Tropic Trooper Goes Mobile With Titan Surveillanceware

blog.lookout.com/titan-mobile-threat

Lookout researchers have recently observed cybercriminals evolving the way they operate to reflect the multitude of platforms people now use to access information: you may read and triage email on a smartphone, switch to a laptop to crank out some work, then flip over to a tablet to catch up on social media or watch a video. To the attackers, it's a numbers game. The more devices they can reach, the more likely they are to compromise a target. Given the rise of mobile productivity, this means that we are seeing a growing number of attackers add mobile capabilities to their toolkits.

The latest threat to follow this trend is Titan, a family of sophisticated Android surveillanceware apps surfaced by Lookout's automated analysis that, based on command and control infrastructure, is linked to the same actors behind Operation Tropic Trooper. Tropic Trooper is a long running campaign, first reported in 2016, that executed targeted desktop attacks against enterprises and military units in Taiwan and the Philippines. All Lookout customers are protected from Titan.

Capabilities

Titan usually comes with busybox and various native libraries that provide a range of functionality, from automated gathering of a user's data to being able to execute attacker specified instructions as superuser. Over time, Titan has evolved considerably with a distinct

trend of malicious code shifting first from Java to native libraries, then moving into second stage components. Analysis of Titan variants found that they contained the following capabilities:

- Retrieve call history
- Retrieve text messages
- Retrieve contact information
- Retrieve a list of Installed packages
- Track device location
- Take a photo with the device camera when a user is first present or when instructed by an attacker
- Record all calls or only calls to attacker specified numbers
- Block text messages to attacker specified numbers
- Take a screenshot
- Send a text message
- Execute attacker specified commands as root
- Upload specific files
- Download attacker specified files

Titan hasn't been seen to trojanize legitimate applications and doesn't contain any legitimate functionality. The authors of Titan have instead opted to simply use the icon of a legitimate app. Application icons used included:

- Zalo - a vietnamese Messaging Application,
- 91 - an unofficial Chinese App Store that was bought by Baidu in 2013 for 1.9 billion,
- YY - a popular Chinese social network,
- Renren - formerly Xiaonei Network, this is a social network primarily used by Chinese college students,
- 58 - an online Chinese marketplace,
- WeChat - a popular Chinese messaging app, and
- FloatingMenu - an application for handling shortcuts and gestures.

Infrastructure

Several domains and IP addresses associated to this family are no longer live however further research is being conducted into 108.61.xxx.xxx which, at the time of writing, is live, running PHP, and exposing information that may provide additional leads. Some Titan variants have been seen to iterate through a list of possible command and control servers when beaconing out. Domains and IPs that Titan has, or is currently, using are listed below.

Domain / IP

Port

mysupport.dnset.com

3350 or 3351

mysupport.zyns.com

3350 or 3351

122.10.94.64

3350 or 3351

202.153.193.73

9006

androidshome.com

9006

www.mark40.25u.com

9006

113.10.221.89

9006

108.61.xxx.xxx

80

As a family that is actively being improved, and given its links to targeted attacks against enterprises and defense institutions, Lookout is continuing to track Titan variants, associated server infrastructure, and geographical regions where they're being deployed.

SHA-1s

e9d4a39e763471c406490e19c22b98d9fa5a9151
3373a1a3151c3ae67903b7503828055c339e988f
dbc73a8cc28fa0bab441ed75e51da206e49cf9e2
1a50b9853e0dc9cc9d7e90e5076dda632589fe9f
80b303c0e09c36084b1e91367465ad621c29c0ad
bfc6390f016715f9adb0876840a76079df4ae3dd
843df2fd5d9c86bd08c90b9e405481ec75d1eb90
6f68376cda0578a6df6ec3059ffda85cda7a0bec

75be9cdcbc3cdcf1bede3c80214995758d5b9c61
ef2dd1b8ce479276c72e17da217e74f1ce9a2ee1
2af65847aad4a976ed72a67c489daf3a100c0d65
5df3b5f59709a3e02386e9297ae2f1b1ef1a6ac3
2aa2f48ea856803b19925a7d0abb3a443f31d095
3ec97bd2e8105fcb530b249e86a4aa7e35e52e44
a2e60c28259e0982a1eb7768fa2433f84e64a817

Want to learn more about threats like Titan and our Threat Advisory services? Contact Lookout today.

Lookout researchers have recently observed cybercriminals evolving the way they operate to reflect the multitude of platforms people now use to access information: you may read and triage email on a smartphone, switch to a laptop to crank out some work, then flip over to a tablet to catch up on social media or watch a video. To the attackers, it's a numbers game. The more devices they can reach, the more likely they are to compromise a target. Given the rise of mobile productivity, this means that we are seeing a growing number of attackers add mobile capabilities to their toolkits.

The latest threat to follow this trend is Titan, a family of sophisticated Android surveillanceware apps surfaced by Lookout's automated analysis that, based on command and control infrastructure, is linked to the same actors behind Operation Tropic Trooper. Tropic Trooper is a long running campaign, first reported in 2016, that executed targeted desktop attacks against enterprises and military units in Taiwan and the Philippines. All Lookout customers are protected from Titan.

Capabilities

Titan usually comes with busybox and various native libraries that provide a range of functionality, from automated gathering of a user's data to being able to execute attacker specified instructions as superuser. Over time, Titan has evolved considerably with a distinct trend of malicious code shifting first from Java to native libraries, then moving into second stage components. Analysis of Titan variants found that they contained the following capabilities:

- Retrieve call history
- Retrieve text messages
- Retrieve contact information
- Retrieve a list of Installed packages
- Track device location
- Take a photo with the device camera when a user is first present or when instructed by an attacker
- Record all calls or only calls to attacker specified numbers

- Block text messages to attacker specified numbers
- Take a screenshot
- Send a text message
- Execute attacker specified commands as root
- Upload specific files
- Download attacker specified files

Titan hasn't been seen to trojanize legitimate applications and doesn't contain any legitimate functionality. The authors of Titan have instead opted to simply use the icon of a legitimate app. Application icons used included:

- Zalo - a vietnamese Messaging Application,
- 91 - an unofficial Chinese App Store that was bought by Baidu in 2013 for 1.9 billion,
- YY - a popular Chinese social network,
- Renren - formerly Xiaonei Network, this is a social network primarily used by Chinese college students,
- 58 - an online Chinese marketplace,
- WeChat - a popular Chinese messaging app, and
- FloatingMenu - an application for handling shortcuts and gestures.

Infrastructure

Several domains and IP addresses associated to this family are no longer live however further research is being conducted into 108.61.xxx.xxx which, at the time of writing, is live, running PHP, and exposing information that may provide additional leads. Some Titan variants have been seen to iterate through a list of possible command and control servers when beaconing out. Domains and IPs that Titan has, or is currently, using are listed below.

Domain / IP

Port

mysupport.dnset.com

3350 or 3351

mysupport.zyns.com

3350 or 3351

122.10.94.64

3350 or 3351

202.153.193.73

9006

androidshome.com

9006

www.mark40.25u.com

9006

113.10.221.89

9006

108.61.xxx.xxx

80

As a family that is actively being improved, and given its links to targeted attacks against enterprises and defense institutions, Lookout is continuing to track Titan variants, associated server infrastructure, and geographical regions where they're being deployed.

SHA-1s

e9d4a39e763471c406490e19c22b98d9fa5a9151
3373a1a3151c3ae67903b7503828055c339e988f
dbc73a8cc28fa0bab441ed75e51da206e49cf9e2
1a50b9853e0dc9cc9d7e90e5076dda632589fe9f
80b303c0e09c36084b1e91367465ad621c29c0ad
bfc6390f016715f9adb0876840a76079df4ae3dd
843df2fd5d9c86bd08c90b9e405481ec75d1eb90
6f68376cda0578a6df6ec3059ffda85cda7a0bec
75be9cdcbc3cdcf1bede3c80214995758d5b9c61
ef2dd1b8ce479276c72e17da217e74f1ce9a2ee1
2af65847aad4a976ed72a67c489daf3a100c0d65
5df3b5f59709a3e02386e9297ae2f1b1ef1a6ac3
2aa2f48ea856803b19925a7d0abb3a443f31d095
3ec97bd2e8105fcb530b249e86a4aa7e35e52e44
a2e60c28259e0982a1eb7768fa2433f84e64a817

Want to learn more about threats like Titan and our Threat Advisory services? Contact Lookout today.

November 16, 2017

Download Case Study
{{consumer="/components/cta/consumer"}}

TAGS:

|

Threat Intelligence
|

Surveillanceware