



“Operation C-Major” Actors Also Used Android, BlackBerry Mobile Spyware Against Targets

- Posted on:April 18, 2016 at 7:07 am
- Posted in:Malware, Mobile, Targeted Attacks
- Author:
  Trend Micro

By Shawn Xing, David Sancho, and Feike Hacquebord

Last March, we reported on Operation C-Major, an active information theft campaign that was able to steal sensitive information from high profile targets in India. The campaign was able to steal large amounts of data despite using relatively simple malware because it used clever social engineering tactics against its targets. In this post, we will focus on the mobile part of their operation and discuss in detail several Android and BlackBerry apps they are using. Based on our investigation, the actors behind Operation C-Major were able to keep their Android malware on Google Play for months and they advertised their apps on Facebook pages which have thousands of likes from high profile targets.

Link to StealthGenie

Several actors involved in Operation C-Major have been rather careless in the past, leaving behind numerous digital traces on the Internet. One of these actors has been actively promoting StealthGenie, a spying app for Android, BlackBerry, and iPhone. This app was marketed as a tool one can use to monitor employees, spouses, and children. However, based on its functionalities, it is no different from malicious applications. The Pakistani owner of StealthGenie got arrested by the Federal Bureau of Investigation (FBI) in 2014 for selling spyware and was fined US$500,000.

For the C-Major actor, it was only a small step to go from promoting StealthGenie to using APT malware that was designed to spy on the armed forces of a nation. In 2013, Operation C-Major used spying apps for BlackBerry phones, which have similar functions to that of StealthGenie's. It was apparent that these apps were developed not for jealous spouses but for the threat actors' intent on stealing sensitive information from organizations like the armed forces.

More malicious apps

Since at least early 2013, actors behind Operation C-Major have been using a variety of malicious apps against high-profile targets in the Indian military, as well as other foreign embassies. From our research, we saw that these apps were downloaded by the hundreds, most likely by the targets in India. Some of these apps, like fake news apps, are promoted on "official" Facebook pages, which is another social engineering trick to lure users into downloading them. Most of these apps are developed by a Pakistani company.

Here is a rundown of what they used during the operation and how each of them functions:

Ringster

This spyware collects the contact list of the targets and it can take screenshots of the targets' phones. It

was available on Google Play in the first half of 2015 before it was removed.

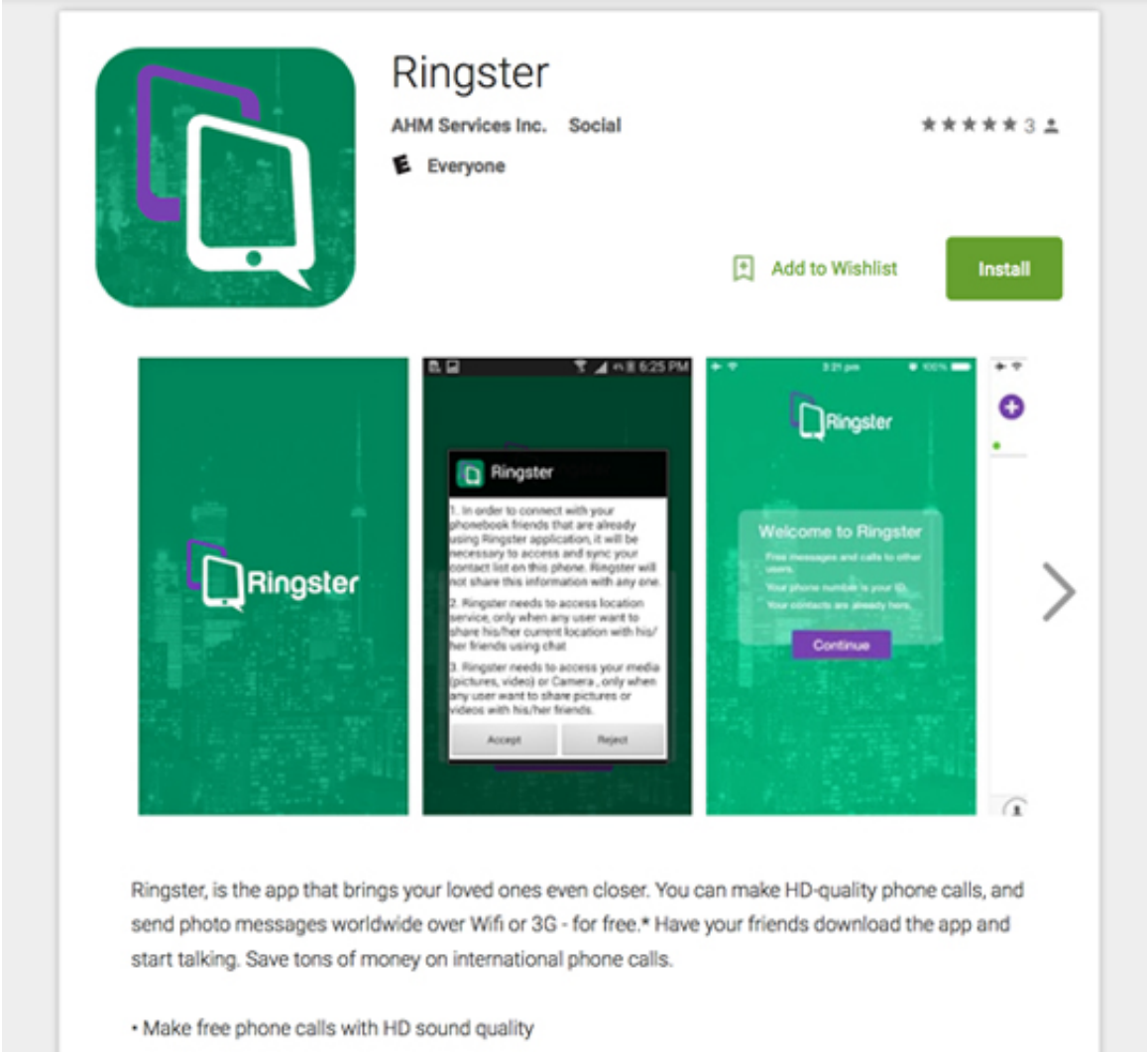

Figure 1. Ringster appealing as a social messaging service provider

Our code analysis reveals that Ringster is reusing a lot of code from Wavecall, a communication tool developed by a company called Yello. Ringster has a hardcoded URL pointing to *mpjunkie[.]com*. This URL makes a clear connection to the other campaigns of Operation C-Major, which we described in our previous post.

SmeshApp

SmeshApp is similar to Ringster but is more powerful. Smesh can steal SMS messages, record videos and calls, and send screenshots. Smesh App was available on Google Play from June 2015 till March of 2016, and has been downloaded hundreds of times before it was pulled. This shows that Operation C-Major used relatively basic malware that remained unnoticed on the Google Play store for a large time window.

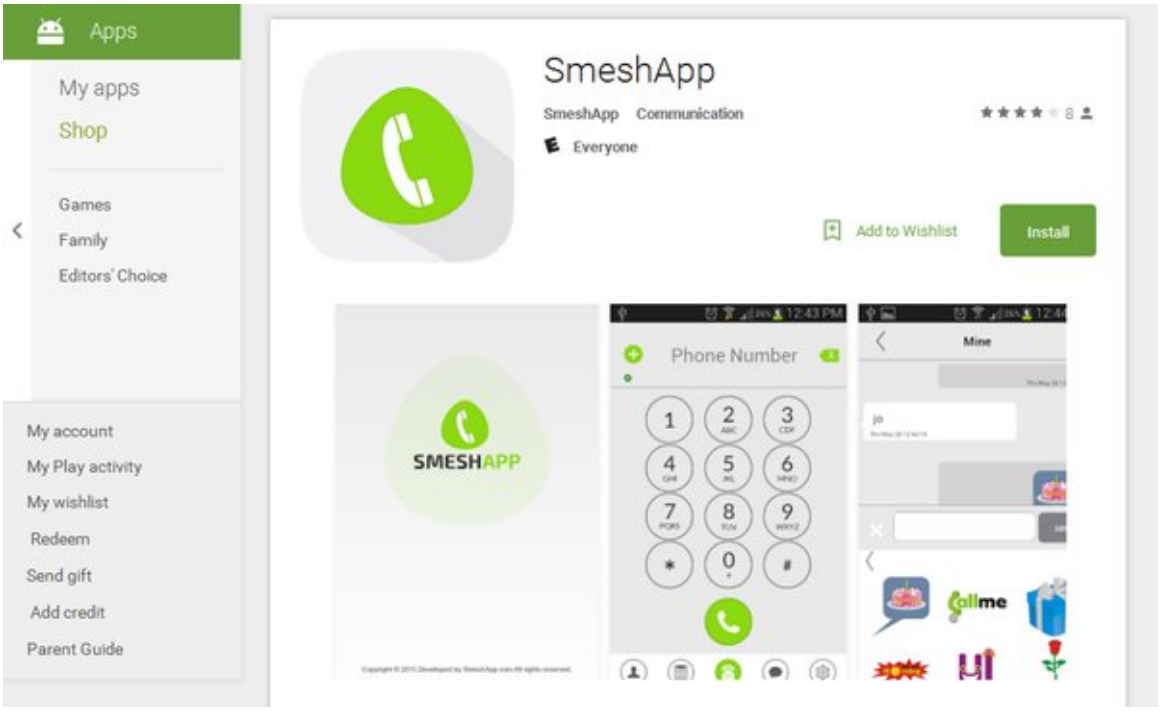

Figure 2. SmeshApp download

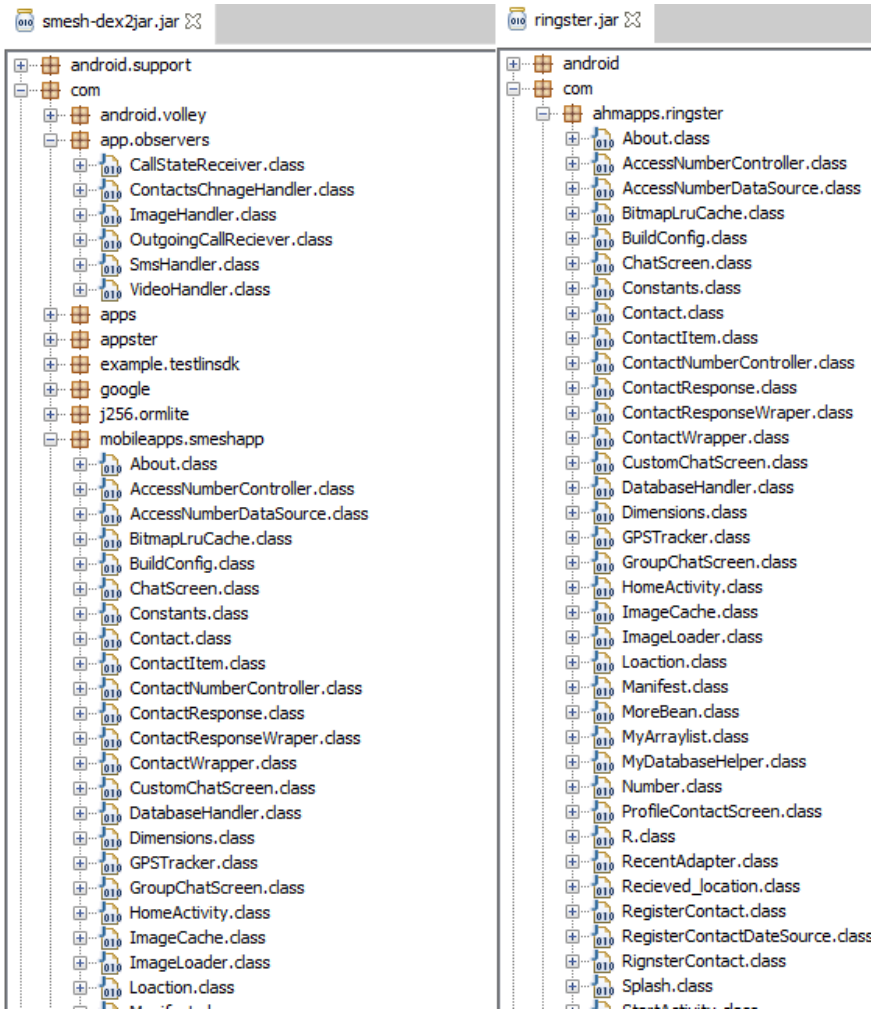

Figure 3. Code comparison between SmeshApp and Ringster

Androrat

Since at least 2015, Operation C-Major started to use Androrat, an off-the-shelf remote administration tool for Android. C-Major may have bought Androrat from an Indonesian vendor. The C&C infrastructure of the Androrat samples overlaps with the infrastructure that is used in other campaigns of C-Major which we described in our previous blog post.

Indian Sena News and India Defense News Apps

Three fake news apps, Indian Sena News, Bharatiya Sena News and India Defense News (IDN) were advertised on Facebook. Prior to being closed, the IDN news Facebook page had more than 1,200 likes from Facebook members that have some relation to the India army. Likewise, the Bharatiya Sena News page had 3,300 page likes. These apps are capable of stealing SMS, making videos, recording calls, sending screenshots, and stealing files.

Figure 4. Facebook page of the fake India Defense News app

Figure 5. Facebook page of the fake Bharatiya Sena News app

Figure 6. Screenshot of Indian Sena News app

Figure 7. Screenshot of IDN news app

BlackBerry malware

It is no surprise that the actors behind C-Major also used BlackBerry malware in their operation. BlackBerry in general has been used a lot by government agencies, probably including the Indian military. As mentioned earlier, the sample we found is spyware for BlackBerry that has similar to StealthGenie’s capabilities. It can exfiltrate GPS location, email address, emails, contacts, calendar data, device identifiers, and user’s stored photos. The application also has the ability to intercept email, phone calls, MMS, and SMS messages.

As far as we know, the BlackBerry malware was never available on BlackBerry World. Most likely social engineering would be needed to get the malware installed on victims’ phones.

Conclusion

Though the C-Major operators don’t seem to have advanced skills, the damage they potentially have caused is significant. Often their C&C servers live for more than a year and in some cases even several years. They manage to keep malicious apps on Google Play for months and steal significant data from high profile targets before the apps are flagged and removed. As we have previously noted, although C-

Major didn't use advanced malware or exploits, there is no reason why they wouldn't continue to develop themselves to more skilled attackers in the future. With this in mind, we will follow their future activities closely.

Trend Micro™ Mobile Security protects users' Android devices and stops threats before they reach them. Trend Micro Mobile Security offers protection and detects these malware using the cloud-based Smart Protection Network™ and Mobile App Reputation technology.

SHA1s for related files:

Smesh app

- 24f52c5f909d79a70e6e2a4e89aa7816b5f24aec
- 202f11c5cf2b9df8bf8ab766a33cd0e6d7a5161a
- 31ac19091fd5347568b130d7150ed867ffe38c28
- 6919aa3a9d5e193a1d48e05e7bf320d795923ea7
- c48a5d639430e08980f1aeb5af49310692f2701b
- 1ce6b3f02fe2e4ee201bdab2c1e4f6bb5a8da1b1
- 59aec5002684de8cc8c27f7512ed70c094e4bd20
- 552e3a16dd36ae4a3d4480182124a3f6701911f2

Ringster

- c544e5d8c6f38bb199283f11f799da8f3bb3807f
- a13568164c0a8f50d76d9ffa6e34e31674a3afc8

Androrat

- 9288811c9747d151eab4ec708b368fc6cc4e2cb5
- 94c74a9e5d1aab18f51487e4e47e5995b7252c4b
- decf429be7d469292827c3b873f7e61076ffbba1
- f86302da2d38bf60f1ea9549b2e21a34fe655b33

India Sena News

- b142e4b75a4562cdaad5cc2610d31594d2ed17c3

BlackBerry spyware

- abcb176578df44c2be7173b318abe704963052b2
- 16318c4e4f94a5c4018b05955975771637b306b4

Related Posts:

- **Indian Military Personnel Targeted by “Operation C-Major” Information Theft Campaign**
- **German Users Hit By Dirty Mobile Banking Malware Posing As PayPal App**

Tags: bogus appsOperation C-majortargeted attack campaign

Featured Stories

- The Panamanian Shell Game: Cybercriminals With Offshore Bank Accounts?
- Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations
- Crypto-ransomware Gains Footing in Corporate Grounds, Gets Nastier for End Users
- SpyEye Creator Sentenced to 9 Years in Federal Prison
- Indian Military Personnel Targeted by “Operation C-Major” Information Theft Campaign

Recent Posts

- Kernel Waiter Exploit from the Hacking Team Leak Still Being Used
- Flashlight App Spews Malicious Ads
- New Flash Vulnerability CVE-2016-4117 Shares Similarities With Older Pawn Storm Exploit
- Chinese-language Ransomware Makes An Appearance
- Pawn Storm Targets German Christian Democratic Union

Cybercrime Across the Globe: What Makes Each Market Unique?

- This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

Popular Posts

Data Protection Mishap Leaves 55M Philippine Voters at Risk
New Crypto-Ransomware JIGSAW Plays Nasty Games
Locky Ransomware Spreads via Flash and Windows Kernel Exploits
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD

Latest Tweets

Error: Rate limit exceeded

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |

- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies