An effective unknown botnet malware detection mechanism for android-based mobile devices

高家緯、曹偉駿

E-mail: 344740@mail.dyu.edu.tw

ABSTRACT

At present, the smart phone system is developing vigorously, in which Android occupies most of the current market share, using the open operating system to provide overall effective applications (APPs) for the users to install. However, while it provides protection, it also brings harms just like a double-edged sword. Some malware may hide in the various Android APPs. This study mainly discusses one of the Android botnets, which abuses the powerful connection function of Android. Its distributed denial of service (DDoS)attacks have the features of the large-scaled botnet, plus the high mobility of the Android mobile device, so it will cause greater harm to the targets than the conventional DDoS attacks, and it is hard to track the attack source. This malware makes the Android connection slower, so that users cannot normally use the network service. What worse, the greater threat is that it blocks the operation of servers; as a result, the uninfected Android smart phones can't normally access the network services. Nowadays, most of the conventional DDoS detection mechanisms are in the server-end, which can only temporarily relieve the DDoS attacks to stabilize the normal service, but don't provide effective solution to the Android botnet problems. Furthermore, the conventional detectors are not designed for mobile devices, so its design mechanism is not suitable for the mobile devices with low performance, limited powers and less storage space. Therefore, in order to design an effective detection mechanism to unknown botnet malware, this study first develops a kind of Android botnet malware based on the HTTP Flood attack, which is the most inundant DDoS attack and is hard to detect; meanwhile, it cannot be detected by the well-known anti-virus software tools. Afterward, we further develop a mechanism that cannot only effectively detect a wide variety of unknown botnet malware, but also detect the botnet malware developed in this study. The performance evaluation and analysis reveal the proposed detection mechanism indeed has high detection accuracy, and is superior to the related studies in terms of performance requirements and practical applications. Thus, we affirm the proposed detection mechanism has extremely high practical application value.

Keywords : Android、Botnet、Distributed Denial of Service、System Security

Table of Contents

REFERENCES

[1]Pu Wang, Marta C. Gonzalez1, Cesar A. Hidalgo, and Albert-Laszlo Barabasi, “ Understanding the spreading patterns of mobile phone viruses, ” Science, vol. 324, no. 5930, pp. 1071-1076, 2009.
[2]Andre van Cleeff, “ Future consumer mobile phone security: A case study using the data-centric security model, ” Information Security Technical Report, vol. 13, no. 3, pp. 112-117, 2008.
[3]Android Developer, http://developer.android.com, 2011.
[4]Margaret Butler “ Android: Changing the mobile landscape, ” IEEE Pervasive Computing, vol. 10, no. 1, pp. 4-7, 2011.
[5]Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer and Yael Weiss “ Andromaly: a behavioral malware detection framework for android devices, ” Journal of Intelligent Information Systems, Online Article, 2011.
[6]Arbor Networks “ Worldwide infrastructure security report ”, vol. vi, 2010.
[7]Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao “ Survey of network-based defense mechanisms countering the DoS and DDoS Problems, ” ACM Computing Surveys, vol. 39, no. 1, pp. 1-46, 2007.
[8]Dmitry Rovniagin and Avishai Wool “ The geometric efficient matching algorithm for firewalls, ” IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 147-159, 2011.
[9]Android Market, http://Market.android.com, 2011.
[10]Android Open Source project, http://Source.android.com, 2011.
[11]Brian C. Williams and Errin W. Fulp “ A biologically modeled intrusion detection system for mobile networks, ” Proceedings of the Broadband Wireless Computing Communication and Applications, no.6, pp. 453-458, 2010.
[12]Kamer Ali Yuksel and Osman Kira “ Enhancing security of linux-based Android devices, ” Proceedings of the 15th International Linux Kongress, no.5, pp. 26-34, 2008.
[13]A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Gleze “ Google Android: A comprehensive security assessment, ” IEEE Security & Privacy, vol. 8, no. 2, pp. 35-44, 2010.
[14]Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi and Marcel Winandy “ Privilege escalation attacks on Android, ” Proceedings of the 13th Information Security Conference pp. 346-360, 2010.
[15]Wook Shin, Shinsaku Kiyomoto, Kazuhide Fukushima and Toshiaki Tanaka “ A formal model to analyze the permission authorization and enforcement in the Android framework, ” Proceedings of the IEEE Social Computing, pp. 994-1002, 2010.
[16]William Enck, Peter Gilbert, Byung-Gon Chun, Landon Cox, Jaeyeon Jung, Patrick McDaniel and Anmol Sheth “ Taintdroid: an information-?ow tracking system for realtime privacy monitoring on smartphones, ” Proceedings of the USENIX Symposium on Operating Systems Design and Implementation, pp. 34-43, 2010.
[17]G.Portokalidis, P.Homburg, K.Anagnostakis, and H.Bo “ Paranoid Android: versatile protection for smartphones, ” Proceedings of the 26th Annual Computer Security Applications Conference, pp. 48-54, 2010.
[18]Avik Chaudhuri “ Language-based security on Android. ” Proceedings of the 4th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, pp. 1-7, 2009.
[19]D. Barrera, H. G. u. c. Kayacik, P. C. van Oorschot and A. Somayaji “ A methodology for empirical analysis of permission-based security models and its application to android, ” Proceedings of the 17th ACM conference on Computer and communications security, pp. 73-84, 2010.
[20]W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka “ Towards formal analysis of the permission-based security model for Android, ” Proceedings of the 5th International Conference on Wireless and Mobile Communications, pp. 87-92, 2009.
[21]Wook Shin, Sanghoon Kwak, Shinsaku Kiyomoto, Kazuhide Fukushima and Toshiaki Tanaka “ A small but non-negligible flaw in the Android permission scheme, ” Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks, pp. 57-62, 2010.
[22]Mohammad Nauman, Sohail Khan, and Xinwen Zhang “ Apex: extending Android permission model and enforcement with user-defined runtime constraints, ” Proceedings of the 5th ACM Symposium on Information Computer and Communications Security, pp. 85-94, 2010.
[23]Asaf Shabtai, Uri Kanonov and Yuval Elovici “ Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method, ” Journal of Systems and Software, vol. 83, no. 8, pp. 1524-1537, 2010.
[24]Cui Xiang, Fang Binxing, Yin Lihua, Liu Xiaoyi, and Zang Tianning “ Andbot: towards advanced mobile botnets, ” Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats, pp. 41-50, 2011.

[25]Shui Yu, Wanlei Zhou, and Robin Doss “ Information theory based detection against network behavior mimicking DDoS attacks, ” IEEE Communications Letters, vol. 12, no. 4, pp. 318-321, 2008.
[26]Tom Fawcett “ An introduction to ROC analysis, ” Pattern Recognition Letters, vol. 27, no. 8, pp. 861-874, 2006.
[27]Wireshark, http://www.wireshark.org, 2011.