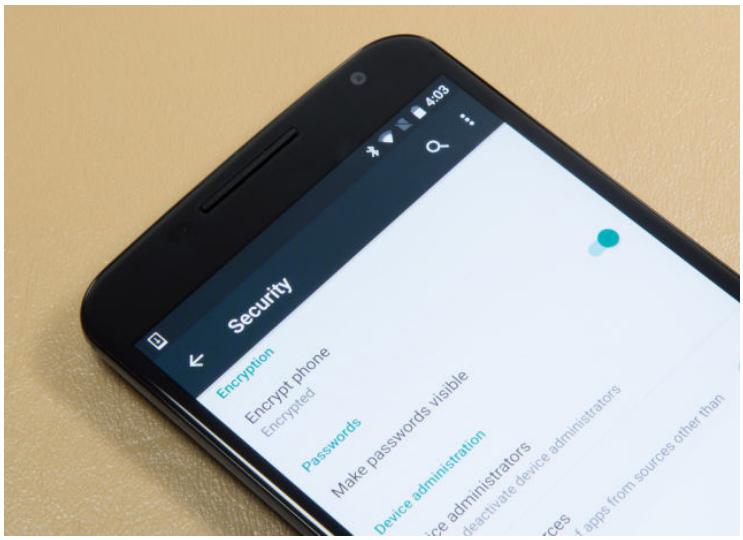
RISK ASSESSMENT —

Majority of Android VPNs can’t be trusted to make users more secure

Study of nearly 300 apps finds shocking omissions, including a failure to encrypt.

DAN GOODIN - 1/28/2017, 11:40 AM



Ron Amadeo

92

Over the past half-decade, a growing number of ordinary people have come to regard virtual private networking software as an essential protection against all-too-easy attacks that intercept sensitive

data or inject malicious code into incoming traffic. Now, a comprehensive study of almost 300 VPN apps downloaded by millions of Android users from Google's official Play Market finds that the vast majority of them can't be fully trusted. Some of them don't work at all.

FURTHER READING
The impossible task of creating a “Best VPNs” list today

According to a research paper that analyzed the source-code and network behavior of 283 VPN apps for Android:

- 18 percent didn't encrypt traffic at all, a failure that left users wide open to man-in-the-middle attacks when connected to Wi-Fi hotspots or other types of unsecured networks
- 16 percent injected code into users' Web traffic to accomplish a variety of objectives, such as image transcoding, which is often intended to make graphic files load more quickly. Two of the apps injected JavaScript code that delivered ads and tracked user behavior. JavaScript is a powerful programming language that can easily be used maliciously
- 84 percent leaked traffic

based on the next-generation IPv6 internet protocol, and 66 percent don't stop the spilling of domain name system-related data, again leaving that data vulnerable to monitoring or manipulation

- Of the 67 percent of VPN products that specifically listed enhanced privacy as a benefit, 75 percent of them used third-party tracking libraries to monitor users' online activities. 82 percent required user permissions to sensitive resources such as user accounts and text messages
- 38 percent contained code that was classified as malicious by VirusTotal, a Google-owned service that aggregates the scanning capabilities of more than 100 antivirus tools
- Four of the apps installed digital certificates that caused the apps to intercept and decrypt transport layer security traffic sent between the phones and encrypted websites

The

VPN app	CA	User-warning	# Installs
Packet Capture [38]	Packet Capture	GUI	100K
DashVPN [10]	ActMobile		100K
DashNet [9]	ActMobile		10K
Exalinks Neopard [30]	Exalinks Root	Privacy Policy	10K

Enlarge / **Apps that intercepted and decrypted TLS traffic.**

researchers—from Australia's Commonwealth Scientific and

Industrial Research Organization, the University of New South Wales, and the University of California at Berkeley—wrote in their report:

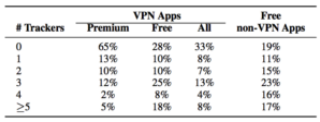
> Our results show that—in spite of the promises for privacy, security, and anonymity given by the majority of VPN apps—millions of users may be unawarely subject to poor security guarantees and abusive practices inflicted by VPN apps... Despite the fact that Android VPN-enabled apps are being installed by millions of mobile users worldwide, their operational transparency and their possible impact on user's privacy and security remains *terra incognita* even for tech-savvy users.

Protocol		Free Apps	Premium Apps
OpenVPN		14%	20%
L2TP/IPSec		5%	0%
SOCKS		4%	0%
Unidentified	UDP:80	0%	10%
	TLS (TCP:443)	15%	10%
	DTLS (UDP:443)	13%	25%
	Other ports	30%	25%
Unencrypted		19%	10%

Enlarge / **Apps that failed to encrypt.**

Not every behavior called out in the report is an automatic indication of a privacy or security failing. A variety of VPNs have been called out in the past for leaking IPv6 and DNS traffic. In some cases, the shortcomings may compromise

only anonymity, rather than allowing attackers to monitor or manipulate traffic to and from a phone. Still, most security and privacy experts agree that at a minimum, the behaviors found in the study are things that should be avoided by VPN developers.



# Trackers	VPN Apps			Free non-VPN Apps
	Premium	Free	All	
0	65%	28%	33%	19%
1	13%	10%	8%	11%
2	10%	10%	7%	15%
3	12%	25%	13%	23%
4	2%	8%	4%	16%
≥5	5%	18%	8%	17%

Enlarge / VPNs with trackers

One of the few apps to be lauded in the study was F-Secure Freedome VPN, made by the Finnish security company F-Secure. In keeping with F-Secure marketing promises, the app blocks all traffic from a pre-defined list of Web- and mobile-tracking domains, including Google Ads, DoubleClick, Google Tag, and comScore. The researchers found at least one site, nytimes.com, where Freedome interfered with embedded content video because the app blocked some of the JavaScript served by the domain. Other than that, one of the researchers told Ars, Freedome had no issues. App licenses cost $50 per year for use on three devices which, in addition to Android, can run Windows, MacOS, or iOS.

The research was based on Google Play apps that, as of November, used a permission called

#	App ID	Class	Rating	# Installs	AV-rank
1	OkVpn [34]	Prem.	4.2	1K	24
2	EasyVpn [15]	Prem.	4.0	50K	22
3	SuperVPN [52]	Free	3.9	10K	13
4	Betternet [19]	Free	4.3	5M	13
5	CrossVpn [7]	Free	4.2	100K	11
6	Archie VPN [4]	Free	4.3	10K	10
7	HarVPN [21]	Free	4.0	5K	10
8	sFly Network Booster [47]	Prem.	4.3	1K	10
9	One Click VPN [35]	Free	4.3	1M	6
10	Fast Secure Payment [17]	Prem.	4.1	5K	5

Enlarge / **VPNs with a malware presence as indicated by VirusTotal**

BIND_VPN_SERVICE, which allows apps to intercept and take full control of all traffic flowing over an affected phone or tablet. The results don't take into account apps that have been added, removed, or modified since then. Still, however the Google Play offerings have changed in the past two months, the findings should serve as a wakeup call for anyone using a VPN app on an Android device. Those relying on an app that isn't Freedome should consider dumping it or at least suspending use of it until they have reviewed the app's performance.

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL
dan.goodin@arstechnica.com
// **TWITTER** @dangoodin001

READER COMMENTS 92 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS