Cyberespionage Campaign Sphinx Goes Mobile With AnubisSpy

blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/

December 19, 2017

Android malware like ransomware exemplify how the platform can be lucrative for cybercriminals. But there are also other threats stirring up as of late: attacks that spy on and steal data from specific targets, crossing over between desktops and mobile devices.

Take for instance several malicious apps we came across with cyberespionage capabilities, which were targeting Arabic-speaking users or Middle Eastern countries. These were published on Google Play — but have since been taken down — and third-party app marketplaces. We named these malicious apps AnubisSpy (ANDROIDOS_ANUBISSPY) as all the malware's payload is a package called *watchdog*.

We construe AnubisSpy to be linked to the cyberespionage campaign Sphinx (APT-C-15) based on shared file structures and command-and-control (C&C) server as well as targets. It's also possible that while AnubisSpy's operators may also be Sphinx's, they could be running separate but similar campaigns.

What can AnubisSpy do?

AnubisSpy can steal messages (SMS), photos, videos, contacts, email accounts, calendar events, and browser histories (i.e., Chrome and Samsung Internet Browser). It can also take

screenshots and record audio, including calls. It can spy on the victim through apps installed on the device, a list of which is in its configuration file that can be updated. This includes Skype, WhatsApp, Facebook, and Twitter, among others.

After the data are collected, they are encrypted and sent to the (C&C) server. AnubisSpy can also self-destruct to cover its tracks. It can run commands and delete files on the device, as well as install and uninstall Android Application Packages (APKs).

AnubisSpy has several modules, each of which has a separate role. AnubisSpy's code is well constructed, indicating the developer/s' know-how. Below is a visualization of the modules:

 *Figure 1: Structure of AnubisSpy's modules*

How is AnubisSpy related to Sphinx?
Sphinx reportedly uses the watering hole technique via social media sites to deliver its payloads — mainly a customized version of njRAT. The Sphinx campaign operators cloaked the malware with icons of legitimate applications to dupe recipients into clicking them. Sphinx was active between June 2014 and November 2015, but timestamps of the malware indicate the attacks started as early as 2011.

A simple WHOIS query of AnubisSpy's C&C server showed it abused a legitimate managed hosting service provider in Belize. We correlated the AnubisSpy variants to Sphinx's desktop/PC-targeting malware through the following:

- Shared C&C server, 86[.]105[.]18[.]107
- Shared technique of decrypting JSON files, and similarity between the file structures of AnubisSpy and Sphinx's malware
- Similar targets (highly concentrated in Middle Eastern countries)

Figure 2: Comparison of file structure in Sphinx's desktop/PC-targeting malware (left) and AnubisSpy (right)

These apps were all written in Arabic and, in one way or another, related to something in Egypt (i.e., spoofing an Egypt-based TV program and using news/stories in the Middle East) regardless of the labels and objects in the apps. Our coordination with Google also revealed that these apps were installed across a handful of countries in the Middle East.

Was AnubisSpy actively distributed?

We analyzed seven apps that were actually AnubisSpy. These were signed with the same fake Google certificates. We found two more apps created by the same developer, but they had no espionage-related codes; we think they were made as experimental projects. Based

on hardcoded strings in the Agent Version, the malicious apps were developed as early as April 2015. Timestamps indicate that the earliest sample was signed on June 2015; the latest variant was signed on May 2017.

AnubisSpy wasn't only published on Google Play. We also found versions of it in third-party app marketplaces, most likely as a way to expand the malware's reach. The apps mainly used Middle East-based news and sociopolitical themes as social engineering hooks and abused social media to further proliferate. Versions of AnubisSpy posed as social news, promotional, healthcare, and entertainment apps.

What does AnubisSpy mean to the mobile landscape?

Persistent and furtive spyware is an underrated problem for the mobile platform. While cyberespionage campaigns on mobile devices may be few and far between compared to ones for desktops or PCs, AnubisSpy proves that they do indeed occur, and may have been more active than initially thought. Will mobile become cyberespionage's main frontier? It won't be a surprise given mobile platform's increasing ubiquity, especially in workplaces.

Beyond its effects, AnubisSpy also highlights the significance of proactively securing mobile devices, particularly if they're on BYOD programs and used to access sensitive data. Enforcing the principle of least privilege and implementing an app reputation system are just some of the best practices that can help mitigate threats.

We disclosed our findings to Google on October 12 and worked with Google on further analyzing the AnubisSpy-related apps. Updates were also made to Google Play Protect to take appropriate action against those apps that have been verified as in violation of Google Play policy. An in-depth technical analysis of AnubisSpy, along with indicators of compromise, is in this **technical brief**.

Trend Micro Solutions

End users and enterprises can also benefit from multilayered mobile security solutions such as Trend Micro™ Mobile Security which is also available on Google Play. For organizations, Trend Micro™ Mobile Security for Enterprise provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from attacks that leverage vulnerabilities, preventing unauthorized access to apps, as well as detecting and blocking malware and fraudulent websites.

Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies. It can protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Malware

Researchers disclosed an attack campaign targeting sectors in the Middle East. This threat actor was called Two-tailed Scorpion/APT-C-23. A mobile component called VAMP was found, with a new variant (dubbed FrozenCell) discovered in October.

By: Ecular Xu, Grey Guo December 19, 2017 Read time: (words)

Content added to Folio