실머신 기반 악성코드 자동 분석 시스템에서의 네트워크 덤프

조영훈*, 나재찬*, 윤종희*
*영남대학교 컴퓨터공학과
e-mail : youn@yu.ac.kr

Network Dump of Automated Malware Analysis System based on Real Machine

Jonghee M. Youn*, Jaechan Na*, Younghun Jo*
*Dept. of Computer Engineering, Yeungnam University

요 약

이전에 쿠쿠 샌드박스(Cuckoo Sandbox)에서 가지고 있었던 가상환경의 분석환경시스템에서 실머신 기반에서 분석이 가능하도록 구현하는 과정에서 네트워크 덤프(Network Dump)와 관련된 문제가 존재한다. 이런 문제를 해결하기 위해 Server PC와 실머신을 NAT(Network Address Translation)를 사용하여 해결할 수 있는지 알아보고 분석한 결과를 가상머신으로 분석한 결과와 비교하여 차이점이 있는지 알아보고자 한다.

1. 서론

이전 쿠쿠 샌드박스(Cuckoo Sandbox)의 시스템에서는 Vmware, VirtualBox, KVM 등과 같은 가상머신 소프트웨어를 이용하여 가상머신위에서 악성코드를 동적분석을 하게 되고, 가상머신 안에서 악성코드가 동작하였던 내용들을 Cuckoo Sandbox로 정보를 전송하여 악성코드의 행위에 대해서 분석할 수 있었다. 하지만 이러한 방법은 분석하고자 하는 악성코드 안에 가상머신을 탐지하는 VMDetect 기술이 적용되어 있다면, 실제 분석자가 원하는 정보를 얻을 수 없게 된다. 이러한 문제를 해결하기 위하여, 가성머신 기반이 아닌 실머신 기반에서 악성코드를 분석하고자 기존 Cuckoo Sandbox에서 Real 머신기반 분석환경을 추가 하고자 하였다. 이 과정에서 문제가 발생하게 되는 문제점들이 있다. 기존 실머신은 공공 네크워크를 사용하여 실머신을 구동하였으나, 이것을 가상머신과 좀더 동일한 환경을 만들기 위하여 NAT(Network Address Translation)을 사용하여 가상머신이 Virtual Network를 이용하듯이 Server PC와 실머신을 내부 네트워크로 연결한다.

본 논문은 먼저 현재 문제점에 대해서 소개하며, 이 문제에 대한 해결을 위한 방법에 대해서 이야기하고, 가상머신의 분석과 실머신 분석 결과의 차이를 분석하여, 결론으로 끝을 맺는다.

2. 네트워크 덤프 문제

현재 Cuckoo Sandbox에서는 네크워크 구성이 Server PC와 실머신 둘다 공공 네트워크로 연결 되어 있다. 이것을 기존 Cuckoo Sandbox가 Virtual Network를 이용하여 가상머신으로 악성코드를 분석하는 것과 유사한 환경을 만들어주기 위해서 NAT(Network Address Translation)를 사용할 것이다.

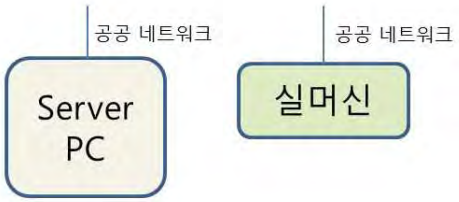

그림 1 기존의 네트워크 구성

3. 네트워크 덤프 문제 해결 방법 : NAT 사용

NAT(Network Address Translation)을 구성하기 위해서는 Server PC에 랜카드가 2개와 HUB가 필요하다. 먼저 Server PC에 network/interface 파일에 ip주소를 static으로 설정해준다. eth0은 외부와 연결 되도록 하고 eth1은 내부와 연결되고 ip주소는 192.168.0.1을 사용한다. 그리고 실머신의 ip주소도 192.168.0.2로 변경시켜 준다. 그 다음 Server PC의 iptables 설정을 nat가 가능하도록 바꿔준다. 바꿔준 내용은 reboot 하면 사라지므로 파일로 저장하여 network/interface에 추가하여 reboot 되어도 자동으로 설정되도록 해준다..

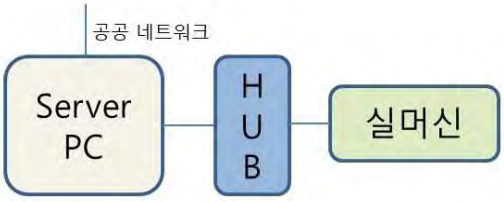

그림 2 NAT를 사용한 네트워크 구성

4. 가상머신과 실머신의 분석 결과 네트워크 부분의 차이점

악성코드를 기존 가상머신에서 분석한 결과와 실머신에서 분석한 결과의 차이점을 보면 가상머신의 분석결과는 그림 3과 그림 4와 같이 Host Involved 정보를 보면 IP Address 에서 DNS server의 주소는 각각 가상머신(168.126.63.1)과 실머신(165.229.11.5와 .8)로 다르고 분석된 주소는 201.7.184.2로 동일한것을 볼 수 있다. 다음 DNS Request 정보를 보면 실머신에만 skydata.co.kr 이라는 Domain을 참조하는데 이것은 실머신에 설치된 복구프로그램으로 이것을 제외하면 가상머신과 실머신 모두 www.codex.kit.net을 참조하는것은 동일하다. 결과적으로 가상머신과 실머신의 분석 결과 네트워크 부분은 별다른 차이점 없이 동일한 것을 알 수 있다.

Hosts Involved

IP Address
168.126.63.1
201.7.184.2

DNS Requests

Domain	IP Address
www.codex.kit.net	201.7.184.2

그림 3 가상머신 통한 분석 결과

Hosts Involved

IP Address
165.229.11.5
165.229.11.8
239.255.255.250
201.7.184.2

DNS Requests

Domain	IP Address
liveinfo.skydata.co.kr	
liveupdate.skydata.co.kr	
www.codex.kit.net	201.7.184.2

그림 4 실머신을 통한 분석 결과

5. 기대 효과 및 결론

본 논문에서 제안한 NAT 기반의 네크워크 구성은 사설 IP의 사용으로 한정된 공인 IP주소의 사용을 절약 할 뿐만 아니라 내부에서는 사설 IP주소만 사용하도록 하여 외부 침입자가 침입할 수 없도록 하게 해준다. 이로써 실머신 기반의 악성코드 자동분석 시스템을 사용하여 좀 더 안전하게 악성코드를 분석할 수 있을 것으로 기대된다.

참고문헌

[1] Vmware, http://www.vmware.com
[2] Virtual Box, http://www.virtualbox.org
[3] KVM, http://www.linux-kvm.org
[4] Cuckoo, http://www.cuckoosandbox.org
[5] Detecting VMWare, http://brundlelab.wordpress.com/2012/10/21/detecting-vmware/
[6] Deep Freeze, http://www.faronics.com/products/deep-freeze/enterprise/
[7] WOL, http://en.wikipedia.org/wiki/Wake-on-LAN