파일 싱크 서비스를 이용한 모바일 봇넷

Mobile Botnet Exploiting File Sync Services

저자
(Authors)

한기문, 김대혁
Ki-Moon Han, Daehyeok Kim

출처
(Source)

한국컴퓨터정보학회 학술발표논문집 22(2), 2014.7, 55-56 (2 pages)
Proceedings of the Korean Society of Computer Information Conference 22(2), 2014.7, 55-56 (2 pages)

발행처
(Publisher)

한국컴퓨터정보학회
The Korean Society Of Computer And Information

URL

http://www.dbpia.co.kr/Article/NODE06603102

APA Style

한기문, 김대혁 (2014). 파일 싱크 서비스를 이용한 모바일 봇넷. 한국컴퓨터정보학회 학술발표논문집 , 22(2), 55-56.

한국컴퓨터정보학회 하계학술대회 논문집 제22권 제2호 (2014. 7)

파일 싱크 서비스를 이용한 모바일 봇넷

한기문°, 김대혁*
°*한국과학기술원 사이버보안연구센터
e-mail:{linuzen, dhkim7}@kaist.ac.kr*°

Mobile Botnet Exploiting File Sync Services

Ki-Moon Han°, Daehyeok Kim*
°*Cyber Security Research Center, KAIST

● 요 약 ●

모바일 장치의 대중화와 이동 통신 기술의 발전이 가속화 되면서, 최근 모바일 봇넷으로 인한 위협이 증가하고 있다. 봇넷의 안정적인 유지와 봇 마스터와 클라이언트 간 통신 채널의 은닉성을 보장하기 위해 다양한 방법이 연구되었다. 본 논문에서는 모바일 환경에서 널리 사용되는 클라우드 기반의 파일 싱크 서비스를 통신 채널로 활용한 새로운 봇넷을 제안한다. 안드로이드 플랫폼 기반의 봇 클라이언트 구현과 실험을 통해 제안하는 봇넷이 사용하는 C&C 채널의 은닉성을 검증하고 공격의 심각성을 보였다.

키워드: 모바일 봇넷(Mobile botnet), C&C 채널(C&C channel), 파일 싱크 서비스(File sync service)

I. 서 론

봇넷(botnet)은 공격자에 의해 감염된 장치들로 이뤄진 네트워크로써 스팸 메일이나 악성 코드 유포에 사용되거나 분산형 서비스 거부 공격(DDoS)과 같은 대규모 사이버 공격에 사용된다. 최근 스마트폰과 같은 모바일 장치 사용의 증가로 기존에 PC들로만 구성되었던 봇넷이 모바일 클라이언트를 활용한 봇넷으로 진화하고 있다.

악성 코드나 스미싱 문자메시지 등으로 사용자의 모바일 장치에 설치된 봇 클라이언트는 공격자인 봇 마스터에게 공격에 필요한 클라이언트 측 정보를 제공하고 봇 마스터로부터 공격 명령을 주기적으로 수신한다. 이를 위해서는 다수의 봇 클라이언트와 이를 통제하는 봇 마스터간의 효율적인 연결유지와 은닉 Command and Control(C&C) 채널의 확보가 중요하다.

봇 클라이언트 간 혹은 봇 클라이언트와 마스터 간채널의 은닉성을 제공하기 위해 일반적으로 많이 사용되는 인터넷 프로토콜인 IRC, HTTP, DNS 등을 활용해 공격 트래픽 탐지 장비를 우회 하거나 P2P 프로토콜과 같은 분산형 통신 채널을 사용하여 중앙 봇 마스터의 노출을 방지 하는 등 다양한 방법으로 진화하였다.

특히 모바일 환경에서 안정적이고 은닉성을 보장하는 C&C 채널을 제공하기 위해 블루투스, 문자메시지(SMS), 그리고 푸쉬 알림 서비스를 사용 하는 등 다양한 방법들이 제안되었다. 제안된 방법들은 모바일 환경에 적합한 프로토콜과 서비스를 활용하지만 은닉성과 확장성에서 한계점을 가진다.

본 논문에서는 모바일 환경에서 널리 사용되고 있는 클라우드 기반의 파일 싱크 서비스를 사용한 실용적인 C&C 채널을 소개하고 이것의 실현 가능성과 심각성에 대해 소개한다. 클라우드 기반의 파일 싱크 서비스는 모바일 디바이스의 저장 공간을 유연하게 해주고 편리한 데이터 공유를 가능하게 하여 많은 사용자를 확보하고 있는 서비스이다. 본 논문에서는 이들 서비스 중 Dropbox의 공개 API를 활용한 봇넷 공격 모델을 제시하고 안드로이드 기반의 실험을 통해 공격의 실용성에 대해 보인다.

II. 시스템 설계

2.1. 공격 모델

본 논문에서 가정하는 공격 모델은 다음과 같다. 사용자의 모바일 장치에는 봇 클라이언트 역할을 수행하는 악성 프로그램이 설치되어 있다고 가정한다. 이 프로그램은 Dropbox API를 사용하여 봇 마스터와 메시지 전송을 위한 통신 채널을 개설한다. 봇 클라이언트와 봇 마스터는 공격 및 제어 메시지를 주고받기 위해 제안하는 Dropbox를 활용한 C&C 채널을 사용한다. 본 논문은 새로운 C&C 채널을 통해 공격 메시지를 은밀히 전송할 수 있음을 보이는데 중점을 둔다.

2.2. 공격 프로토콜

Dropbox는 대표적인 클라우드 기반 파일 싱크 서비스로 Dropbox Sync API[1]를 제공해 여러 기기 간의 자료 동기화가 쉽게 가능하다. 이 API를 사용한 봇 클라이언트와 마스터는 다음과 같이 동작한다.

공격자는 C&C채널로 사용하기 위해 개설한 Dropbox 계정의 특정 폴더에 메시지가 담긴 파일을 업로드 한다. Dropbox Sync API를 사용하는 봇 클라이언트는 공격자 폴더가 업데이트되는 즉시 해당 파일명을 확인하여 명령을 수행하게 된다.

명령 파일 이름의 구조는 *[명령어_인자값].txt*로 명령이 파일명에 나타나 있다. 가능한 명령어에 대한 설명은 표 1과 같으며, 명령어와 인자값 정보를 바탕으로 봇 클라이언트는 공격을 수행한다.

III. 구현 및 실험 결과

3.1. 구현

제안하는 C&C 채널을 사용하는 모바일 봇 클라이언트 프로그램을 안드로이드 플랫폼 버전 4.4.2에서 구현하였다. 구현된 봇 클라이언트 프로그램은 Dropbox의 Sync API[1]를 사용하여 봇 마스터가 2.2절에 소개한 메시지 형태로 Dropbox 저장소에 업데이트하는 공격 메시지를 확인하도록 설계되었다. Dropbox의 Sync API를 활용하여 새로운 공격 메시지가 업데이트 되는 즉시 모바일 봇 클라이언트와 동기화가 될 수 있도록 구현하였다.

3.2. 실험 결과

제안하는 C&C 채널의 은닉성을 평가하기 위해 메시지를 동기화하는데 발생하는 네트워크 트래픽을 패킷 수집 도구인 tcpdump를 사용해 분석했다. 안드로이드 플랫폼에서 동작하는 Dropbox 공식 프로그램과 제안하는 봇 클라이언트 프로그램에서 4개의 명령 메시지를 동기화 시킬 때 발생하는 네트워크 트래픽을 분석하였다. 메시지 파일명은 2.2절에서 소개한 형태를 따르고 파일 본문은 없다.

분석 결과 Dropbox 프로그램과 봇 클라이언트는 동기화를 위해 api.dropbox.com 및 api-notify.dropbox.com 서버와 통신하며 패킷을 송수신 했다. 또한 모든 트래픽이 SSL로 암호화되어 있어 트래픽의 컨텐츠나 흐름 분석으로는 봇 클라이언트가 발생시키는 트래픽을 구분하기 어려운 것을 확인했다.

표 1. 명령어 목록
Table 1. Command List

명령어	GET	PUT	DEL	EXEC
의미	다운로드	업로드	삭제	실행

IV. 관련 연구

모바일 봇넷을 위한 안정적인 C&C 채널을 제공하기 위해 다양한 연구가 진행되었다. SMS를 C&C 채널로 사용한 봇넷[2, 3]은 중앙집중형과 분산형 구조로 제안되었다. 대규모의 봇넷에 SMS를 활용한 채널이 사용되면 과금으로 인한 오버헤드와 통신사의 컨텐츠 분석에 의해 공격이 무력화 될 수 있는 한계가 있다. 블루투스를 통신 채널로 사용하는 봇넷[4]은 독립된 채널을 사용하여 탐지를 우회할 수 있지만 블루투스 자체의 통신 거리 제약 때문에 확장성에 한계를 가진다. 이들과 비교해 제안하는 봇넷 구조는 널리 사용되고 있는 클라우드 기반 서비스를 활용해 높은 은닉성을 가진 C&C 채널을 제공하고 봇넷의 확장성도 보장한다.

V. 결 론

본 논문에서는 클라우드 기반 파일 싱크 서비스인 Dropbox를 활용한 모바일 봇넷 C&C 채널을 제안했다. 제안된 채널은 널리 사용되고 있는 서비스의 통신 채널을 활용하기에 높은 은닉성을 제공한다. 현재 광범위한 실험을 통한 성능 검증을 진행 중에 있다. 또한 Google Drive를 포함한 기타 파일 싱크 서비스 기반의 봇넷 채널을 구현 및 검증 할 계획이며 이 공격법에 대한 방어책에 대해 연구 중에 있다.

참고 문헌

[1] Dropbox-Sync API,[online] *https://www.dropbox.com/developers/sync*

[2] Y. Zeng et al., "Design of SMS commanded-and-controlled and P2P structured mobile botnets," ACM Conference on Security and Privacy in Wireless and Mobile Networks, Apr. 2012.

[3] C. Mulliner et al., "Rise of the ibots: 0wning a telco network," International Conference on Malicious and Unwanted Software, Oct. 2010.

[4] K. Singh et al., "Evaluating bluetooth as a medium for botnet command and control," DIMVA, Jul. 2010.