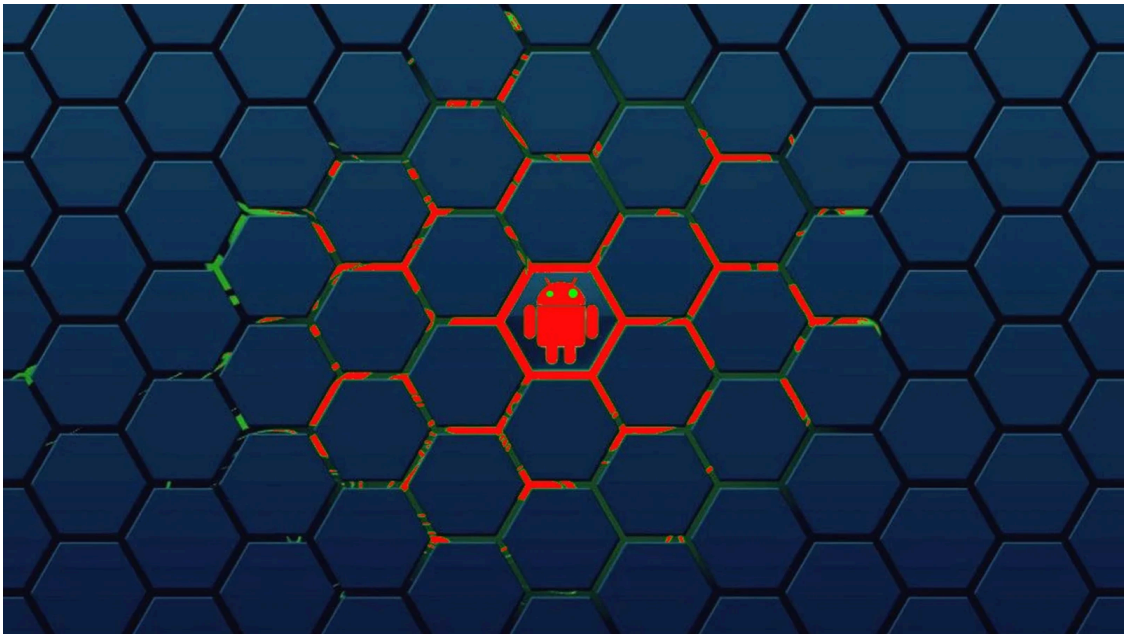
SpyNote Android malware infections surge after source code leak

By Bill Toulas

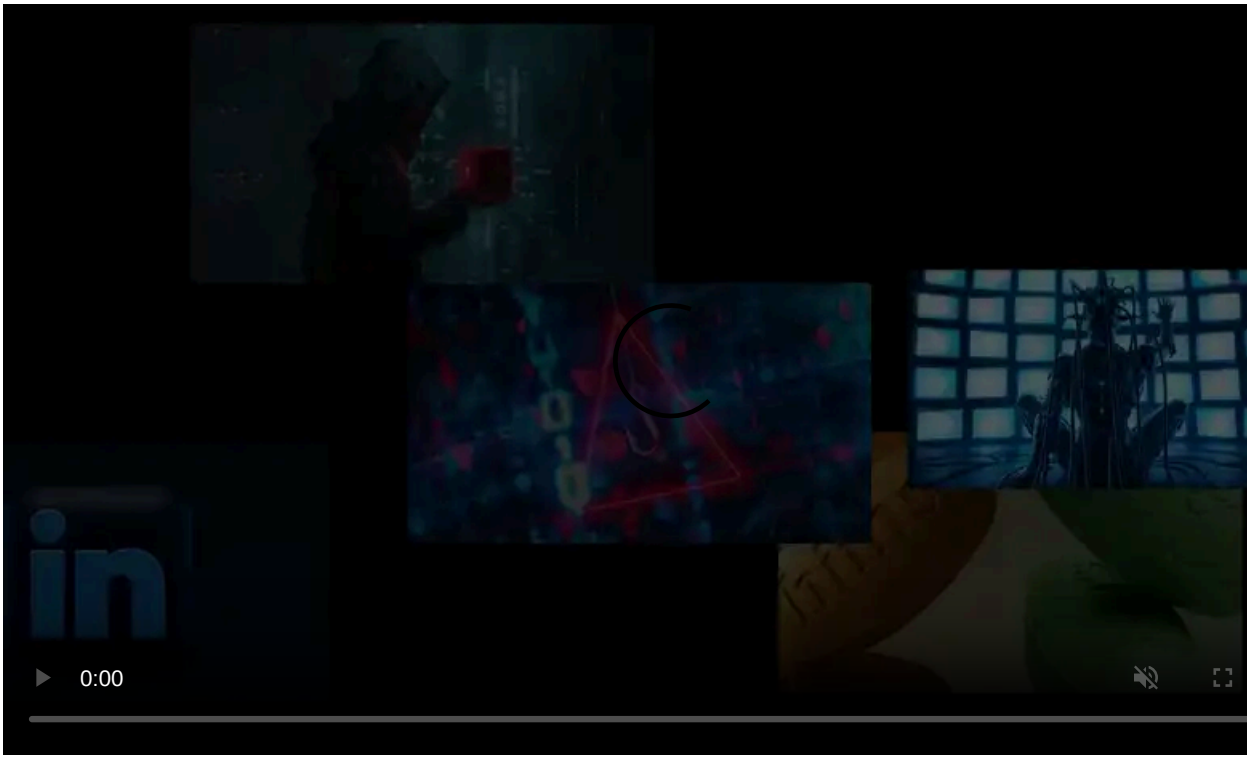
Published: 2023-01-05 · Archived: 2026-04-05 16:09:57 UTC

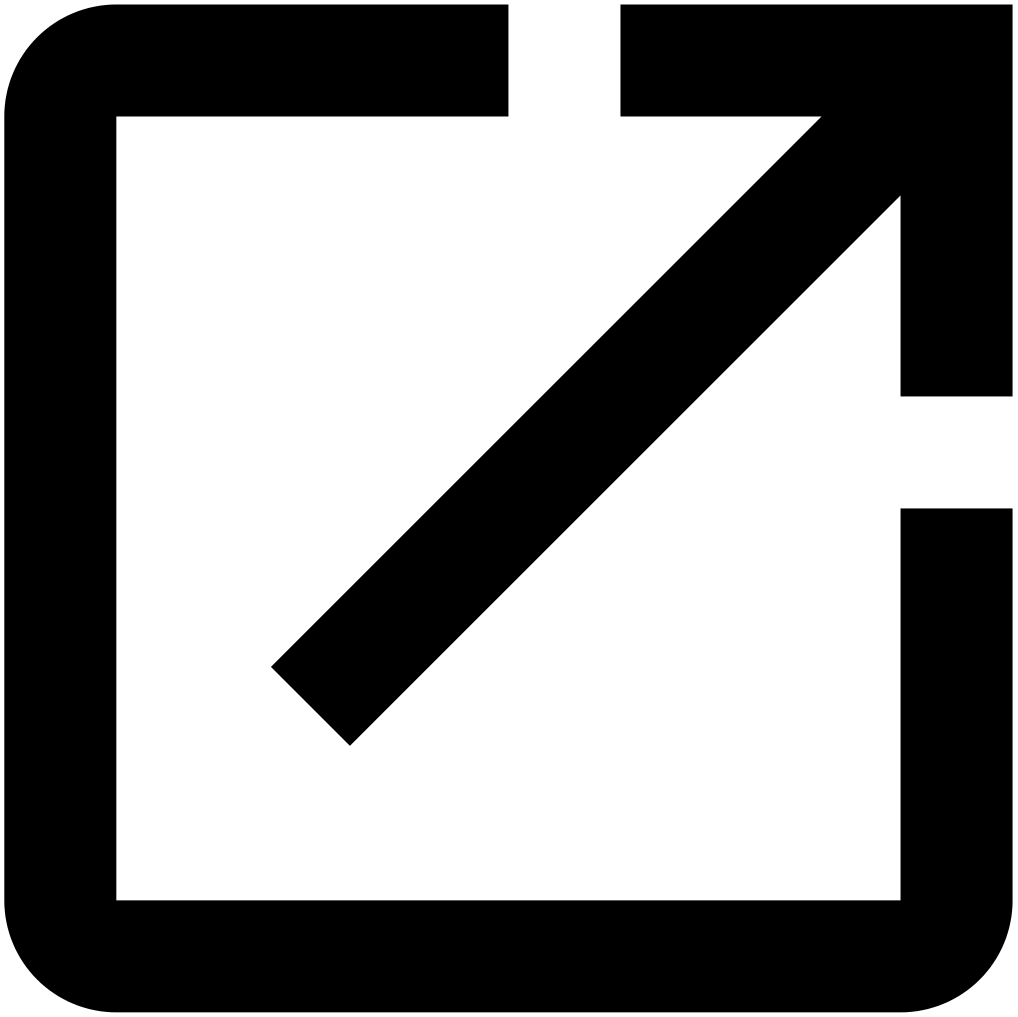


The Android malware family tracked as SpyNote (or SpyMax) has had a sudden increase in detections in the final quarter of 2022, which is attributed to a source code leak of one of its latest variants, known as 'CypherRat.'

'CypherRat' combined SpyNote's spying capabilities, such as offering remote access, GPS tracking, and device status and activity updates, with banking trojan features that impersonate banking institutions to steal account credentials.

CypherRat was sold via private Telegram channels from August 2021 until October 2022, when its author decided to publish its source code on GitHub, following a string of scamming incidents on hacking forums that impersonated the project.


0:00



Threat actors quickly snatched the malware's source code and launched their own campaigns. Almost immediately, custom variants appeared that targeted reputable banks like HSBC and Deutsche Bank.

Icon / App name / Package name	Malware family	Malware variant	Malware types
HSBC UK Mobile Banking (com.employ.mb) 6f606bc5004af2b90b66d6e6e4f29f35a3b4a31dc6974b55434b3c53d70584a4	SpyNote	SpyNote.C	
Deutsche Bank Mobile (com.reporting.efficiency) 114fa822d7a96169c9cd48303f7fbd1af94f57cb46fec576d91ccea11bc5d974	SpyNote	SpyNote.C	
BurlaNubank (com.appser.verapp) 34d70ce1e9eeafdc225abbfa84c24454986a47ca7a41431c38ca16e612d3f818	SpyNote	SpyNote.C	
IMTYBANK (com.resources.installations) 97884c2b74ccffebdc91a439c4316c3215d0eb571a17820ce7da77355f21878c	SpyNote	SpyNote.C	
Kotak Bank (splash.app.main) bd172dbb47a95e7abc3ce76118bf6cd3f742d7c932ec8801cd553509f31eca8e	SpyNote	SpyNote.C	

Some of the banks targeted by SpyNote *(ThreatFabric)*

In parallel, other actors opted to masquerade their versions of CypherRat as Google Play, WhatsApp, and Facebook, targeting a wider audience.

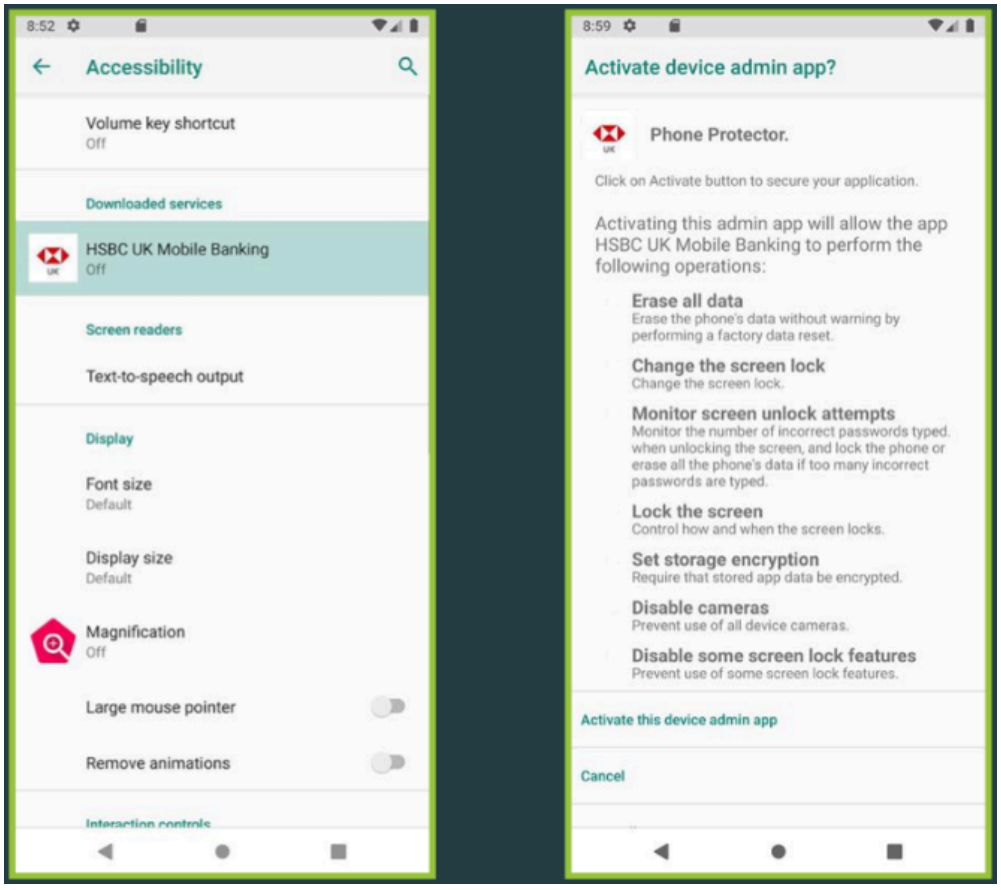
Icon / App name / Package name	Malware family	Malware variant	Malware types
Play Store (com.warned.moon) 7f3b84a0fa394b66422fddf729d7f9ba3000f4dcdcd61eb394005462264595fb	SpyNote	SpyNote.C	RAT Spyware
Sistem Bildirimleri (com.marble.physicians) 08463529d7d681246a0dd1d24a59fa50d354568f04673642bb44cc613a824be9	SpyNote	SpyNote.C	RAT Spyware
CypherRat (splash.app.main) 0dcd025c20d7f5e4b503d40034b5d4b8cf2661df235bcfc7f6e672307650a62f	SpyNote	SpyNote.C	RAT Spyware
Google Play Protect (cmf0.c3b5bm90zq.patch) 71ec22035d5499a89dad13911cc84d17c9021ba40f241702c31dce443ee3d8c4	SpyNote	SpyNote.A	Spyware

Impersonated applications *(ThreatFabric)*

This activity was observed by ThreatFabric analysts, who warn about the possibility of CypherRat becoming an even more widespread threat.

SpyNote malware features

All SpyNote variants in circulation rely on requesting access to Android's Accessibility Service to be allowed to install new apps, intercept SMS messages (for 2FA bypass), snoop on calls, and record video and audio on the device.



Malicious app requesting access to Accessibility Service *(ThreatFabric)*

ThreatFabric lists the following as "standout" features:

- Use the Camera API to record and send videos from the device to the C2 server
- GPS and network location tracking information
- Stealing Facebook and Google account credentials.
- Use Accessibility (A11y) to extract codes from Google Authenticator.
- Use keylogging powered by Accessibility services to steal banking credentials.

To hide its malicious code from scrutiny, the latest versions of SpyNote employ string obfuscation and use commercial packers to wrap the APKs.

Moreover, all information exfiltrated from SpyNote to its C2 server is obfuscated using base64 to hide the host.

Threat actors currently use CypherRat as a banking trojan, but the malware could also be used as spyware in low-volume targeted espionage operations.

ThreatFabric believes that SpyNote will continue to constitute a risk for Android users and estimates that various forks of the malware will appear as we head deeper into 2023.

While ThreatFabric has not shared how these malicious apps are being distributed, they are likely spread through phishing sites, third-party Android app sites, and social media.

For this reason, users are advised to be very cautious during the installation of new apps, especially if those come from outside Google Play, and reject requests to grant permissions to access the Accessibility Service.

Unfortunately, despite Google's continual efforts to stop the abuse of Accessibility Service APIs by Android malware, there are still ways to bypass the imposed restrictions.

Update 1/6/23 - A Google spokesperson has sent BleepingComputer the following comment:

> Google Play Protect checks Android devices with Google Play Services for potentially harmful apps from other sources. Users are protected by Google Play Protect, which can warn users or block identified malicious apps on Android devices

---

Source: https://www.bleepingcomputer.com/news/security/spynote-android-malware-infections-surge-after-source-code-leak/