MOBILE MALWARE AND APT ESPIONAGE

A VIRULENT THREAT

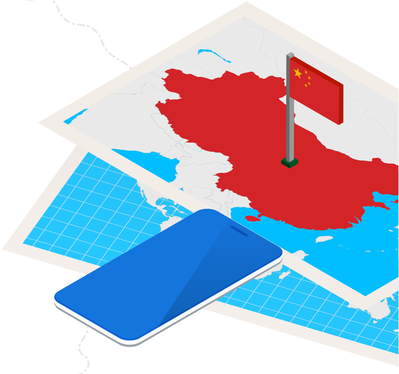
BlackBerry's seminal Mobile Malware Report examines how Advanced Persistent Threat (APT) groups have been leveraging malicious code targeting Android™ and iOS® devices in combination with traditional desktop malware in ongoing surveillance and espionage campaigns.

1 YEAR MINIMUM
time an APT group was conducting mobile malware operations before being identified in 2015

Vietnam's OCEANLOTUS has been conducting mobile malware operations since at least early 2014, pre-dating the identification of the group by a year. A new OCEANLOTUS campaign BlackBerry researchers identified has both a desktop dimension and a new mobile malware family that was propagated via fake apps available in well-known app stores.

2 NEW STATE-SPONSORED APT GROUPS identified in the BlackBerry Mobile Malware Report

A newly identified Chinese APT named BBCY-TA2 by BlackBerry researchers utilized a new Windows malware family dubbed PWNWIN1. Along with another new Chinese APT group named BBCY-TA3, these threat actors engaged in economic espionage against Western and South Asian telecom companies and nearly every large chemical company outside of China.

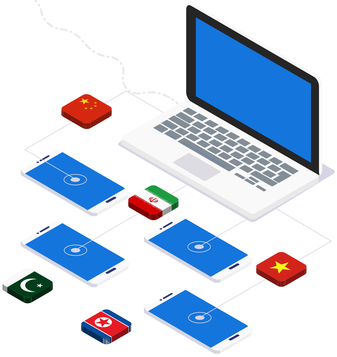


$2,500,000
cost for a zero-click exploit targeting the Android mobile operating system

The going rate for zero-click exploits for the Android operating system hit $2.5 million dollars in 2019, while zero-click iPhone exploits cost about $1 million dollars (Greenberg, 2019)*. The prices reflect the value of vulnerable data and low threat detection rates on mobile devices. The scale of mobile malware in-use by APT groups that BlackBerry researchers observed shows that mobile and traditional desktop malware are both core tactics of APTs.

4 NEWLY IDENTIFIED ESPIONAGE CAMPAIGNS in the BlackBerry Mobile Malware Report

- OPERATION DUALCRYPTOEX uses new malware families that target both Android and Windows® by a newly identified Chinese APT.
- OPERATION OCEANMOBILE by APT group OCEANLOTUS delivered malware via a sophisticated trio of fake mobile apps.
- OPERATION DUALPAK by APT group BITTER targeted Pakistani military with a new mobile malware family distributed via fake apps, SMS, WhatsApp® and other social media platforms.
- OPERATION DUALPAK2 by APT group CONFUCIUS targeted Pakistani government and military with a new Windows malware family distributed via JavaScript version of a chat app.



5,000 MALICIOUS APPS
installed on Android phones over 1.5 years via Google Play

BlackBerry researchers discovered that OCEANLOTUS established a false backstory to give its malicious apps legitimacy and created fake GitHub repositories to show evidence of the developers' code, complete with "contact us" email addresses and customer support for their "products." Such social engineering tactics were common in numerous APT mobile and desktop malware campaigns in the Mobile Malware Report.

CylancePROTECT® for mobile devices provides automated threat detection and continuously prevents malware infections, URL phishing attacks and application integrity without disrupting end-users, leveraging the best of zero trust architectures. **Learn more at BlackBerry.com**

*Greenberg, A. (2019, September 3). Why 'Zero Day' Android Hacking Now Costs More Than iOS Attacks. Retrieved from WIRED: https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/