Malware on Google Play Targets North Korean Defectors

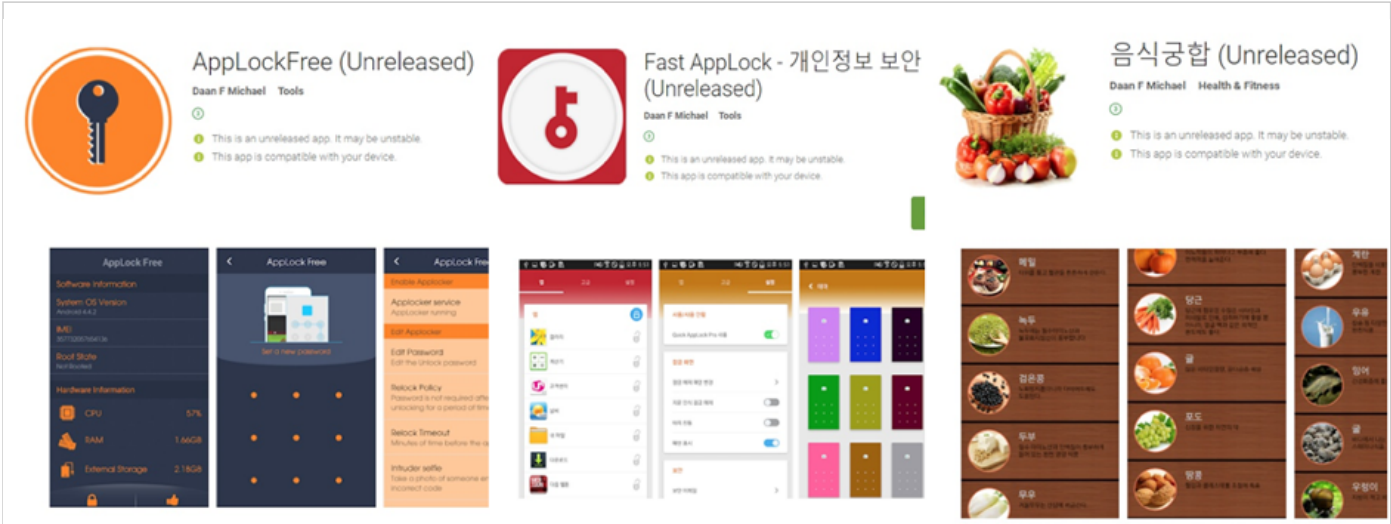
By Jaewon Min (https://securingtomorrow.mcafee.com/author/jaewon-min/) on May 17, 2018 (https://securingtomorrow.mcafee.com/2018/05/)

Earlier this year, McAfee researchers predicted in the *McAfee Mobile Threat Report* (https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2018.pdf) that we expect the number of targeted attacks on mobile devices to increase due to their ubiquitous growth combined with the sophisticated tactics used by malware authors. Last year we posted the first public blog (https://securingtomorrow.mcafee.com/mcafee-labs/android-malware-appears-linked-to-lazarus-cybercrime-group/) about the Lazarus group operating in the mobile landscape. Our recent discovery of the campaign we have named RedDawn on Google Play just a few weeks after the release of our report proves that targeted attacks on mobile devices are here to stay.

RedDawn is the second campaign we have seen this year from the "Sun Team" hacking group. In January, the McAfee Mobile Research Team wrote about (https://securingtomorrow.mcafee.com/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/) Android malware targeting North Korean defectors and journalists. McAfee researchers recently found new malware developed by the same actors that was uploaded on Google Play as "unreleased" versions. We notified both Google, which has removed the malware from Google Play, and the Korea Internet & Security Agency.

Our findings indicate that the Sun Team is still actively trying to implant spyware on Korean victims' devices. (The number of North Korean defectors who came to South Korea exceeded 30,000 in 2016, according to Radio Free Asia (https://www.rfa.org/korean/in_focus/human_rights_defector/defectors-11142016073628.html).) Once the malware is installed, it copies sensitive information including personal photos, contacts, and SMS messages and sends them to the threat actors. We have seen no public reports of infections. We identified these malwares at an early stage; the number of infections is quite low compared with previous campaigns, about 100 infections from Google Play.

Malware on Google Play

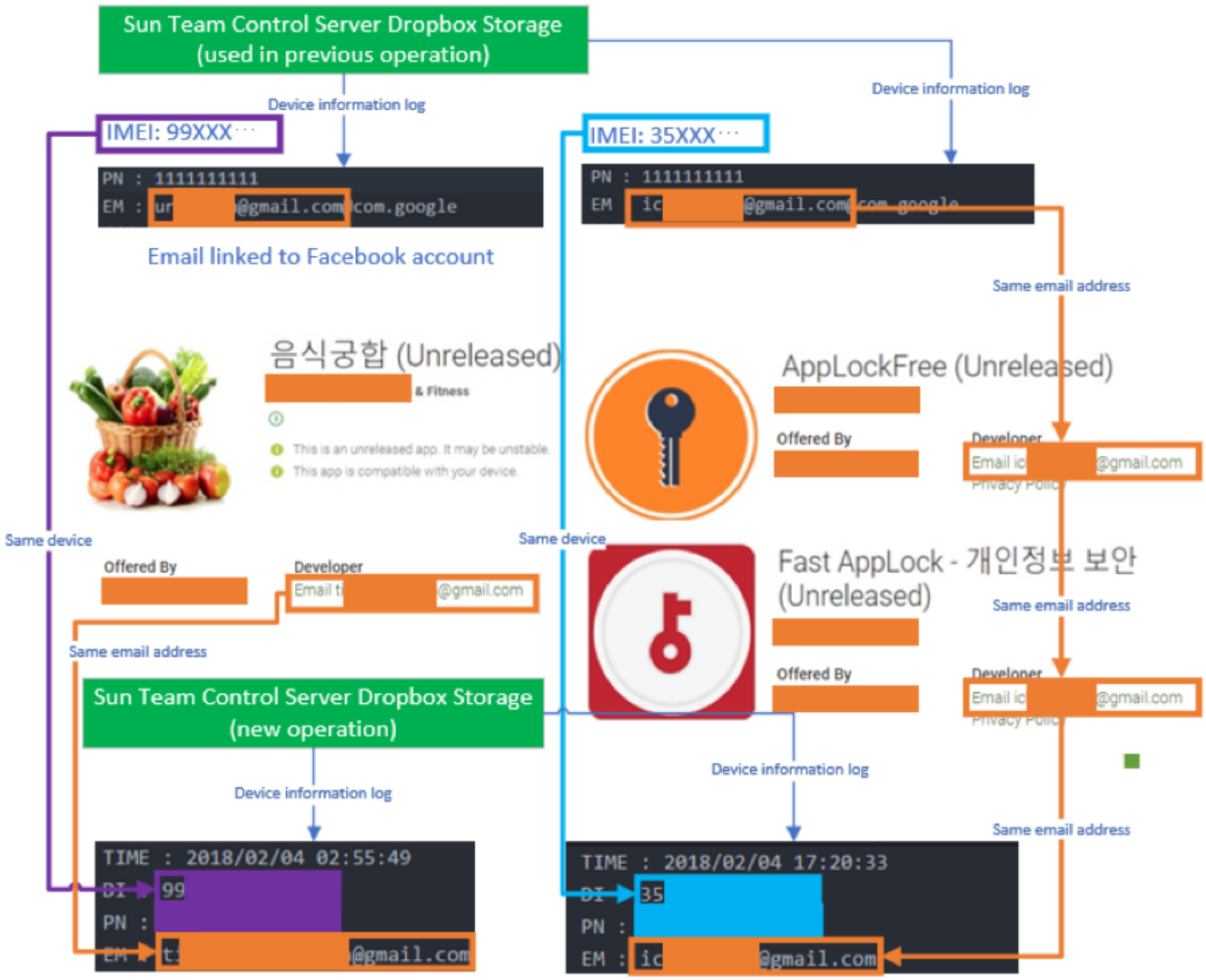


Malware uploaded on Google Play (now deleted).

We found three apps uploaded by the actor we named Sun Team, based on email accounts and Android devices used in the previous attack. The first app in this attack, 음식궁합 (Food Ingredients Info), offers information about food; the other two apps, Fast AppLock and AppLockFree, are security related. 음식궁합 and Fast AppLock secretly steal device information and receive commands and additional executable (.dex) files from a cloud control server. We believe that these apps are multi-staged, with several components. AppLockFree is part of the reconnaissance stage we believe, setting the foundation for the next stage unlike the other two apps. The malwares were spread to friends, asking them to install the apps and offer feedback via a Facebook account with a fake profile promoted 음식궁합.

Links to Previous Operations

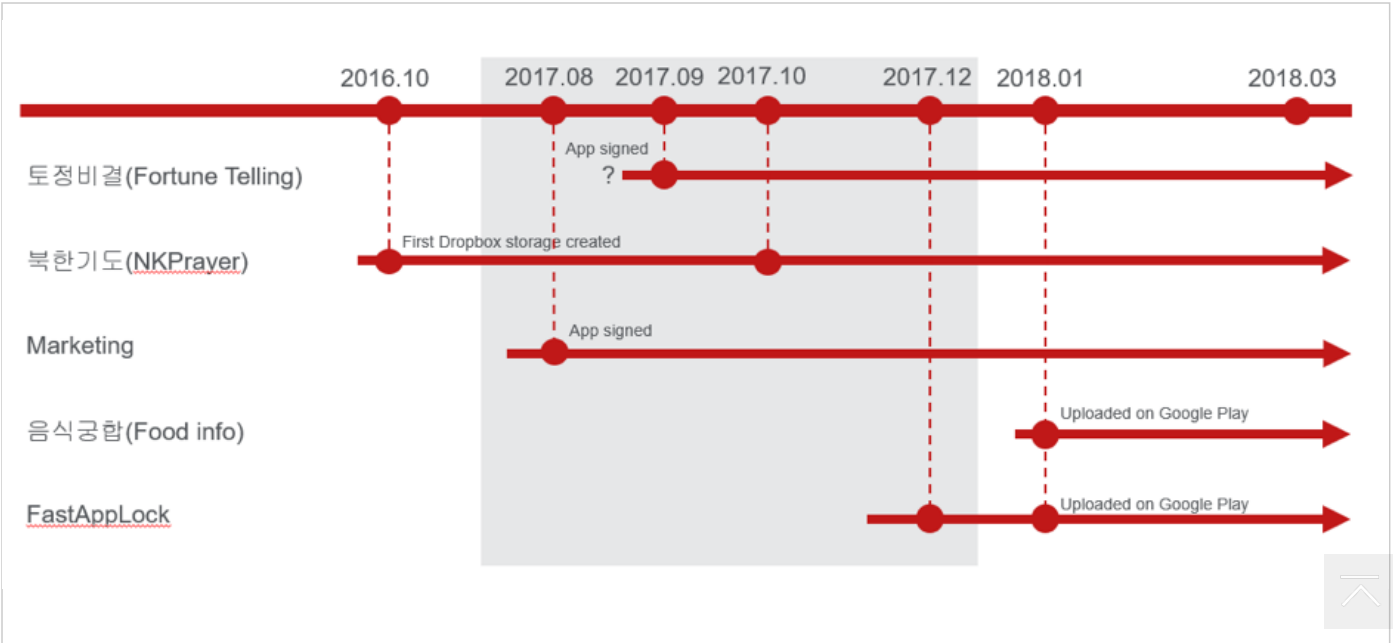
After infecting a device, the malware uses Dropbox and Yandex to upload data and issue commands, including additional plug-in dex files; this is a similar tactic to earlier Sun Team attacks. From these cloud storage sites, we found information logs from the same test Android devices that Sun Team used for the malware campaign we reported in January. The logs had a similar format and used the same abbreviations for fields as in other Sun Team logs. Further, the email addresses of the new malware's developer are identical to the earlier email addresses associated with the Sun Team. The relationship among email addresses and test devices is explained in the following diagram.



The use of identical email addresses ties the two malware campaigns to the same attacker.

About the Actors

After tracking Sun Team's operations, we were able to uncover different versions of their malware. Following diagram shows the timeline of the versions.

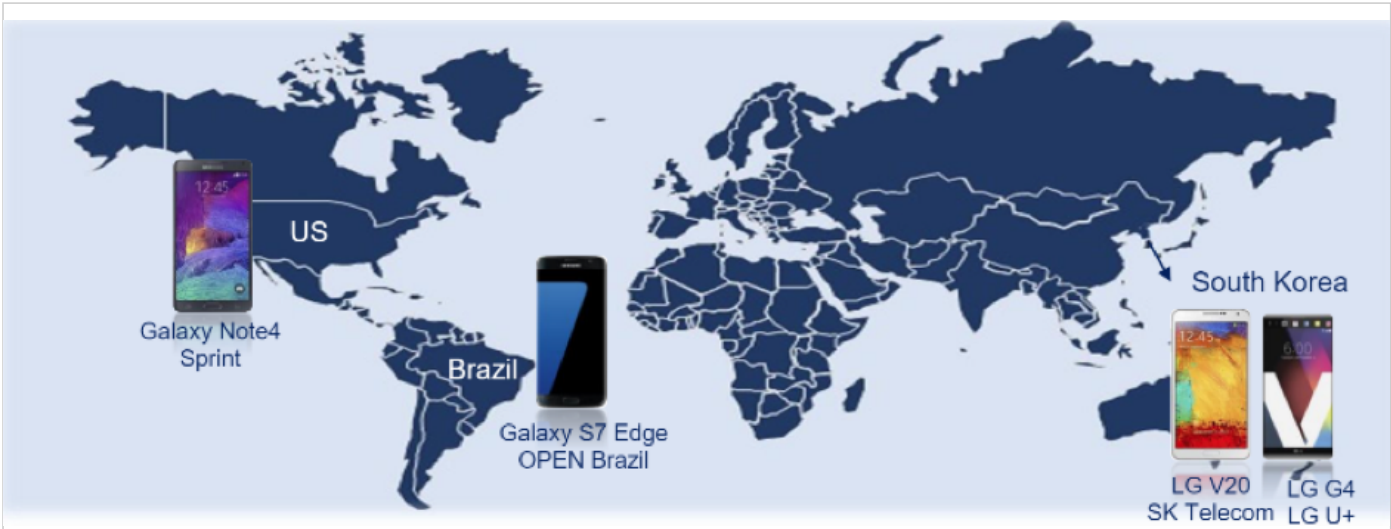


Timeline of different malware versions of Sun Team.

Timeline shows us that malwares became active in 2017. Sun Team's only purpose is to extract information from devices as all of the malwares are spywares. Malwares on Google Play stayed online for about 2 months before being deleted.

In our post of the earlier attack by this actor, we observed that some of the Korean words found on the malware's control server are not in South Korean vocabulary and that an exposed IP address points to North Korea. Also, Dropbox accounts were names from South Korean drama or celebrities.

In the new malware on Google Play, we again see that the Korean writing in the description is awkward. As in the previous operation, the Dropbox account name follows a similar pattern of using names of celebrities, such as Jack Black, who appeared on Korean TV. These features are strong evidence that the actors behind these campaigns are not native South Koreans but are familiar with the culture and language. These elements are suggestive though not a confirmation of the nationality of the actors behind these malware campaigns.



Sun Team's test devices originate from various countries.

Moreover, we uncovered information about the attacker's Android test devices and exploits they tried to use. The devices are manufactured in several countries and carry installed Korean apps, another clue that the threat actors can read Korean. The exploits codes were found uploaded on one of the cloud storages used by Sun Team which are modified versions of publicly available sandbox escape, privilege escalation, code execution exploits that added functions to drop their own Trojans on victims' devices. The modified exploits suggest that the attackers are not skillful enough to find zero days and write their own exploits. However, it is likely just a matter of time before they start to exploit vulnerabilities.

```
                DCB    0
aPmInstallSdcar DCB "pm install /sdcard/Download/SystemUpdate.apk",0
aAmStartservice DCB "am startservice com.android.systemservice/.CMService",0
aPmDStartcheckD DCB "pm =%d, startcheck = ",0x24,"%d",0
aRestarting     DCB "restarting>>>>>>>>",0
```

Modified exploits installing the Sun Team's Trojan.

The most concerning thing about this Sun Team operation is that they use photos uploaded on social network services and identities of South Koreans to create fake accounts. We have found evidence that some people have had their identities stolen; more could follow. They are using texting and calling services to generate virtual phone numbers so they can sign up for South Korean online services.

Conclusion

This malware campaign used Facebook to distribute links to malicious apps that were labeled as unreleased versions. From our analysis, we conclude that the actor behind both campaigns is Sun Team. Be cautious when installing unreleased or beta versions of any app. Also, check the number of downloads to see if an app is widely installed; avoid obscure apps.

McAfee Mobile Security detects this malware as Android/RedDawn.A, B. Always keep your mobile security application updated to the latest version.

‹ Previous Article (https://securingtomorrow.mcafee.com/consumer/family-safety/get-online-privacy-under-control/)
Next Article › (https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/facebook-users-data-exposed-by-suspended-app/)

Categories: McAfee Labs (https://securingtomorrow.mcafee.com/category/mcafee-labs/)
Tags: Google (https://securingtomorrow.mcafee.com/tag/google/), Lazarus (https://securingtomorrow.mcafee.com/tag/lazarus/), malware (https://securingtomorrow.mcafee.com/tag/malware/), mobile (https://securingtomorrow.mcafee.com/tag/mobile/), mobile security (https://securingtomorrow.mcafee.com/tag/mobile-security1/)

Leave a reply

Newsletter Sign Up

First Name *

Last Name *

Email Address *

Country *

--Please Select--

Submit

McAfee on Twitter

Follow us on Twitter (https://twitter.com/McAfee)

mcafee_labs (https://www.twitter.com/mcafee_labs)

Odin, Zepto, Diablo6. These are just a few of the aliases for our most dangerous threat. Get the 411 on Locky... https://t.co/l1QqNYZucq (https://t.co/l1QqNYZucq)

5 hours ago (2018/05/25 03:08:04)
Reply (https://twitter.com/intent/tweet?in_reply_to=999849554299310082) · Retweet (https://twitter.com/intent/retweet?tweet_id=999849554299310082) · Favorite (https://twitter.com/intent/favorite?tweet_id=999849554299310082)

mcafee_labs (https://www.twitter.com/mcafee_labs)

We're almost half way through 2018! What do you think has been the biggest story in the industry so far?

6 hours ago (2018/05/25 01:46:00)
Reply (https://twitter.com/intent/tweet?in_reply_to=999828898803105792) · Retweet (https://twitter.com/intent/retweet?tweet_id=999828898803105792) · Favorite (https://twitter.com/intent/favorite?tweet_id=999828898803105792)

mcafee_labs (https://www.twitter.com/mcafee_labs)

Devices affected by #VPNFilter (https://twitter.com/#search?q=VPNFilter) are network-attached storage (NAS) devices such as Linksys, MikroTik, Netgear, and T... https://t.co/CImN3iFI31 (https://t.co/CImN3iFI31)

12 hours ago (2018/05/24 20:04:07)
Reply (https://twitter.com/intent/tweet?in_reply_to=999742861779324928) · Retweet (https://twitter.com/intent/retweet?tweet_id=999742861779324928) · Favorite (https://twitter.com/intent/favorite?tweet_id=999742861779324928)

Next Article

(https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/facebook-users-data-exposed-by-suspended-app/)

Consumer Threat Notices (https://securingtomorrow.mcafee.com/category/consumer/consumer-threat-notices/)

Sensitive Data on 3 Million Facebook Users Potentially Exposed by Suspended App