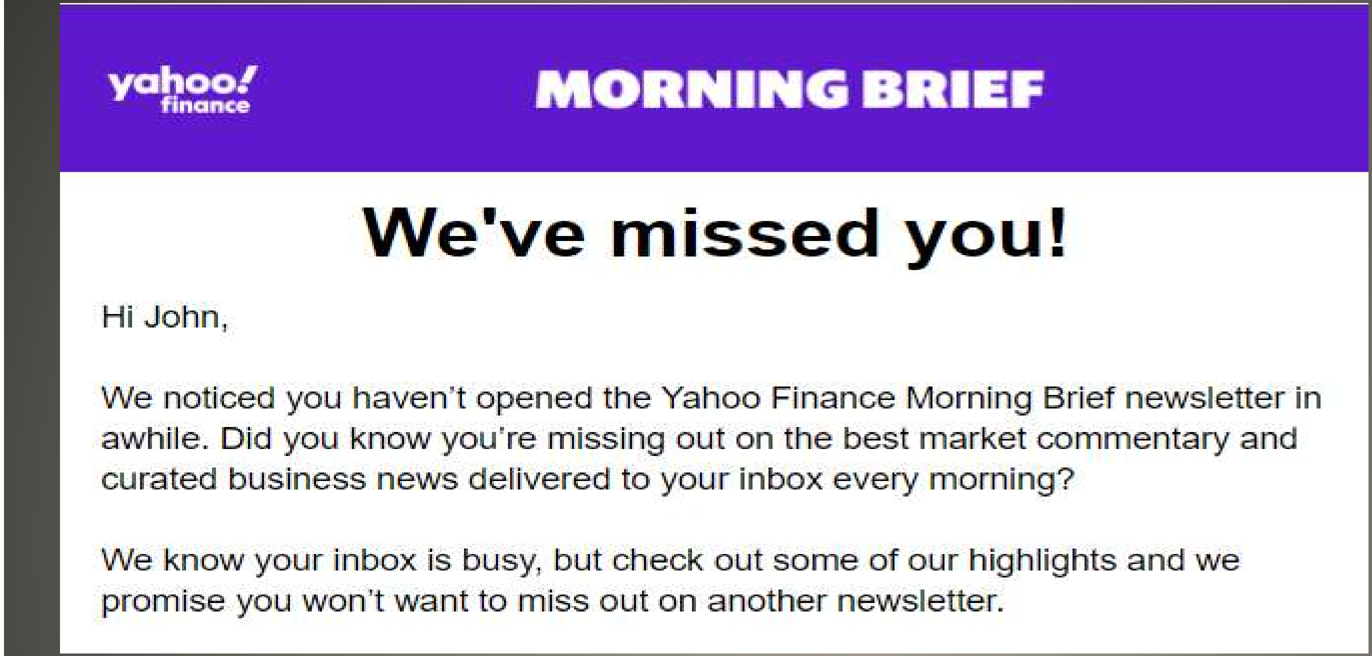
Surface
Surface Laptop 3 - Surface Pro 7 - Compare devices - Surface Go 2

Sale
Get the best discounts, deals and savings on PCs, laptops ...

Download Center
SDKs, redistributables, tools, and more. Microsoft Update ...

Microsoft Teams
Sign up to Microsoft Teams for free chat tools for your next group ...

More results from microsoft.com »



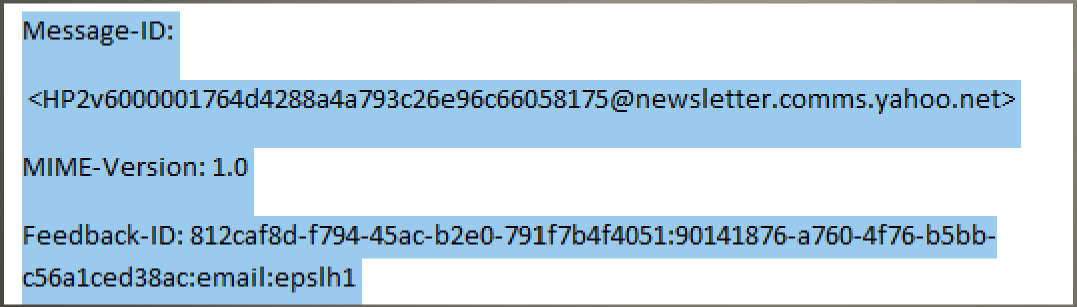
MORNING BRIEF

We've missed you!

Hi John,

We noticed you haven't opened the Yahoo Finance Morning Brief newsletter in awhile. Did you know you're missing out on the best market commentary and curated business news delivered to your inbox every morning?

We know your inbox is busy, but check out some of our highlights and we promise you won't want to miss out on another newsletter.

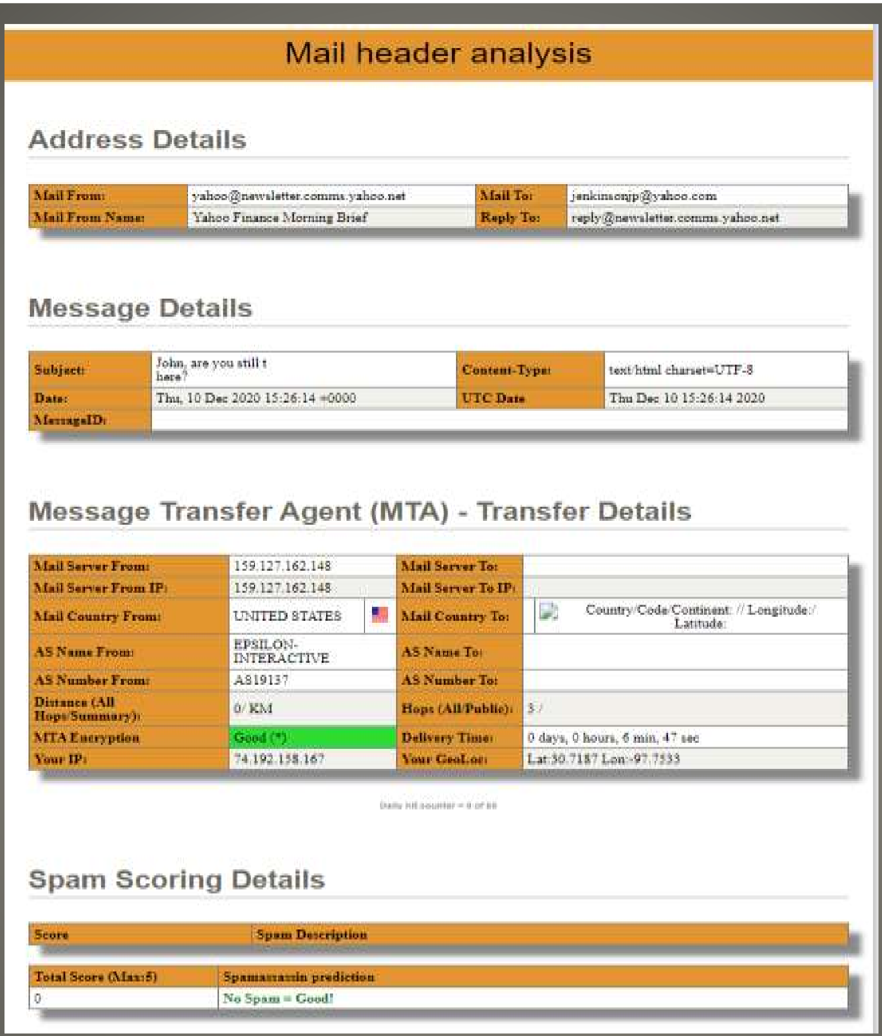


```
Message-ID:

 <HP2v6000001764d4288a4a793c26e96c66058175@newsletter.comms.yahoo.net>

MIME-Version: 1.0

Feedback-ID: 812caf8d-f794-45ac-b2e0-791f7b4f4051:90141876-a760-4f76-b5bb-
c56a1ced38ac:email:epslh1
```



Mail header analysis

Address Details

Mail From:	yahoo@newsletter.comms.yahoo.net	**Mail To:**	jenkinsonjp@yahoo.com
Mail From Name:	Yahoo Finance Morning Brief	**Reply To:**	reply@newsletter.comms.yahoo.net

Message Details

Subject:	John, are you still t here?	**Content-Type:**	text/html charset=UTF-8
Date:	Thu, 10 Dec 2020 15:26:14 +0000	**UTC Date**	Thu Dec 10 15:26:14 2020
MessageID:			

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	159.127.162.148	**Mail Server To:**	
Mail Server From IP:	159.127.162.148	**Mail Server To IP:**	
Mail Country From:	UNITED STATES 🇺🇸	**Mail Country To:**	Country/Code/Continent: // Longitude:/ Latitude:
AS Name From:	EPSILON-INTERACTIVE	**AS Name To:**	
AS Number From:	AS19137	**AS Number To:**	
Distance (All Hops/Summary):	0/ KM	**Hops (All/Public):**	3 /
MTA Encryption	Good (*)	**Delivery Time:**	0 days, 0 hours, 6 min, 47 sec
Your IP:	74.192.158.167	**Your GeoLoc:**	Lat:30.7187 Lon:-97.7533

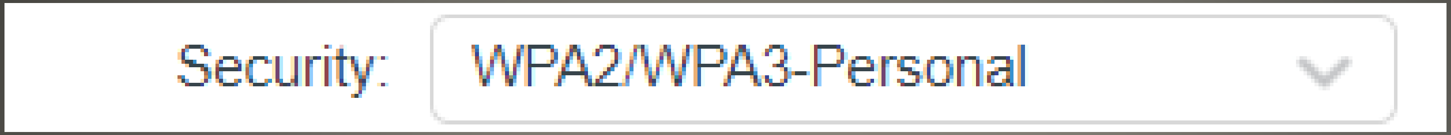
Daily hit counter = [illegible]

Spam Scoring Details

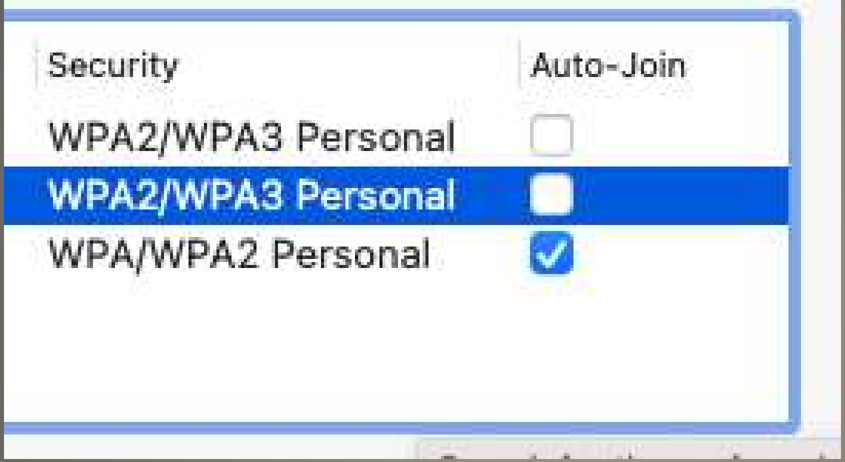
Score	**Spam Description**

Total Score (Max:5)	**Spamassassin prediction**
0	No Spam = Good!

E-Mail header mailheader.org



Security: WPA2/WPA3-Personal

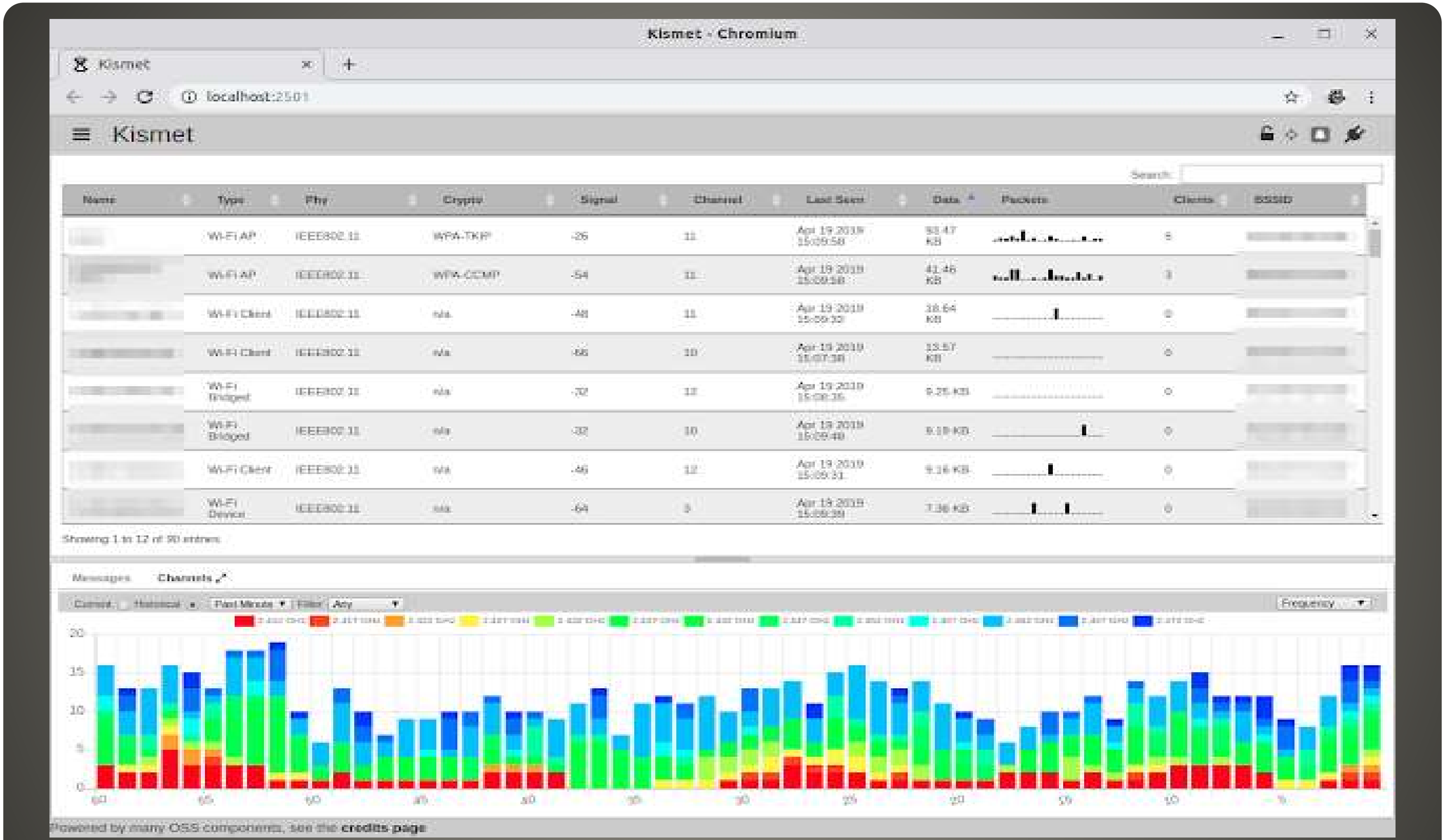


Security	Auto-Join
WPA2/WPA3 Personal	□
WPA2/WPA3 Personal	□
WPA/WPA2 Personal	☑

WPA3

- Wi-Fi 6 WPA3
  Faster?
- More and More
- 86 wi-fi at my home

Wi-Fi



Name	Type	Phy	Crypto	Signal	Channel	Last Seen	Data	Packets	Clients	BSSID
[redacted]	Wi-Fi AP	IEEE802.11	WPA-TKIP	-26	11	Apr 19 2019 15:09:58	93.47 KB		5	[redacted]
[redacted]	Wi-Fi AP	IEEE802.11	WPA-CCMP	-54	11	Apr 19 2019 15:09:58	41.46 KB		3	[redacted]
[redacted]	Wi-Fi Client	IEEE802.11	n/a	-48	11	Apr 19 2019 15:09:32	18.64 KB		0	[redacted]
[redacted]	Wi-Fi Client	IEEE802.11	n/a	-66	10	Apr 19 2019 15:07:38	13.57 KB		0	[redacted]
[redacted]	Wi-Fi Bridged	IEEE802.11	n/a	-72	12	Apr 19 2019 15:08:26	9.25 KB		0	[redacted]
[redacted]	Wi-Fi Bridged	IEEE802.11	n/a	-32	10	Apr 19 2019 15:09:48	9.19 KB		0	[redacted]
[redacted]	Wi-Fi Client	IEEE802.11	n/a	-46	12	Apr 19 2019 15:09:31	9.16 KB		0	[redacted]
[redacted]	Wi-Fi Device	IEEE802.11	n/a	-64	3	Apr 19 2019 15:09:39	7.36 KB		0	[redacted]

Showing 1 to 12 of 90 entries

Powered by many OSS components, see the **credits page**

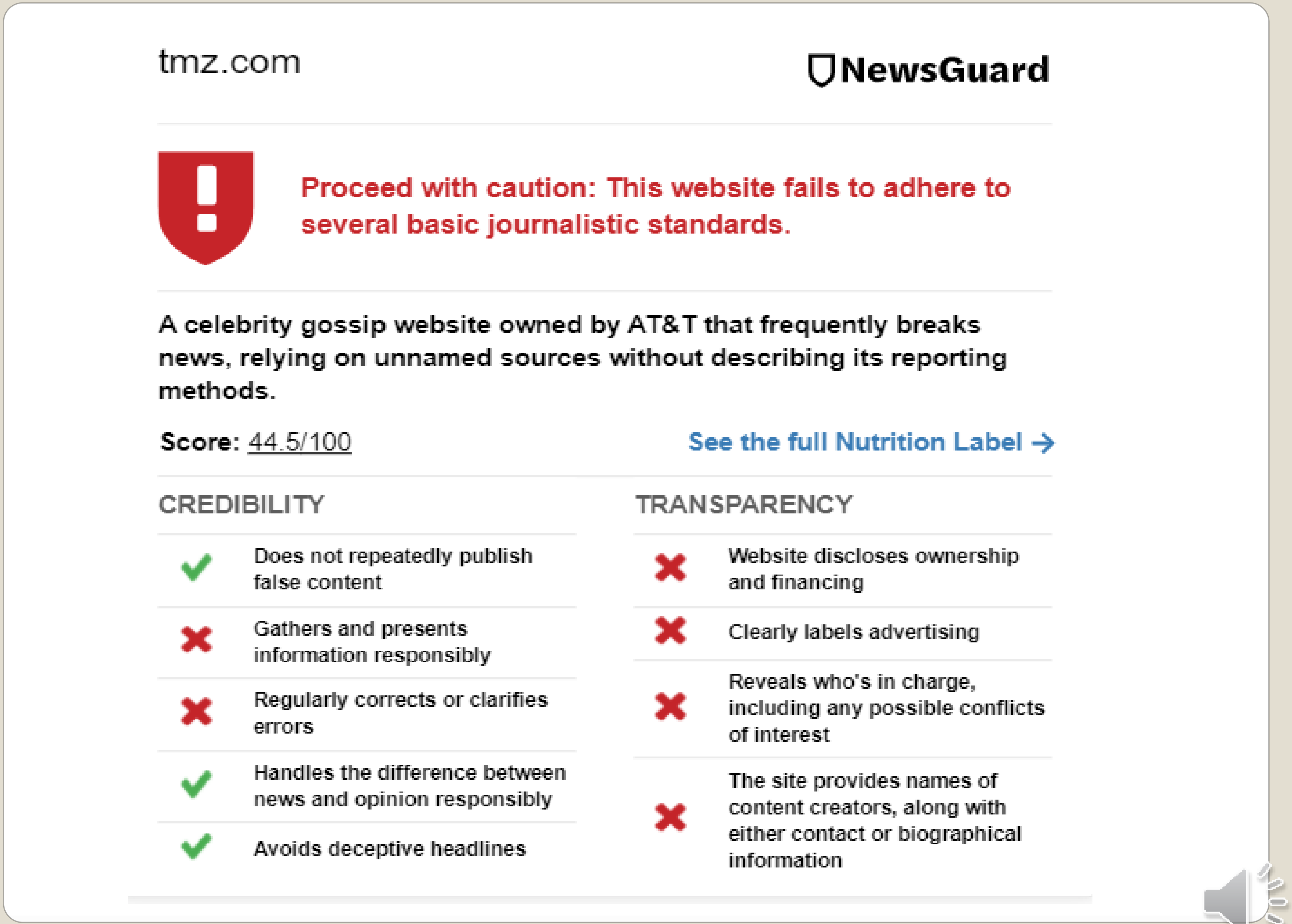
Kismet

Wi-Fi

- Kismet wireless IDS
  old machine
  Raspberry Pi
- WiFi Pineapple
- A wealth of apps

- APT32
  - Facebook claims
  - CyberOne group
    - CyberOne Security
    - CyberOne technologies
    - Hành Tinh
- APT10
  - Stone Panda 2009
  - NOT ransomware detects - undetectable

Advanced Persistent Threat



tmz.com

NewsGuard

Proceed with caution: This website fails to adhere to several basic journalistic standards.

A celebrity gossip website owned by AT&T that frequently breaks news, relying on unnamed sources without describing its reporting methods.

Score: 44.5/100

See the full Nutrition Label →

CREDIBILITY	
✓	Does not repeatedly publish false content
✗	Gathers and presents information responsibly
✗	Regularly corrects or clarifies errors
✓	Handles the difference between news and opinion responsibly
✓	Avoids deceptive headlines

TRANSPARENCY	
✗	Website discloses ownership and financing
✗	Clearly labels advertising
✗	Reveals who's in charge, including any possible conflicts of interest
✗	The site provides names of content creators, along with either contact or biographical information

Microsoft patching updating

- 58 patches latest patch Tuesday !
- 22 Remote code execution !!

- 0-click wormable vulnerability

  Microsoft Teams

  chat message as trigger

  Teams runs on macOS, Linux, ChromeOS, etc.

  NO CVE !

Microsoft patching policy shift

- *"..not to issue CVEs [for flaws in] products that automatically update without user's interaction."*

QUESTIONS ?

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs,
Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com