

Security-reducing apps

a call to action
for AVs to
update their
UwS and PUA
policies



AppEsteem[®]

Good News 😊

AVS have these traditional UwS and PUA apps (pretty much) under control in Windows and MacOS:

- Scary system utilities
- Tricky bundler offers
- Unwanted system changes
- Fake and misleading apps



Bad News ☹️

New security-reducing apps that don't obtain informed user consent skirt AV policies, leaving consumers at risk:

- Installing self-signed trusted root certs
- Resource borrowing
- Disabling/changing security settings
- Secretly monitoring targeted users



Informed user consent

- Says what will happen
- Explains the risks and how they're mitigated
- Requires agreement
- Isn't buried in EULA or privacy policy
- Isn't opt-out



But why do security-reducing apps need informed consent?

The risks and violating examples by category...



Installing self-signed trusted root certificates



Why apps do it: bypass browser/OS settings

- They want the browser to trust them when they say they're a specific website
- They want the OS to trust running a dynamically-signed executable

What this means

- Consumer must self-manage each trust instead of relying on OS

Risks to customer

- Fake websites, phishing
- Fake apps

Example apps installing self-signed trusted root certificates without informed consent

- VPN Proxy Master
- AdLock
- Stereoscopic Player

The image displays several screenshots illustrating the installation of self-signed certificates without user consent:

- Command Prompt (Top Left):** Shows the execution of `sigcheck64.exe -tv` for `Sigcheck v2.82`. The output lists valid certificates not rooted to the Microsoft Certificate Trust List, including one issued by `ThisISSparta,we` with a valid date of 10:35 PM 3/3/2023.
- Command Prompt (Middle Left):** Shows the execution of `sigcheck64.exe -tv` for `Sigcheck v2.82`. The output lists valid certificates not rooted to the Microsoft Certificate Trust List, including one issued by `AdLock CUSTOM CA 2` with a valid date of 9:32 PM 8/23/2002.
- Command Prompt (Bottom Left):** Shows the execution of `sigcheck64.exe -tv` for `Sigcheck v2.82`. The output lists valid certificates not rooted to the Microsoft Certificate Trust List, including one issued by `3dTV.at Root` with a valid date of 4:59 PM 12/31/2039.
- Certificate Manager (Top Right):** Shows the 'Trusted Root Certification Authorities' list. A certificate issued by `ThisISSparta,we` is highlighted in red.
- Certificate Manager (Middle Right):** Shows the 'Trusted Root Certification Authorities' list. A certificate issued by `3dTV.at Root` is highlighted in red.
- Certificate Manager (Bottom Right):** Shows the 'Trusted Root Certification Authorities' list. A certificate issued by `3dTV.at Root` is highlighted in red.

Resource Borrowing

Why apps do it: to monetize local network/compute

- Use local network for aggregators, VPN
- Use local compute for mining

What this means

- Consumers don't know what's happening on their machines
- They can't self-monitor the sharing

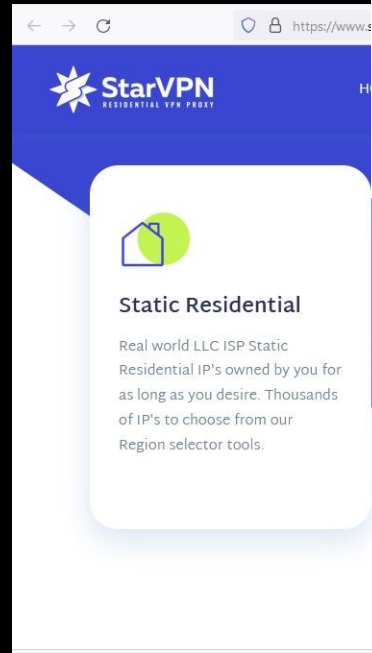
Risks to customer

- Hosting unwanted, illegal, or fraudulent activities
- Losing privacy
- Agreeing to an unfair trade



Example apps borrowing resources without informed consent

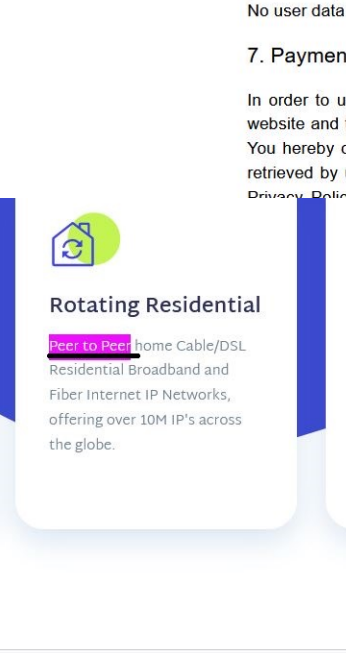
- UrbanVPN
- Star VPN
- 8K Video Downloader



StarVPN
RESIDENTIAL VPN PROXY

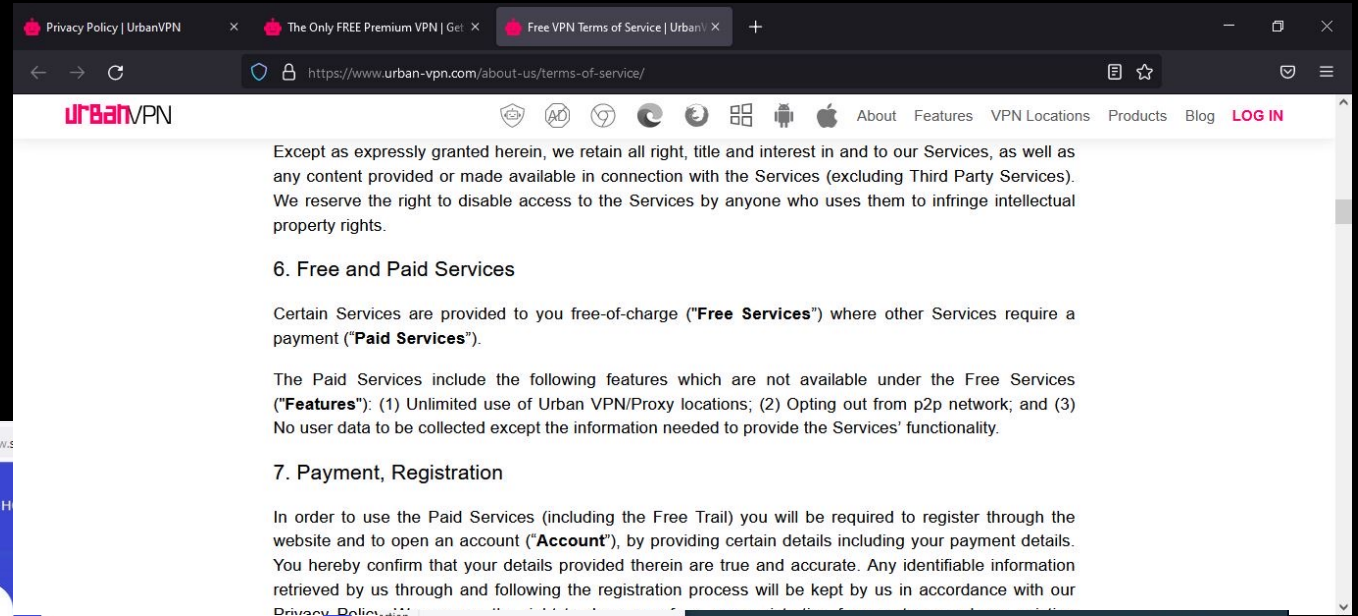
Static Residential

Real world LLC ISP Static Residential IP's owned by you for as long as you desire. Thousands of IP's to choose from our Region selector tools.



Rotating Residential

Peer to Peer home Cable/DSL Residential Broadband and Fiber Internet IP Networks, offering over 10M IP's across the globe.



UrbanVPN

Except as expressly granted herein, we retain all right, title and interest in and to our Services, as well as any content provided or made available in connection with the Services (excluding Third Party Services). We reserve the right to disable access to the Services by anyone who uses them to infringe intellectual property rights.

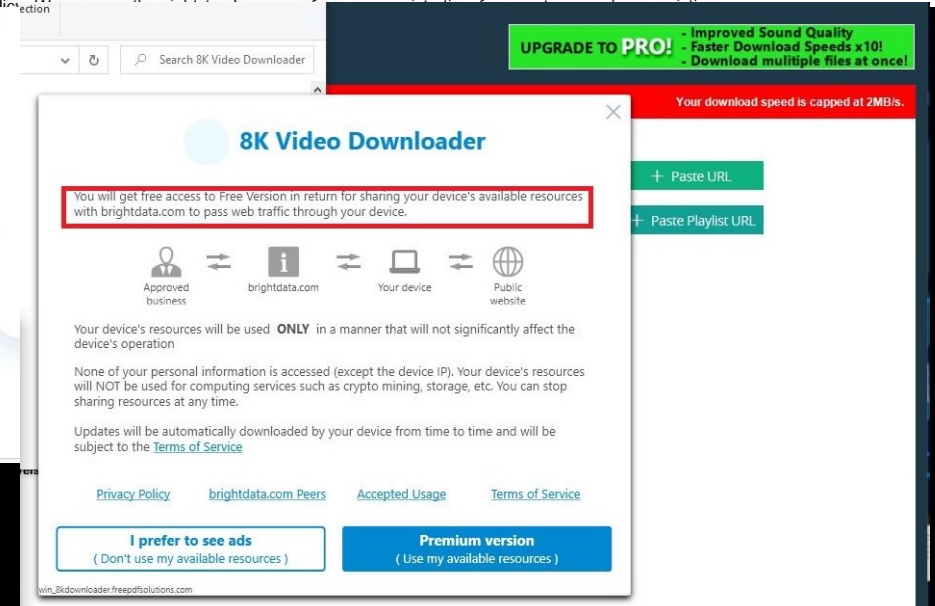
6. Free and Paid Services

Certain Services are provided to you free-of-charge ("**Free Services**") where other Services require a payment ("**Paid Services**").

The Paid Services include the following features which are not available under the Free Services ("**Features**"): (1) Unlimited use of Urban VPN/Proxy locations; (2) Opting out from p2p network; and (3) No user data to be collected except the information needed to provide the Services' functionality.

7. Payment, Registration

In order to use the Paid Services (including the Free Trail) you will be required to register through the website and to open an account ("**Account**"), by providing certain details including your payment details. You hereby confirm that your details provided therein are true and accurate. Any identifiable information retrieved by us through and following the registration process will be kept by us in accordance with our Privacy Policy.



8K Video Downloader

You will get free access to Free Version in return for sharing your device's available resources with brightdata.com to pass web traffic through your device.

Approved business ↔ brightdata.com ↔ Your device ↔ Public website

Your device's resources will be used **ONLY** in a manner that will not significantly affect the device's operation.

None of your personal information is accessed (except the device IP). Your device's resources will NOT be used for computing services such as crypto mining, storage, etc. You can stop sharing resources at any time.

Updates will be automatically downloaded by your device from time to time and will be subject to the [Terms of Service](#)

[Privacy Policy](#) [brightdata.com Peers](#) [Accepted Usage](#) [Terms of Service](#)

I prefer to see ads
(Don't use my available resources)

Premium version
(Use my available resources)

UPGRADE TO PRO! - Improved Sound Quality - Faster Download Speeds x10! - Download multiple files at once!

Your download speed is capped at 2MB/s.

+ Paste URL

+ Paste Playlist URL

Disabling/Changing Security Settings

Why apps do it: sell the illusion of control

- Increase speed, memory
- Reduce storage

What this means

- Consumer asked to trade protection for an unquantified benefit
- Consumer must now manage an ever-changing system risk

Risks to customer

- Lose in-depth protection
- Leave system vulnerable for attack



Example apps disabling/changing security settings without informed consent

- VIT Registry Fix
- JIT Cleaner

Things these kinds of apps do

- Disable AV
- Disable security notifications
- Punch unnecessary holes in firewall
- Remove web protection



Secretly Monitoring Targeted Users

Why apps do it: monetize suspicions

- Track partner, child, employee behavior: screens, keystrokes, conversations, history, locations while remaining “hidden”

What this means

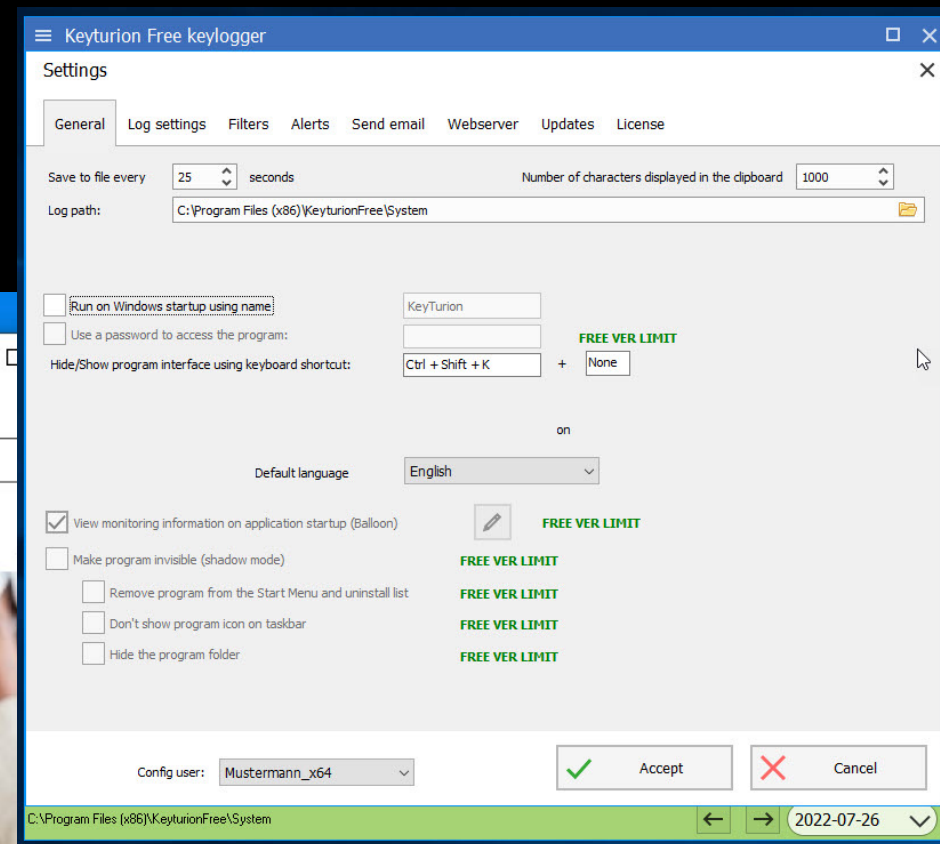
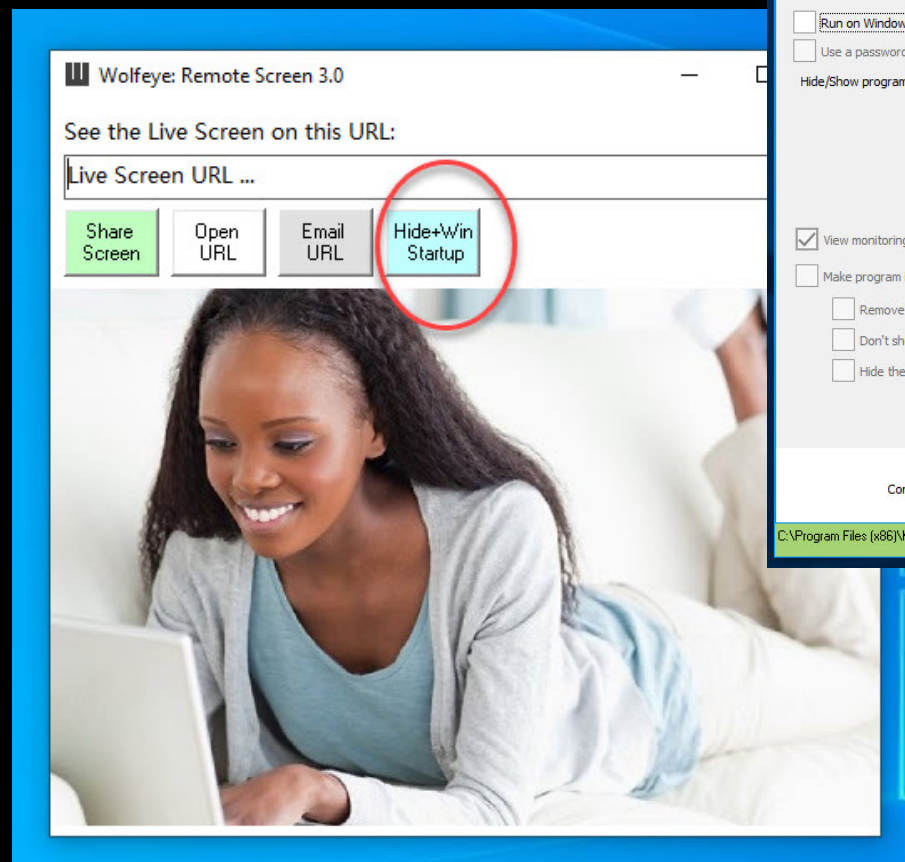
- Targeted consumers don't know they're being watched
- Purchaser must trust what vendor does with private data


Risks to customer

- Targeted users are unknowingly violated
- Private data getting leaked

Example apps secretly monitoring targeted users without their consent

- Keytursion Free Keylogger
- Wolfeye Remote Screen



A close-up photograph of a heavily rusted, brown metal padlock. The padlock is attached to a blue metal door handle. The blue paint on the door is chipped and peeling, revealing a reddish-brown metal underneath. The padlock has a keyhole and several screws on its body.

Security-reducing apps can leave both the system and its users vulnerable. These apps must first obtain informed user consent.

Not blocking violating apps leaves AV customers underserved.

If it's so obvious that security-reducing apps that don't obtain informed user consent are UWS or PUA...

App Name	App Version	Deceptor listing date	AVs detecting before we listed	AVs detecting after 1 week	AVs detecting after 2 weeks	AVs detecting now
VPN Proxy Master	3.11.0.0	3/11/22	0	21	26	27
AdLock	2.1.2.3	9/8/22	1	12	16	16
Steroscopic Player	2.5.1	6/6/22	0	10	15	16
UrbanVPN	2.2.4	3/13/22	0	13	16	18
StarVPN	1.1.18	3/29/22	1	9	26	31
8K Video Downloader	14.0	5/4/22	3	17	18	21
KeyTurion Free Keylogger	6.9	7/27/22	11	23	32	37
Wolfeye Remote Screen	3.0	7/21/22	0	27	50	49
VIT Registry Fix	14.7.0	2/28/22	1	6	21	36
Jcleaner	7.4.0.0	2/24/22	0	7	17	34

...why do so few AVs catch them?

(data from VirusTotal: detects of installers by 66 AVs)

Investigating why AVs miss these apps



- 1) AV Policy survey
- 2) Retrospective Detection Analysis of example apps
- 3) Categorization Analysis of example apps

1) Surveying AV policies and web statements highlights a potential policy gap

AV	What they say...
McAfee	Policy: “Software must gain informed user consent prior to making or modifying key system settings”
Sophos	Policy (matches ACR-007)
Avast	Blog: “[PUPs] can compromise the security of your computer”
BitDefender	Support: “[PUPs] alter system settings – which can mushroom into actual security and privacy issues.”
K7	Blog on self-signed trusted root certs by VPNs
MalwareBytes	Definition of PUP: “unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings, security settings or configuration”
Panda	Definition of PUP: “disabling security measures on computers”
AVG, Avira, ESET, GData, Kaspersky, Microsoft, Norton, Trend, Webroot	No policy, blog, definition, or support article discussing security-reducing apps

2) Retrospectively measuring time to detect after we listed also hints at a policy gap

AV	1 week	2 weeks	Now	Never/ Stopped
Avast/ AVG	4		5	1
Avira	5	4	1	
BitDefender	2	2	2	4
ESET	3	2	1	4
GData	1	3	3	3
K7	7	3		
Kaspersky	4	1		5
MalwareBytes	1	2		7
McAfee	7	3		
Microsoft	6		1	3
Norton	3	5	2	
Panda	8	1	1	
Sophos	9	1		
Trend	1	1	5	3
Webroot	3	3	3	1
No Policy, Statement Policy	Well-aligned	New-ish policy?	Reputation Detections	Policy Gap

3) Analyzing AV detections by category of app highlights which policies each AV is missing

AV	Self-signed trusted root cert	Resource borrowing	Disable or change security	Monitor targeted users
Avast/ AVG	Slow+	Slow+	Slow-	
Avira				Slow+
BitDefender	Never+	Never+		Slow-
ESET	Never	Never+		
GData	Never+	Slow-		Slow-
K7				
Kaspersky	Never		Never	
MalwareBytes	Never	Never	Never+	Never+
McAfee				
Microsoft	Never-	Stopped+		
Norton				
Panda				Slow+
Sophos				
Trend	Never+	Slow-		
Webroot		Slow-	Slow	
No Policy , Statement Policy				

Conclusion

Many AVs don't detect security-reducing apps because...

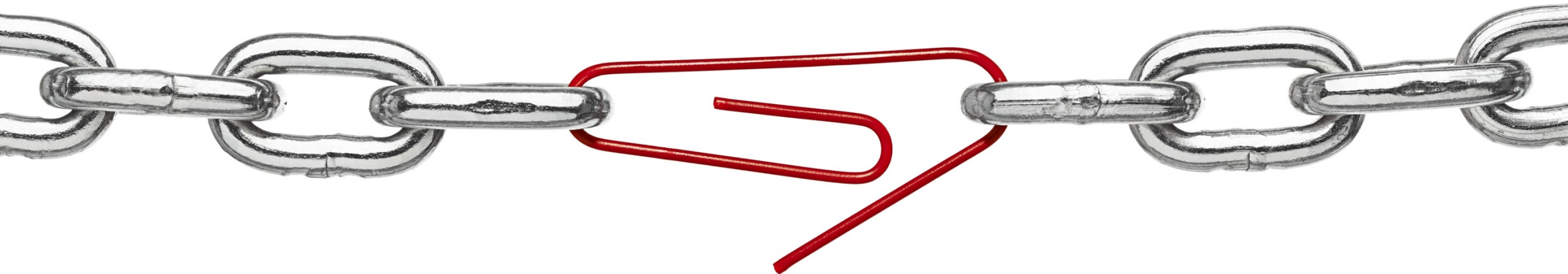
Many AVs lack sufficient

POLICIES

to require informed consent for
security-reducing apps

Our policy (ACR-007):

...Provides explicit notification to all affected parties and **obtains informed user consent** when reducing the default capability of, or moving away from certified versions of, security or safety.



Our call to action

To these AVs...	Summary	Our humble recommendation
Avira, K7, McAfee, Norton, Panda, Sophos	Well-aligned, even if policies are not public	Keep up the great work!
Avast, MalwareBytes	Slow to enforce (detect) existing policies/statements	Enforce your existing security-reducing policies/statements
AVG, BitDefender, ESET, GData, Kaspersky, Microsoft, Trend, Webroot	No policies, slow to detect security-reducing apps	Publish (then enforce) a security-reducing policy/statement for PUA or UwS

“Doesn’t obtain informed user consent, or provide explicit notification to all affected parties, when reducing the default capability of, or moving away from certified versions of, security or safety.”

A great start for your lawyers to consider...

Appendix

The security-reducing apps referenced in the deck

App Name	Version	SHA256 of Installer
VPN Proxy Master	3.11.0.0	9c6d24999f901aec499102e0198aa02000047e6c2da27a043565b88330f119ef
AdLock	2.1.2.3	82e5aa11c802ee31323d72d31a545ec9fafd005aca102ed9a8cad6c8a358bd27
Stereoscopic Player	2.5.1	cd08ac328d16f7b8eb32e09a091754b24c35d9581555c54c0e519c4defba7782
UrbanVPN	2.2.4	5188a0f304dac9935f8830a4c3411f4aeef306b344622801901c3e678e3003fb
StarVPN	1.1.18	d81da58a3544fcfaffae73d9247ecec0bb649e595acb537a6e74b5ab83e045c
8K Video Downloader	14.0	7f5a90b6ea65f0acfe5c0f73d7af0cdd284ae8fd8af3b050730404a493e6e493
KeyTurion Free Keylogger	6.9	d411a03ecdacff84decaa22278fc02e95182678abc73f509ca103dd7d342e936
Wolfeye Remote Screen	3.0	f26c14bfc640abf83b1d5de2a44a0f620e51a7d7786ce56a36906c4d5b9160ab
VIT Registry Fix	14.7.0	5ec159b395831834dc659591288b1b5b5278cb38828604816090204ea9a6acf6
Jcleaner	7.4.0.0	e1d734d527e1512c1eec0cf07d83de3e33e66d9bdba5f3bb6b3a6fd8805786b3



The AV policies/ statements we were able to find

AV	Type	Location
Avast/ AVG	Yes: Blog/ No	https://www.avast.com/c-what-is-pup https://www.avg.com/en/signal/what-is-a-pup
Avira	No	https://www.avira.com/en/potentially-unwanted-applications
BitDefender	Yes: Support	https://www.bitdefender.com/consumer/support/answer/26046/
ESET	No	https://support.eset.com/en/kb2629-what-is-a-potentially-unwanted-application-or-potentially-unwanted-content
GData	No	
K7	No	https://labs.k7computing.com/index.php/beware-of-root-certs-in-vpn/
Kaspersky	No	https://www.kaspersky.com/resource-center/definitions/what-is-pup-pua
MalwareBytes	Yes: Definition	https://www.malwarebytes.com/pup
McAfee	Yes: Policy	https://www.mcafee.com/enterprise/en-us/assets/legal/pup-policy.pdf
Microsoft	No	https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/criteria?view=o365-worldwide
Norton	No	https://us.norton.com/blog/malware/what-are-puas-potentially-unwanted-applications
Panda	Yes: Definition	https://www.pandasecurity.com/en/security-info/pup/
Sophos	Yes: Policy	https://www.sophos.com/en-us/medialibrary/PDFs/install%20guides/unwanted-software-criteria.pdf
Trend	No	https://www.trendmicro.com/vinfo/us/security/definition/potentially-unwanted-app
Webroot	No	https://answers.webroot.com/Webroot/ukp.aspx?pid=17&app=vw&vw=1&solutionid=1705&t=What-is-a-PUA

Presentation Abstract

Security-reducing apps: a call to action

As Avs get better operationalized in their fight against unwanted software (UwS), their combined pressure is driving the software monetization industry toward finding the gaps in AV policies so they can continue to exploit consumers for easy money.

The big gap in AV policies these days, unfortunately, is around apps that make their computers more vulnerable to attacks. The result? A proliferation of apps that needlessly reduce their customers' security postures and set them up for future attacks, without first obtaining informed user consent. Examples of these apps include VPNs that install self-signed trusted root certificates and free apps that monetize by installing proxies that share their internet connection and processor.

Lately these security-reducing apps that don't obtain informed consent are grabbing public attention: articles about them are popping up in both security blogs and computer industry news. Some platforms and AVs are beginning to respond – they detect after others have called them out. But the platforms and AVs have been slow to update their policies, and slow to detect these apps as UwS, which leaves a gap that software monetizers continue to exploit.

Our session will show examples of how these apps reduce their customers' security postures. We will highlight the platform and AV public policy gaps that have led to the spread of them. We'll make suggestions as to how Avs can enhance their policies to better protect their customers from these apps.

Questions?



AppEsteem[®]