

[itworldcanada.com](https://www.itworldcanada.com)

# Understanding Android Malware Families: Riskware – is it worth it? (Article 4) | IT World Canada Blog

*Gurdip Kaur and Arash Habibi Lashkari*

9-12 minutes

---

Riskware is defined as a legitimate program that presents potential risks to the security vulnerabilities on a device. Although it is a legitimate program, bad actors use Riskware to steal information from the device and redirect users to malicious websites or perform functions at the expense of device security.

Typically, Riskware is associated with attackers who hijack devices, gain unauthorized access to devices, collect sensitive information, and disrupt services with the intent to steal information for misuse.

These vulnerabilities can pose legal risks and infringements. This article reveals prominent Android families and provides in-depth insights into the functions, activities and communication processes used by attackers. Readers will gain insights into the dangers and indicators of when a smartphone has been infected by riskware. In addition, the article delves deeper into technical features that can detect riskware on a smartphone. Finally, some preventive measures to protect the device from high-risk goods families are presented.

The technical details in this article stem from our public Android malware dataset called CCCS-CIC-AndMal-2020, published by the Canadian Institute for Cybersecurity CIC in collaboration with Canadian Centre for Cyber Security CCCS.

## Activities and behaviour of riskware families

This section describes the relevant features of Riskware families. Figure 1 presents twenty-one Riskware families that we analyzed for this article. The most popular Riskware families include mobilepay, metasploit, revmob, smspay, smsreg, and talkw.


Riskware		
anydown	metasploit	smsreg
badpac	nqshield	talkw
deng	remotecode	tencentprotect
dnotua	revmob	tordow
jiagu	secneo	triada
kingroot	skymobi	wapron
mobilepay	smspays	wificrack

Figure 1: Riskware Families

Riskware families collect personal and phone information, send/receive SMSs, steal network information, connect to malicious websites, install malicious content on devices, show malicious advertisements, and modify system settings and files on the compromised device. The following observations are derived from Table 1:

Table 1: Activities performed by Riskware families:

Malware Family	Data	Media	Hardware	Actions	Internet	C&C	Anti-virus	Stor
AnyDown					I2, I4			
BadPac			H1, H2		I1, I3			☒
Deng	D1		H1, H2	A1	I2			
Dnotua				A1	I1, I3		☒	☒
Jiagu							☒	☒
Kingroot	D1,		H1, H3	A1	I3			

	D5							
MobilePay	D2				I3, I4			
Metasploit				A1				
Nqshield	D3				I4			
RemoteCode					I3			
RevMob	D1		H1		I1, I2, I3, I4			
Secneo	D2, D5	M1, M2	H1, H2	A3	I1, I3			
SkyMobi	D1		H1		I3			
SmsPay	D5				I4			
SmsReg	D5		H1, H2		I1, I4			
Talkw					I2, I4			
TenCentProtect			H1		I1, I3			
Tordow	D2, D5	M1		A2, A3	I3			
Triada	D5		H1	A1				
Wapron	D1, D4				I2, I4			
WiFiCrack			H2		I1			

<p>D1: Collect personal information (phone number, email address, app accounts) and browser history</p> <p>D2: Collect user contacts</p> <p>D3: Send / receive spam emails</p> <p>D4: Steal banking credentials</p> <p>D5: Send / receive SMS</p>	<p>H2: Get location (GPS)</p> <p>H3: Lock phone or change PIN</p> <p>A1: Ask for root privileges</p> <p>A2: Block / delete / use phone apps</p> <p>A3: Execute after phone reboot</p> <p>I1: Steal network information (WiFi, II</p>
---	--