**시스템 보안**

|  |  |
| --- | --- |
| 과 목 | 시스템보안 |
| 담 당 교 수 | 송유진 |
| 조 원 | 김진우, 김태환 |
| 제출일자 | 2018년 10월 31일 |

1. 최근의 보안 동향
2. 인공지능을 통한 취약점 분석

최근 인공지능 개발이 활발하게 이루어지고 있는데 만약 인공지능 기술을 공격에 활용하면 투자 비용이 크게 낮아지게 된다. 특히 AI를 통한 퍼징 공격이 자주 이루어 질 것으로 예측된다.

1. 보조 배터리를 닮은 값싼 안드로이드 해킹 툴 등장

옥스포드 대학의 연구원이 보조 배터리를 통해 스마트 폰이 충전되는 동안 발생하는 전류 내에서 가짜 통신채널을 생성해 해킹하는 기법인 파워 스니치라는 공격 방법을 개발하였다.이 공격의 데이터 추출 속도는 초당 2비트 정도로 느리지만 데이터를 보호하기 위해 데이터 차단 기능이 탑재된 보조배터리에도 공격 성공이 가능하다고 한다.

이 공격을 막기위한 방법은 간단한데 충전 동안 전원을 꺼두면 배터리로 위장된 디코더가 아무것도 할 수 없다고 한다.

1. 맥용 멀웨어, 인기 불법 프로그램인 어도비 지 통해 퍼져

최근 발견된 맥용 멀웨어, 어도비 지라는 해적판 지원 프로그램이 퍼지고 있다. 이 멀웨어는 프로그램 실행 시 정상 작동하지 않을 뿐만 아니라 방화벽 검사 후 백도어와 암호화폐 채굴 코드도 심고있다.

1. 예상 가능한 새로운 공격 방법
2. 인공지능을 통한 신상 조사

현재도 구글링 같은 방법을 통해 많은 사람들의 신상 정보가 유출되거나 타겟으로 잡고 모든 개인 정보가 드러나는 경우가 많다. 하지만 AI가 도입되면 인간이 처리하는 것과는 수준이 다른 효율성을 보여주게 될 것이다.

이를 막을 방법으로 예상되는 것은 현재 구글에서 사용되고 있는 “당신은 로봇입니까?” 같은 인간과 AI를 구별하기 위한 새로운 검증방법 개발이 필요할 것이다.

1. RansomSNS

최근 대다수의 사람들은 SNS에 사진을 올리고 글을 남기며 추억을 남긴다. 하지만 Ransomware에서 저장장치를 두고 인질극 하듯이 SNS계정을 탈취 한 뒤 모든 데이터를 지우고 인질극을 벌인다면 어떻게 될까? 만약 상관이 없거나 모든 파일이 되어 있다면 다행이지만 그렇지 않다면 공격자의 말을 따를 수 밖에 없을 것이다.

이를 방지하기 위해서는 소중한 사진 같은 경우에는 백업파일을 만들거나 보안성이 강한 비밀번호를 사용하는 등 계정 보안 관리에 신경 써야 할 것이다.

1. 소감
2. 김태환

조사를 하며 확실히 대다수의 보안관련 소식들은 옛날에 이미 발견한 해킹 기법이 많았다. 물론 거기까지는 예상했지만 AI같은 기술의 발전에 따라 기존의 해킹 기법이 아니라 새로운 기술에서 비롯되는 신선한 방법들이 많아서 놀랐다. 또한 인간은 항상 실수하는 생물이며 해커는 항상 그 실수를 발견할 것이라는 생각을 하였다.

1. 김진우
2. 출처
3. <https://www.boannews.com/media/view.asp?idx=74728&page=2&kind=1&skind=5&search=title&find=>
4. <https://www.boannews.com/media/view.asp?idx=75321&page=1&kind=1&skind=5&search=title&find=>
5. <https://www.boannews.com/media/view.asp?idx=75372&page=1&kind=1&skind=5&search=title&find=>