# 사회공학과 악성코드를 이용한 단말침투 및 정보수집 방법에 대한 연구

이현우*, 윤호상**, 신동일*, 신동규*
*세종대학교 컴퓨터공학과
**국방과학연구소
e-mail:whl1260@gce.sejong.ac.kr

# A Study on the Penetration and Information Collection Method using Social Engineering and Malicious Code

Hyunwoo Lee*, Hosang Yooun**, Dongil Shin*, Dongkyoo Shin*
*Dept. of Computer Engineering, Sejong University
**Agency for Defense Development

요 약

제 4차 산업이 다가오는 이 시점에서 보안이 잘 갖추어진 네트워크 조직에서도 사람과 PC와 같은 단말에 대한 취약점이 드러나면 결국 네트워크 전체가 무너질 수 있다. 그러므로 단말에 대한 보안이 중요시되고 있다. 암호화된 장비를 갖추거나 물리적 망 분리를 한다하여도 사회공학을 통한 보안 위협은 여전히 존재하고 있기 때문이다. 본 논문에서는 사회공학을 통해 사람과 PC와 같은 단말을 통해 침투하고 악성코드를 유포하여 공격 대상의 정보를 수집하는 방법에 대하여 연구한다.

## 1. 서론

정보기술이 발달함에 따라 제 4차 산업이 다가오고 있는 이 시점에서 보안의 필요성이 두각을 나타낸다. 인터넷을 통해 악의적인 콘텐츠가 손쉽게 유통될 수 있는 구조가 되면서, IT 자산에 대한 보호가 점차 어려워지게 되었다 [1]. 기존에 사용되고 있는 악성코드와 사회공학이 기계학습, 데이터마이닝 등 최첨단 기술들과 접목되어 고도화된 보안 위협요소가 되고 있다. 특히 보안의 가장 취약한 사람을 대상으로 하는 공격들이 많이 나타난다.[2] 따라서 본 논문에서는 사회공학과 악성코드를 조합하여 사람과 PC와 같은 단말로의 침투 및 이를 통한 정보수집 방법에 대한 연구를 진행하고 보안을 위협하는 공격 방법론에 대해서 제시한다.

본 논문의 구성은 2장에서 실제 사용되고 있는 사회공학과 악성코드의 방법 및 원리를 분석하고 3장에서 분석한 방법들을 이용한 단말침투 및 정보수집 방법에 대해 공격 방법론을 제시하고 4장에서 결론과 향후 연구방향을 제시하였다.

## 2. 관련연구

### 2. 1 사회공학

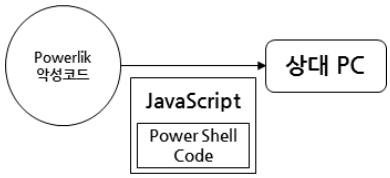
사회공학(Social Engineering)은 컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여, 정상 보안 절차를 깨뜨리고 비 기술적인 수단으로 정보를 얻는 행위이다.[3] 쉽게 말하면 악성코드와 같은 PC의 리소스를 파괴하거나 서버의 서비스를 중단하는 공격 기법과는 다른 형태로 보안에 가장 취약한 사람을 대상으로 어깨너머로 훔쳐보기, 휴지통 뒤지기, 피싱(phishing), 스미싱(smishing, SMS phising), 파밍(pharming) 등 사람을 이용하여 정보를 획득하는 형태이다. 사회공학은 인간 기반과 컴퓨터 기반으로 나눌 수 있다. 인간 기반 사회공학은 인간관계를 이용하여 직접 접근하여 정보를 획득하거나 유, 무선 통화를 도청하는 등 대상이 인간이 된다. 반대로 컴퓨터 기반 사회공학은 위조된 이메일을 보내 공격 대상의 정보를 획득하는 피싱, DNS 스푸핑(spoofing)을 이용하여 공격 대상의 신용 및 금융 정보를 획득하는 파밍, 실제 있는 사람 또는 기업을 사칭하여 링크 접속을 유도한 뒤 개인 정보를 획득하는 스미싱 등이 있다.

최근의 사이버 공격은 정찰, 준비, 표적화, 추가 접속, 데이터 수집, 그리고 유지 등의 단계를 통해 이루어진다.[4] 이러한 형식의 공격 행위는 지능형 지속 공격, 즉 APT(Advanced Persistent Threat)이다. APT는 해커가 다양한 보안 위협을 만들어 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격을 뜻한다.[5] APT는 하나의 공격 방법, 수단이 아니라 특정 대상을 목표로 다양한 해킹 기술을 이용해 지속적으로 공격하는 행위를 뜻한다.

### 2. 2 Powerlik

악성코드는 수행하는 행위에 따라 탐지 및 차단하는 기법이 달라질 수 있다.[6] Powerlik은 2014년에 등장한 파일리스(Filelsee) 악성코드이다. 윈도우 레지스트리 값에 악의적인 코드를 삽입 후 감염시키는 방식이다. 구체적인 감염 방식은 Run 레지스트리 키에 악성코드를 삽입하고 JScript.Encode 스크립트와 PowerShell 스크립트를 순서대

로 실행시킨다. 최종적인 목표는 PowerShell 스크립트가 악의적인 쉘 코드를 실행하여 dllhost.exe 프로세스에 코드를 삽입한 뒤 사용자의 PC 정보를 원하는 C&C 서버로 전송한다.



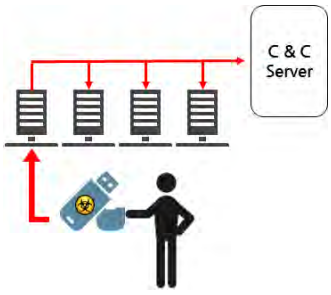

(그림 1) Powerlik 악성코드 형태

(그림 1)과 같이 Powerlik 악성코드는 Power Shell 코드가 담겨있는 자바 스크립트를 인코딩하여 상대 PC에 유포하여 감염시킨다.

## 3. 본론

### 3.1 단말 침투 방법

상대 PC의 침투하는 강력한 방식 중 하나는 사회공학 방식이다. 국내의 대표적 사례로 농협 대란은 2011년 4월 농협 전산망에 있는 자료가 대규모로 손상되어 수일에 거쳐 서비스가 마비되는 사건이 있었다. 감염 원인은 외주업체 직원이 2010년 9월에 카페에서 받은 웹 하드 무료 다운로드 쿠폰으로 업무 노트북에 영화를 다운받는 과정에서 악성코드가 심어진 것이다. 악성코드는 7개월 동안 잠복해있었고 최고위관리자의 비밀번호 등 각종 중요한 정보들을 탈취하였다. 즉 APT 형식의 공격이다.

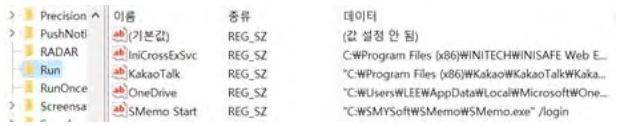



(그림 2) USB를 통한 APT

(그림 2)는 USB에 악성코드를 심어 사용자에게 유포하는 방식이다. 2.2에서 분석한 Powerlik 악성코드를 USB에 심어 공격대상 기업직원 또는 개인에게 무료로 제공한다. USB를 받은 직원 또는 개인은 사내에서 쓰는 업무용 노트북이나 PC 또는 개인의 PC에서 USB를 이용하게 만들어 악성코드를 감염시킨다. 감염시키는 방법은 호기심을 유발할 문서 파일을 이용하는 것이다. 문서 파일인 PDF, HWP, DOC에서 제공하는 매크로 기능을 활용해 사용자의 PC에 악성코드를 삽입한다. 하지만 문서파일은 기본적으로 매크로가 비활성화 상태로 있기 때문에 중요해 보이는 본문 내용을 약간 흐리게 처리한 뒤 매크로 기능을 활성화 시켜야 본문 내용을 확인 할 수 있게끔 유도하여 매크로 기능을 활성화 시킨다. 활성화된 매크로는 레지스트리에 인코딩된 악성코드를 삽입시킨다.

### 3.2 정보수집 방법

정보수집은 Powerlik 악성코드를 이용한다. 단말 침투 방법에서 제안한 USB 유포 방식과 매크로 감염 방식을 통해 악성코드를 삽입한다.




(그림 3) 악성코드를 삽입 할 레지스트리 경로

(그림 3)은 악성코드가 삽입되는 레지스트리 경로이다. Run 레지스트리는 OS가 실행될 때 자동으로 프로그램이 시작되는 경로를 넣어주는 곳이다. (기본값) 의 데이터에 인코딩된 스크립트를 삽입한다. JScript.Encode 스크립트는 PowerShell 스크립트를 갖고 있다.

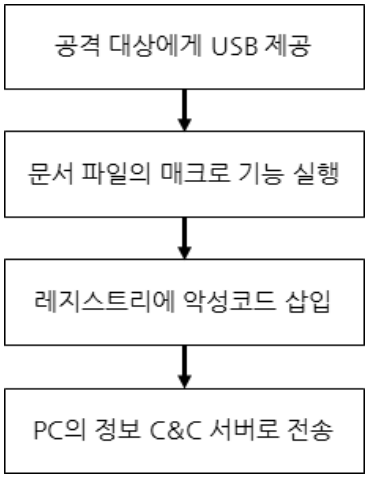
<표 1> 정보수집 코드

| 시스템의 UUID | Windows 버전 |
|---|---|
| PUSH EBP<br>MOV EBP,ESP<br>SUB ESP,10<br>PUSH ESI<br>LEA EAX,[LOCAL.4]<br>PUSH EAX<br>CALL DWORD PTR DS:[10003098]<br>MOVZX EAX,BYTE PTR SS:[EBP-1]<br>PUSH EAX<br>MOVZX EAX,BYTE PTR SS:[EBP-2]<br>PUSH EAX<br>MOVZX EAX,BYTE PTR SS:[EBP-3]<br>PUSH EAX<br>MOVZX EAX,BYTE PTR SS:[EBP-4]<br>PUSH EAX<br>MOVZX EAX,BYTE PTR SS:[EBP-5]<br>PUSH EAX<br>MOVZX EAX,BYTE PTR SS:[EBP-6]<br>PUSH EAX<br>PUSH malware.10003210<br>PUSH 103<br>MOV ESI,malware.1232A648<br>PUSH ESI<br>CALL DWORD PTR DS:[10003114]<br>ADD ESP,24<br>MOV EAX,ESI<br>POP ESI<br>LEAVE<br>RETN | PUSH EBP<br>LEA EBP,DWORD PTR SS:[ESP-78]<br>SUB ESP,9C<br>PUSH 98<br>LEA EAX,[LOCAL.8]<br>PUSH 0<br>PUSH EAX<br>MOV [LOCAL.9],9C<br>CALL malware.1000236A<br>ADD ESP,0C<br>LEA EAX,[LOCAL.9]<br>PUSH EAX<br>MOV BYTE PTR DS:[ESI],0<br>CALL DWORD PTR DS:[10003070]<br>TEST EAX,EAX<br>JE SHORT malware.1000210C<br>MOVZX EAX,WORD PTR SS:[EBP+72]<br>PUSH EAX<br>MOVZX EAX,WORD PTR SS:[EBP+70]<br>PUSH EAX<br>PUSH [LOCAL.6]<br>PUSH [LOCAL.7]<br>PUSH [LOCAL.8]<br>PUSH malware.100031F8<br>PUSH 103<br>PUSH ESI<br>CALL DWORD PTR DS:[10003114]<br>ADD ESP,20<br>MOV EAX,ESI<br>ADD EBP,78<br>LEAVE<br>RETN |

<표 1>은 공격 대상의 다양한 PC 정보를 수집하는 코드이다. 시스템의 UUID와 Windows 버전을 획득할 수 있고 C&C서버로 HTTP 통신을 통해 데이터를 전송하면 정보수집이 완료된다.

### 3.3 공격 방법론

3.1과 3.2에서 분석한 방법들을 활용하여 전체적인 단말침투 및 정보 수집을 할 수 있게 되었다. 전체적인 프로세스는 (그림 4)와 같이 진행된다.




(그림 4) 침투 및 수집 과정

처음 단계는 침투과정으로써 실제 있는 개인 또는 기업을 사칭하여 공격대상에게 악성코드가 심어진 무료 USB를 제공한다. 그 다음 단계는 사용자의 호기심을 끄는 문서 파일을 통해 매크로 기능을 활성화시킨다. 활성화된 매크로가 사용자 PC의 레지스트리에 인코딩된 악성코드가 삽입한다. 삽입된 악성코드는 PC의 정보를 획득하여 지정된 C&C 서버로 데이터를 전송하게 된다. 이로써 사용자의 PC는 사회공학과 악성코드를 통해 감염되었다.

## 4. 결론 및 향후과제

본 논문에서는 사회공학과 Powerlik 악성코드를 활용하여 상대 PC를 대상으로 정보를 획득할 수 있는 가능성을 보았다. 보안이 중요시되고 있는 현대 사회에서 컴퓨터에 대한 보안의식과 물리적인 보안 강화에 힘을 써야 할 것이다. 향후 연구과제로는 Powerlik 악성코드의 원리를 활용하여 쉘 코드를 통해 파일을 다운받는 기능도 구현할 수 있기 때문에 다양한 악성코드를 심어 많은 데이터를 획득할 수 있고 더 나아가 같은 네트워크에 있는 PC들도 접근할 수 있는 좀 더 확장되고 다양한 방식의 연구가 필요할 것으로 예상된다.

## Acknowledgement

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD160066BD).

## 참고문헌

[1] 김지훈, 조시행. (2010). 사이버 환경에서의 보안위협. 정보보호학회지, 20(4), 11-20.
[2] 임민철. “보안 시작-끝은 결국 사람”...안랩 2017 위협 전망. ZDNet Korea. 2017. 01. 03.
[3] 양대일. 「정보 보안 개론」. 한빛아카데미(2013). p499
[4] 김영수, 김익균. (2013). 최근의 사이버 공격 동향과 지능형 보안. 한국정보과학회 학술발표논문집,718-719.
[5] 김환표. 「트렌드 지식사전2」. 인물과상사(2014).
[6] 강부중, 한경수, 임을규. (2012). 악성코드 현황 및 탐지 기술. 정보과학회지, 30(1), 44-53.