كشف البوت نت على أساس تحليل المعلومات في الشبكة و جهاز المستخدم

سوزان بندر المطيري

د.سوسن محفوظ

المستخلص

واحدة من تهديدات شبكة الإنترنت الأكثر خطورة هو الروبوتات . يتم تشغيل الروبوتات في خلفية آلة للخطر ويحافظ على التواصل مع الخادم C&C لاستقبال الأنشطة و الأوامر الخبيثة . أنشطة يتم القيام بها دون علم صاحب جهاز الكمبيوتر للخطر .يستخدم سيد الروبوتات الروبوتات لشن هجمات خطرة مثل (دوس)، وسرقة البيانات، الاحتيال والبريد الالكتروني غير المرغوب.

و حجم الروبوتات عدد كبير عادة ما الذي يمكن أن يكون بالملايين الجنود المصابين .وتتناول هذه الأطروحة مشكلة الروبوتات والتفريق بين تدفقات الاشارة داخل سجلات الشبكات في جهاز المضيف . نقترح التقنية عامة التي هي قادرة على الكشف عن الروبوتات الجديد في مراحل مبكرة . هذه التقنية يمكن أن تنفذ على ثلاثة مستويات: على الجانب المضيف، إلى جانب شبكة أو مزيج من الاثنين معا . أنواع حركة الاتصالات الروبوتات التي نهتم بها هيHTTP : P2P ، IRC و DNS.

وقد تم تقييم هذه التقنية المقترحة مع مجموعة من مجموعات البيانات الخبيثة الحقيقية . وتم اقتراح HANABot خوارزمية المعالجة المسبقة واستخراج ميزات التفريق بين السلوك الروبوتات من السلوك الشرعي . وقد أظهرت نتائج التصنيف أنها دقيقة مع معدل إيجابي منخفض . وعلاوة على ذلك، تم تقديم مقارنة بين بعض المناهج الحالية في المدى من الميزات المحددة. وأداء التقنية المقترحة يتفوق بعض المناهج المقدمة من حيث التفريق بدقة تدفقات الروبوتات داخل السجلات الشبكة.

GENERAL BOTNET DETECTION BASED ON NETWORK AND HOST ANALYSIS

Suzan Bandar Al Mutairi

Supervised By
Dr. Saoucene Alaye Mahfoudh

ABSTRACT

One of the most serious cyber-security threats is the botnet. The botnet runs in the background of the compromised machine and maintains communication with the C\&C server to receive malicious commands. Malicious activity is executed without the knowledge of the owner of the compromised computer. Botnet master uses botnet to launch dangerous attacks such as Distributed Denial of Service (DDoS), finishing, Data stealing, Click fraud and spamming. The size of the botnet is usually very large and millions of infected hosts may belong to it.

This thesis addresses the problem of detecting botnet flows records within Netflow traces and activities in the host. We propose a general technique that is capable of detecting a new botnet in early stages. Our technique can be implement at three level: the host level, the network level or a combination of both. The botnet communication traffic we are interested in includes HTTP, P2P, IRC and DNS using IP fluxing.

The proposed technique has been evaluated with a collection of real malicious and legitimate datasets. HANABot algorithm is proposed to preprocess and extracted features to differentiate the botnet behavior from the legitimate behavior. The results of our experiment show a high level of accuracy and a low positive rate. Furthermore, a comparison between some existing approaches was given, focusing on specific features and performance. The proposed technique outperforms some of the presented approaches in terms of accurately detecting botnet flow records within Netflow traces.