Threatpost | The first stop for security news

- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook

Featured Posts

All

 Schneider Electric Patches XXE Vulnerability In…

 Ahead of GDPR, Information Governance Comes…

 Researchers Say More Spectre-Related CPU Flaws…

 TeenSafe Tracking App Exposes Thousands of…

 One Year After WannaCry: A Fundamentally…

 Critical Linux Flaw Opens the Door…

- Podcasts

Latest Podcasts

All

 Threatpost News Wrap Podcast for May…

 Podcast: The Evolution of Deception Technology

 A Look Inside: Bug Bounties and…

 Podcast: Why Manufacturers Struggle To Secure…

 Podcast: How Millions of Apps Leak…

 Threatpost RSA Conference 2018 Preview

Recommended

- Videos

Latest Videos

All

 Akamai CSO Talks Cryptominers, IoT and…

 HackerOne CEO Talks Bug Bounty Programs…

 A Closer Look at APT Group…

 Programs Controlling ICS Robotics Are 'Wide…

 The 'Perfect Storm' of Disinformation and…

 Cisco Warns of Critical Flaw in…

Recommended

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

Search

Join thousands of people who receive the latest breaking **cybersecurity news** every day.

Sign Up

E-mail

*

I agree that Threatpost may, at times, send information via email about new posts on the site, promotional offers from our partners, and premium assets like white papers, webcasts, videos, events etc. I understand that I can withdraw this consent at any time via the unsubscribe link included in every email.

Sign Up

Welcome > Blog Home>Facebook > RedDawn Espionage Campaign Shows Mobile APTs on the Rise

0 0 0 0 0

RedDawn Espionage Campaign Shows Mobile APTs on the Rise

by Tara Seals May 18, 2018 , 8:42 am

A sophisticated and targeted mobile espionage campaign has been found targeting North Korean defectors. Mounted by a relatively new APT actor known as Sun Team, the offensive used Google Play and Facebook as attack vectors; and overall, it shows how quickly the mobile threat landscape is evolving as APTs shift tactics to focus on this segment.

The RedDawn campaign, as it has been dubbed by the researchers that observed it, planted three "unreleased" beta apps in Google Play that target Korean-speaking users. They masquerade as something useful. One is called Food Ingredients Info, and the other two claim to be security-related (Fast AppLock and AppLockFree).

Related Posts

What Will GDPR's Impact Be On U.S. Consumer Privacy?

May 24, 2018 , 3:29 pm

New Facebook-Spread Malware Triggers Credential Theft, Cryptomining

May 10, 2018 , 2:00 pm

Facebook Introduces 'Clear History' Option Amid Data Scandal

May 2, 2018 , 12:07 pm

"We are witnessing an evolution of the traditional kill chain, where the platform is truly becoming agnostic," Raj Samani, chief scientist at McAfee, said in an email interview. "Mobile malware is over 14 years old, and the evolution of mobile threats into mobile APTs is a testament of the fact of how critical mobile devices have become to us in our digital life."

In reality, the food app and Fast AppLock secretly steal sensitive data like contacts, messages, call recordings and photos, and they're also capable of receiving commands and additional executable (.dex) files from a C2 server. AppLockFree, on the other hand, appears to be part of a reconnaissance effort, setting the foundation for a future wave of attacks.

"We believe this group behind this campaign is just getting started," said Samani.

As for how the malicious apps made it into the official store in the first place, he explained that the apps were meant to be an innocuous-looking initial foundation for the attack.

"The initial stage that was uploaded on Google Play was just enough to go under their radar, but enough to carry out surveillance to download additional custom made payloads depending on the intentions of the attacker," Samani noted. "This kind of sophistication is traditionally what we see with attacks on the PC side, to see this kind of tactics coming to mobile devices is genuinely a sign this is the year of mobile malware."

After being installed on Android devices, the malware uses Facebook to infiltrate the victims' friends, through messages asking them to install the apps and offering feedback via a Facebook account with a fake profile. This proved to be virulent; although the initial infection group totaled around 100 people, the Sun Team was able to scale its campaign far beyond, the research showed.

"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," said researchers. "We have found evidence that some people have had their identities stolen; more could follow. They are [also] using texting and calling services to generate virtual phone numbers so they can sign up for South Korean online services."

Samani said that the Bouncer app-vetting tool and Google Play Protect both failed to detect the rogue apps in Google Play; Google Security however immediately responded to a request for a takedown. This is unlikely to be the end of it, though: RedDawn is the second campaign observed this year from the Sun Team hacking group. In January, a similar Android malware effort was found targeting North Korean defectors and journalists.

"[The fact that this] is the second attempt this year, despite the fact that we had called out/dismantled their previous efforts in January, is a testament to the fact they will come back with new tactics and strategies," Samani said.

Based on the Dropbox and Yandex cloud storage sites the malware uses to upload data and issue commands, it's clear that RedDawn was the work of the same crew. For instance, researchers found information logs from the same test Android devices that Sun Team used for the January malware campaign.

"The logs had a similar format and used the same abbreviations for fields as in other Sun Team logs," McAfee said in an analysis published on Thursday. "Further, the email addresses of the new malware's developer are identical to the earlier email addresses associated with the Sun Team."

As for who's behind Sun Team, the profile of the targeted victims (North Korean defectors) as well as some of the attributes in the campaign point north. For instance, some of the Korean words found on the malware's control server are not in South Korean vocabulary; and, an exposed IP address points to North Korea. Even so, Dropbox accounts were names from South Korean celebrities.

"These features are strong evidence that the actors behind these campaigns are not native South Koreans but are familiar with the culture and language," researchers noted.

RedDawn is an indicator of how nation-state spy tactics are evolving, Samani said. Aside from the Sun Team, researchers also recently identified that the Lazarus APT has also shifted its attention to mobile, using more sophisticated attack techniques of late, such as using forged signatures to bypass security verifications in the operating system. Also, last week a piece of North Korean spyware was found targeting Apple iOS devices.

"It's not just Korea, but we have seen mobile devices been targeted in Iran as well as other emerging countries, as well as among immigrants living in the U.S.," he explained. "If you're a person of interest on the run or constantly on the move (may it be North Korean defectors or protesters in Iran), smartphones are likely to be your preferred method of accessing the internet."

Categories: Facebook, Government, Malware

Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email

Post Comment

Notify me when new comments are added.

Recommended Reads

May 24, 2018 , 3:29 pm
Categories: Facebook, Privacy, Web Security

What Will GDPR's Impact Be On U.S. Consumer Privacy?

by Lindsey O'Donnell

GDPR may be going in effect Friday, but U.S. citizens have a ways to go before seeing similar privacy regulations from the U.S government.

Read more...

May 10, 2018 , 2:00 pm
Categories: Facebook, Featured, Hacks, Malware

New Facebook-Spread Malware Triggers Credential Theft, Cryptomining

by Lindsey O'Donnell

A new malware campaign being rapidly spread on Facebook is infecting users' systems to perform credential theft, cryptomining, and click fraud.

Read more...

0 0 0 2 0

May 2, 2018 , 12:07 pm
Categories: Facebook, Privacy, Web Security

Facebook Introduces 'Clear History' Option Amid Data Scandal

by Lindsey O'Donnell

Facebook hopes to improve data privacy with a new feature letting users flush their history so that it is cleared from their account.

Read more...

Top Stories

MassMiner Takes a Kitchen-Sink Approach to Cryptomining

May 3, 2018 , 4:26 pm

"Equi-Facts": Equifax Clarifies the Numbers for Its Massive Breach

May 8, 2018 , 12:45 pm

RedDawn Espionage Campaign Shows Mobile APTs on the Rise

May 18, 2018 , 8:42 am

One Year After WannaCry: A Fundamentally Changed Threat Landscape

May 17, 2018 , 11:25 am

Bezop Cryptocurrency Server Spills 25K in Private Investor, Promoter Data

April 25, 2018 , 10:46 am

RIG EK Still Makes Waves, This Time with a Stealthy Backdoor

May 16, 2018 , 7:19 am

Intel's 'Virtual Fences' Spectre Fix Won't Protect Against Variant 4

May 24, 2018 , 11:18 am

Adobe Patches Critical Bugs In Flash Player, Creative Cloud

May 8, 2018 , 12:56 pm

Join thousands of people who receive the latest breaking **cybersecurity news** every day.

Sign Up

Categories
Black HatCloud SecurityCritical InfrastructureCryptographyFacebookFeaturedGovernmentHacksIoTMalwareMobile SecurityPodcastsPrivacyRSACSecurity Analyst SummitSlideshowUncategorizedVideosVulnerabilitiesWeb Security

Authors

Michael Mimoso
Tom Spring
Christopher Brook