정 보 보 호 학 회 지
제27권 제3호, 2017. 6

금융정보를 탈취하는 파밍 악성코드 분석 및 대응방안

이 세 빈*, 이 지 오*, 염 흥 열*

요 약

최근 많은 사용자가 인터넷을 통해 수많은 웹페이지에 접속하고 정보를 수집하면서 인터넷의 사용량이 증가한 만큼 악성코드에 감염될 확률은 증가하고 있다. 공격자들은 웹을 통해 사용자들의 정보탈취를 목적으로 악성코드를 유포하는데 그 중 파밍 (pharming) 악성코드를 통해 금융정보 탈취를 하고 있다. 파밍 악성코드에 감염된 사용자들은 웹페이지에 접속 시 원래 페이지가 아닌 공격자가 만든 파밍 페이지로 유도되어 금융정보 및 공인인증서가 유출된다. 유출된 금융정보를 통해 사용자들은 심각한 금전적인 피해가 발생할 수 있다. 본 논문에서는 최근 파밍 악성코드를 통해 금융정보를 유출하는 방법에 대해 분석하고 대응방안을 제시한다.

Ⅰ. 서 론

최근 인터넷의 발전을 통해 많은 사용자가 인터넷을 통해 수많은 웹페이지에 접속하고 정보를 수집한다. 인터넷을 사용하는 사용자들이 증가한 만큼 공격자들은 이러한 사용자들을 타겟으로 한 공격도 증가하고 있다. 악성코드를 유포하는데 다양한 방법을 사용하는데 그 중 웹페이지에 접속만 해도 악성코드에 감염되는 드라이브 바이 다운로드(Drive-by-Downlo ad) 공격이 존재한다. 드라이브 바이 다운로드 공격은 자바, 어도비 플래쉬 플레이어와 같은 어플리케이션의 취약점을 이용하여 악성코드를 다운로드하고 실행해 사용자의 PC에 악성코드를 감염시킨다. 사용자가 웹페이지에 접속만 해도 감염되고 사용자는 악성코드에 감염에 된 것을 인지하기 힘들기 때문에 사용자들의 방문이 많은 웹페이지에 드라이브 바이 다운로드 공격을 통한 악성코드를 유포하게 된다면 대량의 악성코드 감염이 발생할 수 있기 때문에 매우 위험한 공격이다[1].

드라이브 바이 다운로드 공격을 통해 감염되는 악성코드 중 사용자에게 금전적인 피해를 주는 악성코드는 대표적으로 파밍 악성코드와 랜섬웨어 악성코드가 존재한다. 그 중 파밍 악성코드는 국내 인터넷 서비스 사용자의 금융 정보를 주로 노리는 악성코드이다. 파밍 악성코드는 감염된 사용자가 웹페이지에 접속 시 정상적인 웹페이지가 아닌 공격자가 제작한 파밍 페이지로 접속을 유도하고 있다. 공격자는 유포하고 있는 파밍 악성코드의 탐지 되는 것을 막고 사용자가 금융정보를 입력하도록 점점 지능적인 방법을 통해 금융정보를 탈취해 심각한 금전적인 피해를 입힐 수 있어 주의가 필요하다[2].

본 논문에서는 사용자의 금융정보를 노리는 파밍 악성코드의 유포방식 및 금융정보를 탈취하는 방법에 대해 분석하며 대응방안을 제시한다.

Ⅱ. 파밍 악성코드 유포 과정

공격자가 파밍 악성코드를 유포하는 방법은 드라이브 바이 다운로드 공격, 애드웨어를 통한 감염 등 다양한 방법이 존재한다. 그중 드라이브 바이 다운로드를 통해 유포하는 과정에 대해 설명한다.

2.1. 드라이브 바이 다운로드

드라이브 바이 다운로드(Drive-by-Download)는 웹사이트 접속만으로 사용자의 동의 없이 악성코드에 감염되게 하는 악성코드 유포 기법을 말한다. 이 기법은 웹사이트에 존재하는 응용프로그램의 취약점을 공격함

본 연구는 미래창조과학부와 IITP의 정보통신·방송 연구개발사업의 일환으로 수행하였음.[R0190-16-2054]. (과제명 : 타인도용이 불가능한 생체신호 기반의 웨어러블 본인인식 기술개발)
* 순천향대학교 정보보호학과 (tkaqls12@gmail.com, myjiolee11@gmail.com, hyyoum@sch.ac.kr)

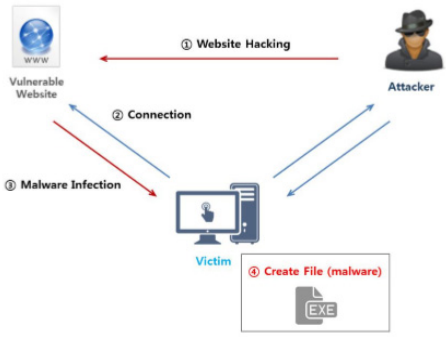
으로 악성코드 유포가 이루어지게 된다. 여기서 사용되는 응용프로그램은 어도비 플래시 플레이어, 실버라이트, 오라클 자바 등이 존재하며 드라이브 바이 다운로드 공격에서는 해당 프로그램들에 대한 취약점을 공격하게 된다. 따라서 인터넷 서비스 사용자가 어플리케이션이 갖는 취약점을 패치하는 업데이트를 실행하지 않은 어플리케이션을 이용하고, 해커가 공격한 특정 웹사이트에 접속하게 된다면 사용자의 동의 없이 악성코드에 감염되며, 사용자 PC에서 악의적인 행위가 동작하게 된다[3].

드라이브 바이 다운로드는 특별한 과정 없이 발생하기 때문에 대다수는 사용자는 악성코드에 감염되는 것을 인지할 수 없기 때문에 효과적인 악성코드 유포 기법으로 다양한 악성코드에서 이용되고 있다. 드라이브 바이 다운로드는 외부 사이트 참조 및 경유/유포 사이트, 자바스크립트 난독화, 익스플로잇 킷이 유기적으로 결합된 형태로 해커가 공격을 시도하기 쉽다는 이유도 존재한다.

해당 기법에서 사용되는 익스플로잇 킷(Exploit Kit)이란 응용프로그램의 취약점을 공격하는 취약점 코드 및 악성코드 유포 사이트 등에 대한 정보를 가지고 있으며, 해당 도구를 이용하여 자동으로 웹사이트 취약점을 공격하게 된다. 이러한 익스플로잇 킷은 매우 정교하고 자동화되어 사이버 범죄자들이 이용하기 쉬우며, 블랙마켓을 통해 구하기도 간편하여 악성코드 유포 파급력 이외에 드라이브 바이 다운로드 기법이 애용되는 이유로 평가된다[4].

드라이브 바이 다운로드의 동작 과정은 [그림 1]와 같으며, 크게 4단계로 구분할 수 있다.

1) 공격자는 악성코드의 파급력을 높이기 위해, 방문자가 많고 취약한 웹사이트를 해킹하여 악의적인 코드를 삽입한다.
2) 업데이트되지 않은 취약점을 가지고 있는 인터넷 서비스 사용자는 해킹된 웹사이트에 접속한다.
3) 해킹된 페이지에 존재하는 악의적인 코드로 인해 여러 경유지 사이트와 악의적인 콘텐츠를 포함한 페이지로 연결하며, 악의적인 콘텐츠에 있는 취약점 공격코드를 실행한다.
4) 웹페이지에 접속한 사용자 PC에 사용자의 동의가 없어도 악성코드를 생성하고 실행한다[2].



〔그림 1〕 드라이브 바이 다운로드 감염 과정〔3〕

Ⅲ. 파밍 악성코드를 통한 정보탈취 분석

본 장에서는 파밍 악성코드 분석을 통해 감염 PC의 금융정보 탈취를 위해 파밍 페이지 유도 및 공인인증서 탈취를 위해 사용한 방법에 대해 제시한다.

3.1. 파밍 악성코드

파밍(Pharming) 악성코드는 악성코드의 한 종류로서, 감염된 피해자의 hosts 파일 조작, DNS조작 및 프록시를 통해 원본 사이트에 접속 시 유사하게 제작된 파밍 사이트로 접속을 유도해 사용자가 입력한 계정정보 및 금융정보를 탈취하는 악성코드이다[5].

3.2. 파밍 페이지 유도를 통한 금융정보 탈취

파밍 악성코드의 종류마다 수행하는 기능이 다르기 때문에 본 논문에서는 최근 유포되는 파밍 악성코드에서 수행되는 기능에 대해 분석한다.

파밍 악성코드에 감염되면 사용자가 웹페이지 접속 시 원본페이지가 아닌 파밍 페이지로 유도하기 위한 IP 주소를 획득하기 위해 특정 웹사이트로 연결을 요청한다. 특정 웹사이트로 연결을 요청해 받아온 통신 데이터에서 IP 주소 파싱을 통해 사용자가 웹사이트로 접속 시 해당 IP주소로 접속하도록 유도해 원본 사이트가 아닌 파밍 페이지로 접속된다. 와이어샤크를 통해 해당 통신 패킷의 데이터를 확인하면 [그림 2]와 같이 “r.pengyou.com” 주소로 특정 GET 요청을 전송한다. 요청이 성공하면 통신에 대한 응답으로 공격자의 IP주소가 포함된 데이터를 받는 것을 확인할 수 있다. 이후

```
GET /fcg-bin/cgi_get_portrait.fcg?uins=28[illegible] HTTP/1.1
Host: r.pengyou.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36

HTTP/1.1 200 OK
Server: QZHTTP-2.38.18
Cache-Control: max-age=86400
Content-Type: text/html
ETag: "141090184"
Date: Sat, 22 Apr 2017 11:22:25 GMT
Content-Length: 126
Connection: keep-alive

portraitCallBack({"2889622357":["http://qlogo2.store.qq.
com/qzone/2889622357/28[illegible]",78,-1,0,0,0,"[illegible].212",0]})
```

〔그림 2〕 통신을 통한 파밍 페이지 IP주소 획득

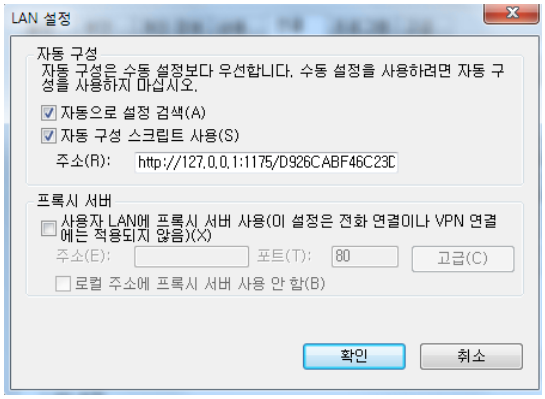
사용자가 웹페이지에 접속 시 정상페이지의 IP주소가 아닌 해당 주소로 접속하게 된다.

파밍 악성코드에서 웹페이지에 접속 시 공격자의 서버주소로 유도하는 대표적인으로 사용자의 hosts 파일을 변조해 유도하는 방법, DNS 주소를 변조하는 방법과 PAC(Proxy Auto-Config)를 이용한 기법 등 다양한 기법이 존재한다. 최근 파밍 악성코드에서 자주 사용되는 PAC를 통해 파밍 페이지로 유도하는 방법 대해 제시한다[6].

PAC는 웹브라우저를 통해 수동으로 프록시 설정하지 않아도 등록된 스크립트를 통해 특정 URL 접속 시 자동으로 프록시를 통해 접속할 수 있는 기능이다.[7] 악성코드에서 [그림 3]과 같이 레지스트리 조작을 통해 감염 PC의 자동 구성 스크립트 사용이 설정되어 있고 주소로 “127.0.0.1:포트/스크립트 파일명”으로 설정되어 있다. 감염 PC에서 웹페이지로 접속 요청 시 해당 스크립트를 실행하고 접속 요청한 URL이 해당 스크립트에 존재하는 URL과 일치할 때 파밍 페이지로 유도하게 되고 일치하지 않을 때 정상적인 웹페이지로 접속하게 된다[8].

PAC에 설정되어 있는 스크립트의 내용을 확인하면 난독화 되어있다. 난독화를 해제하면 [그림 4]와 같이 확인할 수 있다. 해당 스크립트에는 암호화 함수와 공격자가 파밍 페이지로 유도하려는 URL을 암호화 과정을 통해 생성한 암호문이 삽입되어 있다. 감염 PC에서 웹브라우저를 통해 URL 접속 시 접속한 URL을 암호화 과정을 통해 암호문을 생성한다. 생성한 암호문과 삽입되어 있는 암호문이 일치할 경우 정상적인 웹페이지 접속이 아닌 파밍 페이지로 접속하고 일치하지 않을 경우 정상적인 웹페이지로 DIRECT로 접속한다.

감염 PC의 레지스트리 조작을 통해 네이버 웹페이지



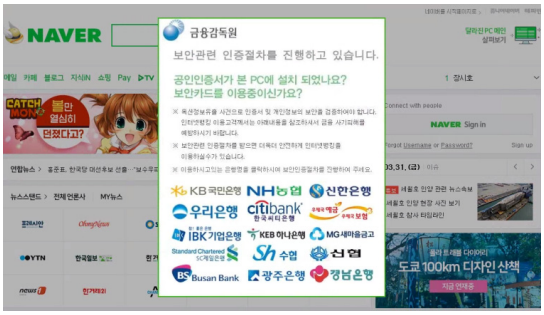
〔그림 3〕 PAC 스크립트

```
var aox = {
    "2d92cfbff": 1,
    "556a14727": 1,

     .... 생략 ....

    "b80657ee4": 1
};
var sx = "53,4f,43,4b,53,20,31,32,37,2e,30,2e,30,2e,31,3a";
var xc = "";
for (i in sx.split(',')) {
    xc += String.fromCharCode('0' + 'x' + sx.split(',')[i])
}
var aoo = xc + "1175";
var hasOwnProperty = Object.hasOwnProperty;

function FindProxyForURL(wo, osx) {
    if (hasOwnProperty.call(aox, axnak(osx))) {
        return aoo
    }
    return String.fromCharCode(68, 73, 82, 69, 67, 84, 59)
}
```

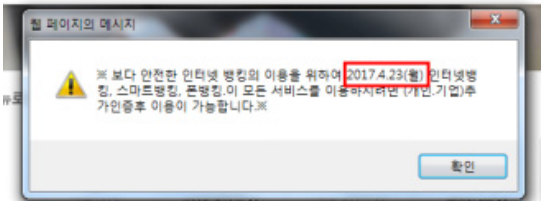
〔그림 4〕 PAC 스크립트 데이터

를 시작페이지로 등록한다. 네이버 웹페이지에 접속 시 정상적인 네이버 웹페이지가 아닌 공격자가 제작한 네이버 파밍 페이지로 접속이 유도된다. 파밍 페이지로 제작된 가짜 네이버 웹페이지는 실제 네이버 웹페이지와 매우 유사하게 제작되었으며 [그림 5]와 같이 금융감독원으로 위장해 보안 관련 인증절차를 진행하고 있다는 팝업창을 출력한다. 해당 팝업창에서는 안전한 인터넷 뱅킹을 위하여 팝업창에 출력된 은행명을 클릭하면 보안인증절차를 진행해달라는 내용이 존재하는데 해당 은행을 클릭하면 실제 은행 관련 페이지가 아닌 공격자가 제작한 파밍 페이지로 유도된다[9].

은행 관련 파밍 페이지로 접속하게 되면 [그림 6]과 같이 팝업창을 출력하는데 사용자의 금융정보를 수집하기 위해 감염 PC의 시스템 시간을 출력하며 해당 날짜



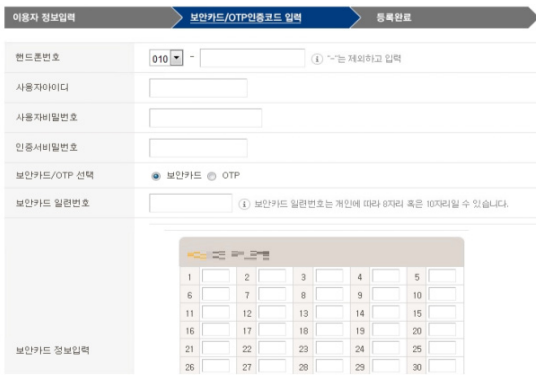
〔그림 5〕 네이버 파밍 페이지



〔그림 6〕 은행 관련 파밍 페이지 팝업창

이후에 안전한 인터넷 뱅킹을 위하여 서비스를 이용하려면 추가인증이 필요하다는 내용을 언급하면서 로그인을 통해 사용자의 금융정보 입력을 유도하고 있다.

감염 PC에서 은행 관련 파밍 페이지에 로그인 시도 시 정상적인 로그인 정보를 요청하지 않고 [그림 7]와 같이 로그인에 불필요한 정보까지 입력을 요구하고 있다. 은행 관련 파밍 페이지에서 입력을 요구하는 금융정보는 [표 1]과 같다. 감염 PC에서 금융정보를 입력해 인증을 시도할 경우 정상적으로 로그인되지 않고 입력한 정보를 공격자의 명령제어(C&C) 서버로 전송해 사용자의 금융정보를 탈취하고 있다. 사용자의 계좌번호, 계좌비밀번호, 인증서 비밀번호와 보안카드 정보까지



〔그림 7〕 파밍 페이지를 통한 금융정보 탈취

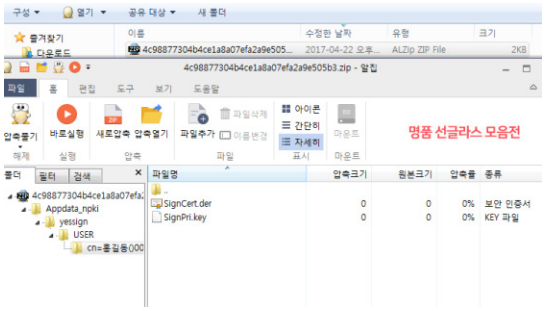
〔표 1〕 파밍 페이지를 통해 유출하는 금융정보

수집하는 금융정보	
이름	주민(사업자)등록번호
계좌번호	계좌비밀번호
핸드폰번호	사용자아이디
사용자비밀번호	인증서비밀번호
보안카드 일련번호	보안카드 정보

입력하도록 유도하고 있어 해당 정보가 유출될 경우 공격자는 사용자의 온라인 뱅킹 서비스를 사용할 수 있다. 공격자는 탈취한 금융정보를 통해 감염 사용자에게 금전적인 피해를 입힐 수 있다[9].

3.3. 공인인증서 탈취

파밍 악성코드에 감염된 PC에서 파밍 페이지 유도를 통한 금융정보 탈취뿐만 아니라, 감염 PC에서 NPKI 폴더가 존재하는지 확인한다. NPKI 폴더가 존재할 시 해당 폴더를 [그림 8]과 같이 압축해 TEMP 폴더에 저장한다. 압축된 공인인증서 파일을 공격자의 명령제어 서버로 전송해 감염된 PC의 공인 인증서를 유출한다. 파밍 페이지 유도를 통해 획득한 감염 사용자의 금융정보와 유출한 공인 인증서 파일을 통해 공격자는 공인인증서 로그인을 통해 사용자의 온라인 뱅킹 서비스를 이용할 수 있기 때문에 금전적인 피해가 발생할 수 있다.



〔그림 8〕 공인인증서 탈취

Ⅳ. 대응방안

파밍 악성코드를 통해 금융정보 유출되면 심각한 금전적인 피해가 발생할 수 있기 때문에 악성코드 감염을

막기 위해 사용자는 백신 프로그램 및 안티 익스플로잇 프로그램 설치와 어플리케이션의 업데이트를 통해 최신 버전을 유지해야 한다.

악성코드 감염경로는 다양하고 백신에 의해 탐지되지 않을 경우 파밍 악성코드에 감염되면 공인인증서 파일과 금융정보는 쉽게 탈취할 수 있기 때문에 추가적인 인증방법 또는 기존의 공인인증서의 인증방법을 대체할 방법이 필요하다. 한국인터넷진흥원에서 2016년 9월에 발표한 '바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인" 에서 스마트폰 환경에서 생체정보를 이용해 공인인증서를 연계할 수 있는 가이드라인을 제시하였고 은행 어플리케이션에서도 기존의 비밀번호 입력 대신 생체정보를 통해 공인인증서 로그인이 가능하다[11]. PC 환경에서 스마트폰의 생체인증을 통해 공인인증서 로그인을 할 경우 기존의 공인인증서 탈취 및 금융정보를 탈취를 막을 수 있다[12].

Ⅴ. 결 론

본 논문에서 파밍 악성코드 유포 방법 및 금융정보를 탈취하는 파밍 악성코드에 대한 분석 및 대응방안에 대해 연구를 수행하였다.

백신 설치 및 어플리케이션 최신버전 업데이트를 통해 악성코드 감염 확률을 상당히 낮출 수 있지만, 사용자의 부주의로 인해 감염될 수 있고 공격자는 사용자의 금융정보를 탈취하기 위해 다양한 방법을 연구해 사용자의 심리를 생각하고 정교한 공격 방법을 사용하고 있다. 공격자는 수집된 금융정보를 통하여 사용자에게 심각한 금전적 피해를 입힐 수 있으므로 기존의 공인인증서의 인증방법 대신 생체인증을 사용한 인증방법은 기존 파밍 악성코드를 통해 금융정보 유출을 막을 수 있으므로 인증기술 개발이 필요하다.

참 고 문 헌

[1] 유동현, "드라이브 바이 다운로드를 통해 유포되는 악성코드의 수집을 위한 웹 크롤 러 설계", 순천향대학교 대학원, 석사학위논 문, 2017년 2 월

[2] 이지오,염흥열, "지속적인 파밍 악성코드 위 협 분석", 정보보호동계학술대회, 2016

[3] 김종기, "웹사이트를 통해 유포되는 메모리 상주형 악성코드의 탐지에 관한 연구", 순천향대학교, 석사학위논문, 2016년 2월

[4] 이재철, 신효정, 김형식, "웹 익스플로잇 킷 에 의한 감염 경로 분석", 보안공학연구 논 문지, 13(4), pp.299-314, 2016년 8월

[5] 정대용, 김기범, 이상진, "전자금융사기 위 험 분석과 대응방안에 관한 연구 = A St udy on Risk Analysis and Counter measures of Electronic Financial F raud", 한국정보보호학회논문지, 27(1), pp.11 5-128, 2017년 2월

[6] 한국인터넷진흥원, "금융 소비자를 위협하는 악성코드 위협사례 분석", KISA Rep ort, 2013년 6월

[7] Wikipedia, "Proxy auto-config", https://en.wikipedia.org/wiki/Proxy_auto-config

[8] AhnLab "ASEC REPORT VOL.74", p10-12, 2016년 2월

[9] 하우리, "2014년에 등장한 파밍의 기술", 2015년 1월

[10] 박진규, 이정호, "전자금융거래 환경에서 보안카드 실수입력방지기법 적용을 통한 피싱/파밍 사고 방지 방안", 한국정보보호학회 학회지, 23(6), pp.30-40, 2013년 12월

[11] 한국인터넷진흥원, "바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인", 2016년 9월

[12] 김재우, 박정효, 전문석, "바이오인증 기반의 전자서명을 이용한 스마트 뱅킹 시스템 설계", 한국산학기술학회논문지, 16(9), p p.6282-6289, 2015년 9월

〈저 자 소 개〉

이 세 빈 (Sebin Lee)
정회원

2016년 2월 : 순천향대학교 정보보호학과 졸업
2016년 3월~현재 : 순천향대학교 일반대학원 정보보호학과 석사과정
관심분야 : 정보보호, 악성코드 분석

이 지 오 (Jio Lee)
정회원

2017년 2월 : 순천향대학교 정보보호학과 졸업
2017년 3월~현재 : 순천향대학교 일반대학원 정보보호학과 석사과정
관심분야 : 정보보호, 악성코드 분석

염 흥 열 (Heung Youl YOUM)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 10월 : ITU-T SG17 부의장
2016년 11월~현재 : ITU-T SG17 의장
2016년 5월~현재 : 개인정보보호포럼 의장
관심분야 : 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜