금융정보를 탈취하는 최근 파밍 악성코드 연구

노정호* · 박대우*

*호서대학교 벤처대학원

Recent pharming malware code exploiting financial information

Jung-ho Noh* · Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : network87@hanmail.net, prof_pdw@naver.com

요 약

국가와 사회의 인프라가 사이버로 연결되어 있다. 최근 대구지역 IP로 확인되는 성형외과, 치과, 병원 등 홈페이지에 금융 정보를 탈취하는 악성코드가 전파되고 있다. 특히 금융 정보는 중요한 개인정보보호 대상이다. 금융정보의 탈취는 개인의 금전적인 손실로 이어진다. 본 논문에서는 금융정보를 탈취하는 최근의 파밍 악성코드를 분석한다. 사회공학적 방법이 동원된 공격 파일은 다운로더로 위장하여 배너속에 실행파일로 전파 되고 있다. 사용자가 배너를 선택하면 공격 파일은 악성코드를 사용자에 PC를 감염시킨다. 감염된 PC는 파밍 사이트로 사용자를 유도하여 금융정보와 개인의 보안카드 정보를 탈취한다. 탈취된 금융정보는 사용자에게 금전적인 손실을 발생시킨다. 본 논문에 연구는 안전한 금융보안 거래에 기여할 것이다.

ABSTRACT

The infrastructure of the country and society is connected to cyberspace. Malicious codes that steal financial information from websites such as plastic surgeons, dentists, and hospitals that are confirmed as IP in Daegu South Korea area are spreading In particular, financial information is an important privacy target. Takeover of financial information leads to personal financial loss. In this paper, we analyze the recent pharming malicious code that takes financial information. Attack files with social engineering methods are spread as executables in the banner, disguised as downloaders. When the user selects the banner, the attack file infects the PC with malicious code to the user. The infected PC takes users to the farming site and seizes financial information and personal security card information. The fraudulent financial information causes a financial loss to the user. The research in this paper will contribute to secure financial security.

키워드

사이버보안, 정보탈취, 악성코드, 파밍

Ⅰ. 서 론

사회공학적 방법이 다양해지면서 개인정보 손실이 증가하고 있다. 사용자가 많은 SNS(Social Networking Service)를 통해 악성코드가 담겨져 있는 광고 및 링크를 '선물을 준다'라는 제목과 함께 링크를 걸어 놓고 클릭을 유도하는 경우가 있다. 이러한 방식에 넘어가게 된다면, 특정 글에 공유가 되거나 개인 식별정도를 입력할 경우 사기에 당할 수 있다. 또한 특정 제품을 받고 싶을 경우 악성코드가 숨겨져 있는 소프트웨어를 다운받도록 유도하는 방식도 있으며, SNS를 이용하여 외부 웹사이트로 유도하기도 한다.

또 다른 방식으로는 기사를 보기 위해 클릭하자 해당 포털 로그인 창이 열리는 경우이다. 일반적인 사람들이라면 사용중인 포털 검색창에서 해당 로그인 창이 뜨면 별 생각 없이 계정 아이디와 패스워드를 입력하게 된다. 하지만 주소창을 확인해본다면 포털 주소가 아닌 다른주소로 되어 있는 경우가 있다. 이러한 경우는 스마트폰이 악성코드에 감염되었을 수도 있으며, PC로 접속했을때도 마찬가지면 해당 매체 사이트의 도메인 서버가 해킹 및 DNS 주소값이 변조돼 피싱 사이트로 연결된 것으로 파악할 수 있다.

포털 계정정보가 유출이 되면 연결되있는 다른 계정까지 해킹이 가능해지기 때문에 개인정보뿐만이 아닌 금융정보까지 유출되어 사용자에게 금전적인 손실을 발생시킬 수 있어 주의가 필요하다.

본 논문에서는 사용자의 개인정보 뿐만이 아닌 금융정보까지 안전하게 거래할 수 있는 파밍 악성코드에 대해 분석한다.

II. 본 론

2.1 악성코드

악성코드가 계속해서 기술 발전이 이루어짐에 따라 성코드 방어 시스템의 발전도 계속해서 이루어졌다.

과거 특정 악성코드에만 있는 표식을 기반으로 악성코드를 찾아내는 시그니처 기법이 주류를이루었으나 악성코드 자체는 동일하지만프로텍터(Protector)를 이용하여 간단하게 다수의 변종악성코드를 만들어 배포하는 방법으로 탐지 로직을 회하였다. 이에 몇 년 전에 등장한 개념이 악성코드를 자동으로 동적 분석하여 악성코드가 발생하는 수많은 행위를 점수화 하여 이를 토대로 탐지하는 악성코드 동적 분석 기법이 소개되었다.

이 기법은 샌드박싱된 공간에서 구동시키고 행위를 수집하여 악성 행위를 판단한다. 이 기법은 별도의 하드웨어 장비 형태로 바이너리가 들어오는 진입로에 위치하여 사용자에게 전달되기 전에 시스템에서 검사하거나 호스트 내의 보안 프로그램에 내장되어 사용자가 다운로드한 프로그램을 실행 시점에 먼저 검사하는데 활용되고 있다[1].

2.2 사이버보안

현재 국가사이버안보 합동 대응으로 대한민국은 평시에 사이버보안은 국가정보원을 중심으로 18개 기관이 참여하는 민·관·군 합동대응팀을 구성·운영 중이다. 하지만, 대통령훈령인 '국가사이버 안전관리규정'에 근거하고 있어서 국가사이버안보를 위한 임무·기능 및 권한에는 한계가 있다.

급속하게 발전하는 사이버안보의 기술과 사이버안보의 인프라를 위한 인터넷 네트워크를 스캔하고, 탐지하는 것만으로는 국가사이버안보를 위한 실시간 사이버안보 대응에는 한계가 있다.

따라서 국가차원의 사이버안보 합동대응을 강화하고 관련 유관기관과 연계기관의 역할을 정책과 매뉴얼 식의 총체적인 대응에 필요한 국가사이버안보 합동 대응이 필요하다.

더불어 국가 사이버안보를 위해서는 외국과의 국가 사이버안보 공조 대응을 위해, 사이버 공격, 취약점, 기술, 전문가, 수사 및 처벌에 대한 국제 공조를 수행하여 국가 사이버안보를 위한 정책 연구여, 세계 각국과 사이버안보를 위한 규범을 식별하고, 사이버범죄와 사이버테러 및 사이버전쟁에 대비한 국제 공조가 필요하다.

사이버안보무기와 운영체제 기술 연구개발도 필요하다[2].

2.3 파밍

파밍(Pharming) 이란 피싱(Phishing)과 조작(Farming)의 합성어로, 악성프로그램에 감염된 PC를 조작하여 피해자가 정상 사이트로 접속하더라도 가짜 은행사이트로 접속을 유도하여 금융거래정보를 빼낸 후 금전적인 피해를 입히는 수법을 말한다.

공격자는 악성코드를 사용자에게 전송하게 되고 사용자는 이를 자신의 컴퓨터 혹은 스마트폰에 깔게 됨으로써 적합한 사이트의 주소가 변경되어 악의적 사이트에 접속되게 된다. 사용자는 의심 없이 자신의 정보를 입력함으로써 공격이 성공 하게된다.

기존 피싱 또는 파밍수법에서 보안카드전체 입력요구가많았다면, MITM 기법에서는 피해자가 정상 금융거래를 진행한다고 생각하고, 보안카드를 정상적으로 두 개만 입력하여도 공격자의 공격이 성공할 때까지 피해자가 해킹사실을 인지하기 어렵다[3].

III. 결 론

본 논문은 금융정보를 탈취하는 파밍 악성코드에 대해 분석에 대하여 연구하였다.

가장 중요시 되는 안전한 금융거래를 하기 위해서는 사용하는 금융 홈페이지에 접속할 때 인터넷 주소창에 녹색 인증창이나 자물쇠 표시를 확인해야한다. 진짜 금융 홈페이지는 SSL 인증서가 보안서버에 설치되어있어, 홈페이지의 위·변조 여부를 확인해주기 때문이다.

또한 파밍은 기본적으로 악성코드에 감염이 되어있는 디지털기기여야하므로, 백신 프로그램과 운영체제를 최신상태로 유지하고 보안점검은 주기적으로 실시해야 개인정보 및 금융정보 손실을 줄일 수 있다.

참고문헌

[1] Kyeong-sik Lee, Hwa-jae Choi, Jeong-chan Park "Research on Bypass the malware dynamic analysis and Response method", Korea Information Science Society, pp.1069-1071, 2017.6

[2] Seung-hyeon Ham, Dea-woo Park*, "Study on Policies for National Cybersecurity", Journal of the Korea Institute of Information and Communication Engineering, Vol.21, No.9, pp.1666~1673, 2017.9

[3] Hwa-jeong Seo, Ho-won Kim*, "Design and Implementation of Physical Secure Card for Financial Security", Journal of the Korea Institute of Information and Communication Engineering, Vol. 19, No. 4, pp.855~863 2015.4