16011069 장지혁

6.1 과제 주제

최근 발생된 컴퓨터 바이러스와 관련된 기사를 찾아보고, 해당 바이러스의 형태 및 증상에 대해서 기술하세요.

'수신된 이메일에 바이러스가 발견됐습니다!' 피싱 메일 유포중' - 보안뉴스 21/09/14

'수신된 이메일에서 바이러스 활동이 발견되었다'면서 이메일 검사를 유도하는 피싱메일이 발견된 내용이다. 계정안전을 위해 표기된 **검사링크를 클릭하도록** 유도하면서 발신자 표시를 NHN 한국사이버결제(전자결제 전문업체명)로 사칭하여 위장하였다. 사용자가 **링크를 클릭할 시 해당 메일 계정과 패스워드를 탈취하는 피싱사이트로 이동**하였다. 이러한 바이러스는 **메일을 이용하여 전파**되므로 **매크로 바이러스**라고 할 수 있다. 사용자가 아이디와 패스워드를 입력하면 본인 계정의 이메일이 감염되었다는 문구를 보여주며, 피싱사이트에 입력된 **사용자의 아이디와 패스워드는 공격자 서버로 전송되게끔** 설계되었다.

6.2 과제 주제

스턱스넷 웜에 대하여 알아보고 (역사 및 감염된 나라), 감염시 증상에 대해서 기술하세요.

스턱스넷 웜은 **2010 년 6 월** 컴퓨터 보안회사 VirusBlokAda 에서 발견한, 마이크로소프트 윈도우를 통해 감염되어 **지멘스 산업(독일의 엔지니어링 회사)의 소프트웨어 및 장비를 공격하는 웜 바이러스**이다. 윈도우가 설치된 임의의 컴퓨터에 감염이 되고, 지멘스사의 시스템만을 감염시켜 장비를 제어하고 감시하는 특수한 코드를 담고 있는 웜 바이러스이다.

감염된 나라에는 **이란, 인도네시아, 인도**가 감염된 컴퓨터 중 약 80% 가까이 차지했으며, 이외에 아제르바이잔, 미국, 파키스탄 등이 있다.

대부분의 악성 소프트웨어와는 달리 스턱스넷은 **일반적인 컴퓨터와 네트워크에는 거의 해를 끼치지 않는다**. 스턱스넷은 공격 목표에만 타격을 입히기 위한 웜 바이러스이다. 심지어 무작위로 전염되지만 지멘스 소프트웨어가 없으면 휴면상태에 들어가 특정 날짜에 자기 자신을 삭제하는 안전장치 또한 있었다.

하지만 **공격목표(지멘스 소프트웨어)를 발견하면 공정제어 신호를 중간에서 가로채어 가짜신호를 보내는 중간자 공격**을 하여 지멘스 소프트웨어가 오작동을 감지해 시스템을 정지시키지 않게 한다.

최초 감염은 USB 를 통해 이루어졌고 **이후에는 윈도우 기반 컴퓨터간의 원격 프로시저 호출** 등의 프로토콜을 통해 인터넷에 노출되지 않은 폐쇄망으로 연결된 컴퓨터를 감염시켰다.

6.3 과제 주제

트로이 목마의 사례를 하나 찾아보세요.

'이란계 APT 공격 단체, 셸클라이언트 트로이목마로 항공우주·통신업체 공격' – ITWORLD 21/10/09

이란 기반 해커 그룹(멀카막)이 2018 년 개발된 트로이목마 프로그램을 사용해 항공우주 업체와 통신 업체를 공격한 사건이다. **중동, 미국, 유럽, 러시아가 주요 공격 대상 국가**였고, **목적은 기업의 인프라와 기술, 중요 자산에 대한 정보 탈취**였다.

멀카막이 사용한 악성코드 도구는 **쉘클라이언트 'RAT'** 이다. 멀카막은 2018 년부터 이를 사용하였다.

쉘클라이언트는 **3 가지의 배포방식**이 있는데,

1.윈도우 설치 관리자 도구를 사용해 시스템 서비스(nhdService)를 설치하는 방법
2.서비스 컨트롤 매니저(SCM)을 사용해 드롭박스 계정과 정보를 주고받는 리버스 쉘을 생성하는 방법
3. 공격 대상 시스템에 침입해 정보를 수집하여 지속적으로 전파시킬 가치가 있는 경우 사용하는 악성코드 방법

이 있다. 이러한 방법들을 사용하여 **파일 및 디렉토리 운영, CMD 및 파워쉘 열기, 쉘 명령 실행 등**을 일으켜 내부 전파를 일으킨다.