온라인 게임 내의 핵 프로그램 탐지 방법

이창선*, 유진호**
*상명대학교 경영학과 박사과정(정보시스템 보안전공)
**상명대학교 경영학과 교수
e-mail:crattack@gmail.com

A Study on Online Game inside Hack Program Detecting Method

Chang-Seon Lee*, Jinho Yoo**
*Department of Business Administration(Information Systems & Security), Sangmyung University
**Department of Business Administration, Sangmyung University

요 약

온라인 게임에서 핵 프로그램을 탐지하는 방식 중 하나인 시그니처 탐지 방식의 문제점을 제시와 제시된 문제점을 보완하기 위한 발전된 시그니처 탐지 방식을 적용하므로 인하여 기존의 가지고 있던 문제를 개선할 수 있는 방법이다. 이 방식을 기존에 탐지하고 있는 방식과 병행할 경우 핵 프로그램을 수집해야하는 번거로움과 미 탐지로 인한 게임내의 핵 프로그램을 탐지하는데 일조할 것으로 보인다.

1. 서론

온라인 게임에서 핵 프로그램을 사용하는 유저를 찾는 것은 지속적으로 연구되어 왔다. 다양한 방법으로 불법 프로그램 사용자들을 탐지하고 제재하고 있다. 불법 프로그램 사용자를 탐지하는 방법에는 시그니처 기반 탐지 방법, 유저의 행동 패턴을 탐지하는 휴리스틱 방법[2][3], 데이터 마이닝등 기법들이 있다. 여기에서는 시그니처 기반으로 한 탐지 방법에서 시그니처를 효과적으로 활용할 수 있는 방법에 대해 제안하려고 한다.

본 논문의 구성은 2장에서는 시그니처를 기반으로 한 탐지 방법에 대해 설명하고 3장에서는 발전된 시그니처 기반의 탐지방법을 제안하도록 하겠다. 마지막으로 4장에서는 향후 연구방향에 대해 제시하였다.

2. 시그니처 기반의 탐지 방법

시그니처란 바이너리 상에서의 고유의 패턴을 찾는 것을 의미한다[1][2]. 시그니처 기반의 탐지 방식은 메모리 상 또는 파일 상에서 문자열을 추출하거나, Hex 값을 추출하여 적용한다. 추출한 시그니처가 존재하는지에 따라 핵 프로그램이 동작하고 있는지를 확인하는 방법이다.

시그니처의 단점은 첫째, 핵 프로그램을 수집되어야 탐지가 가능하며,[그림 1.] 둘째는, 추출한 시그니처에서 1byte라도 변경되면 탐지가 되지 않는 것에 있다.[그림 2.] 이렇듯 수집되지 않은 핵 프로그램은 사용 된다. 수집 되지 않은 핵 프로그램이 많으므로 핵 프로그램을 수집을 모두 할 수 없다. 따라서, 시그니처 기반의 핵 프로그램 탐지 방식은 제한되어 사용된다.

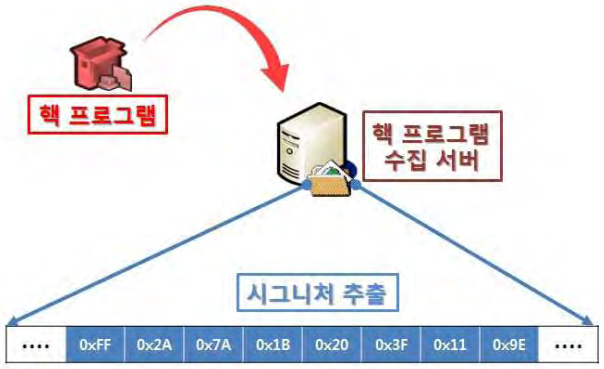

그림 1. 신규 핵 프로그램 시그니처 추출

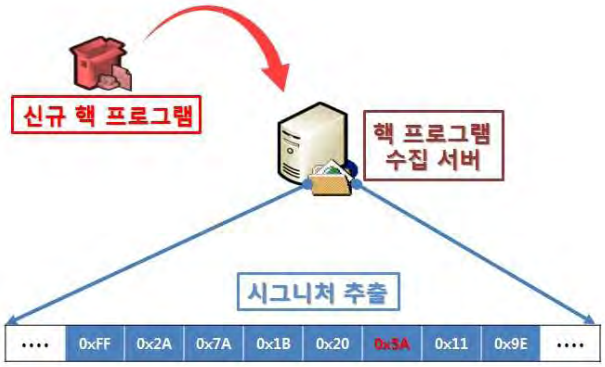

그림 2. 신규 핵 프로그램 시그니처 우회

3. 발전된 시그니처 기반의 탐지 방법

기존의 시그니처 탐지 방식은 수집되어야만 핵 프로그램을 탐지가 가능하다. 본 논문에서 제시하는 방식은 수집

되지 않은 핵 프로그램에 대해 탐지할 수 있다. 구현 방법은 다음과 같다.

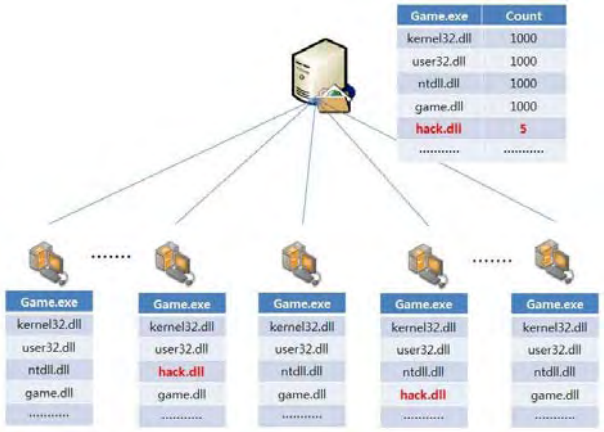

그림 3. 발전된 시그니처 기반 탐지 방법

발전된 시그니처의 경우 처음에는 수집 기간이 필요하다. 정상적인 모듈에 대한 카운트를 지정하여, 서버에서는 카운드 횟수가 낮은 부분에 대해서는 악성코드로 판단한다. 물론, 카운트가 낮은 DLL이라고 모든 핵 프로그램은 아니지만 가능성이 높은 경우이므로 수집을 통해 핵 프로그램 유무를 판단해야 한다.

또한, 게임 핵 프로그램은 멀웨어와 달리 운영체제에서 사용되지 않고 게임에서 이득을 취하는 목표이 있으므로 그림 3과의 방식을 적용할 수 있다.

4. 향후 연구 방식

핵 프로그램은 그림 3과 같이 DLL 형태로 동작하는 경우도 있지만 멜 웨어와 같이 메모리상의 부분으로 나뉘어 동작하는 사례도 있으므로, 메모리 상에서 나눠진 핵 프로그램을 찾는 방식을 연구해야 할 과제이다.

참고문헌

[1] J.-Y. Xu, A. H. Sung, P. Chavez, and S. Mukkamala. Polymorphic malicious executable scanner by api
sequence analysis. In Proc. of the 4th International Conference on Hybrid Intelligent Systems (HIS'04), Kitakyushu, Japan, pages 378.383. IEEE, December 2004

[2]Jose Nazario, "Defense and Detection Strategies against Internet Worms" artech House, 2004

[3] M. Christodorescu and S. Jha. Static analysis of executables to detect malicious patterns. In Proceedings of the 12th USENIX Security Symposium (Security'03), pages 169-186. USENIX Association, USENIX Association, Aug. 2003.

[4] S. G. Masood. Malware Analysis for Administrators. http://www.symantec.com/connect/articles/malware-analysis-administrators. 2004