중소기업융합학회 논문지 제5권 제1호 pp. 25-30, 2015 ISSN 2234-4438

APT 공격과 대응 방안 연구

한군희
백석대학교, 정보통신학부

APT attacks and Countermeasures

Kun-Hee Han[1*]
[1*]Division of Information and Communication, Baekseok University

요 약 APT공격은 해커가 다양한 보안 위협을 만들어 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격을 뜻한다. 지능형 지속 공격이라 한다. 특정 조직 내부 직원의 PC를 장악한 뒤 그 PC를 통해 내부 서버나 데이터베이스에 접근한 뒤 기밀정보 등을 빼오거나 파괴한다. APT의 공격 방법은 제로데이와 루트킷 이렇게 크게 두 가지 공격이 있다. APT의 공격 과정은 침투, 검색, 수집, 유출 단계 4단계로 구분된다. 과정을 통하여 APT에 어떻게 대응할 수 있는지 두 가지 방안으로 정의하였다. 기술을 통한 악성코드 공격자의 공격 소요 시간을 지연시키는 방안과 공격에 대한 탐지 및 제거 할 수 있는 방안으로 나누어서 설명하였다.

키워드 : 지능형 지속 위협, APT 공격, 악성코드, 보안

Abstract The APT attacks are hackers created a variety of security threats will continue to attack applied to the network of a particular company or organization. It referred to as intelligent sustained attack. After securing your PC after a particular organization's internal staff access to internal server or database through the PC or remove and destroy the confidential information. The APT attack is so large, there are two zero-day attacks and rootkits. APT is a process of penetration attack, search, acquisition, and is divided into outlet Step 4. It was defined in two ways how you can respond to APT through the process. Technical descriptions were divided into ways to delay the attacker's malicious code attacks time and plan for attacks to be detected and removed through.

Key Words : APT(Advanced Persistent Threats), APT ATTACK, malicious code, security

1. 서론

IT가 발달하면서, 은행 및 기업을 운영하는 많은 핵심 정보들이 컴퓨터 시스템에 저장되어 있다. 또한 인터넷과 SNS와 같은 소셜 네트워크의 발달은 공격 대상의 개인정보 수집에 용이한 상황을 만들어 주었고. 공격 또한 고도화 지면서 피해를 주고 있다. 그래서 더욱 전문 해커들에게 쉬운 공격 대상이 되고 있다. APT 공격은 점점 더 다양한 목적을 가지고 있으며 공격 대상도 확대되고 있다. 우리나라는 2004년부터 꾸준히 지능형 지속 위협(APT, Advanced Persistent Threats) 공격을 받고 있다.

Received 2015-02-07 Revised 2015-02-25 Accepted 2015-03-06
*Corresponding author: Kun-Hee Han (hankh@bu.ac.kr)

APT 공격을 받은 기업은 시스템 핵심 데이터 파손은 물론 기업 중요 정보 유출로 인하여 기업의 신뢰성 또한 하락되어 매출 감소로까지 이어져 큰 피해가 생긴다. APT 대응을 위한 필요성과 인식은 높아지고 있지만, 솔루션 도입이나 구체적인 보안 대책 실행은 미흡하다. 국내 기업의 10곳 중 7곳이 관련 보안 솔루션이 없는 것으로 나타났다.[1]

연구의 구성은 2장에는 관련 연구를 살펴본다. 3장에는 APT(Advanced Persistent Threats)와 APT의 공격 방법에 대하여 자세히 알아보고, 4장에는 APT 공격에 따른 대응방안을 기술하였다. 마지막으로 5장에서는 연구를 마무리 짓는다.

2. 관련연구

2.1 랜섬웨어(ransomware)

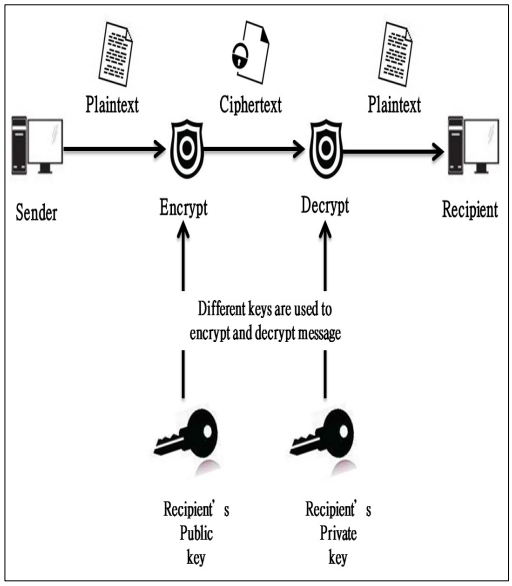

Fig. 1. Ransomware Attack

악성코드란 악성 행위를 위해 개발된 컴퓨터 프로그램을 말한다. 컴퓨터 사용자에게 해를 끼치는 모든 코드(바이러스, 웜, 스파이웨어, 트로이 목마 등)이 해당된다.

2015년 4월 21일 새벽 1시 38분부터 오전 11시 12분까지 국내 대형 온라인 커뮤니티인 클리앙에서 '랜섬웨어'의 하나인 크립토록커(CryptoLocker)가 유포되었다. 랜섬웨어는 감염된 PC의 파일을 암호화한 후 '인질의 몸값(ransom)'을 요구하여 ransom을 내야 암호화를 풀 수 있는 키를 전달해 주는 악성코드이다.[2]

2.2 멀웨어(Malware)

악성 소프트웨어(malicious software)의 줄임말로, 사용자의 동의 없이 PC에 설치되는 모든 소프트웨어를 말한다.

우리가 많이 알고 있는 바이러스나 웜, 스파이웨어, 애드웨어, 트로이목마 등을 모두 통칭해서 멀웨어라 부른다. 감염된 웹사이트에 들어가서 악성 링크를 클릭하면 시스템이 쉽게 감염이 되며 알지 못하는 사이에 멀웨어가 설치될 수 있다.

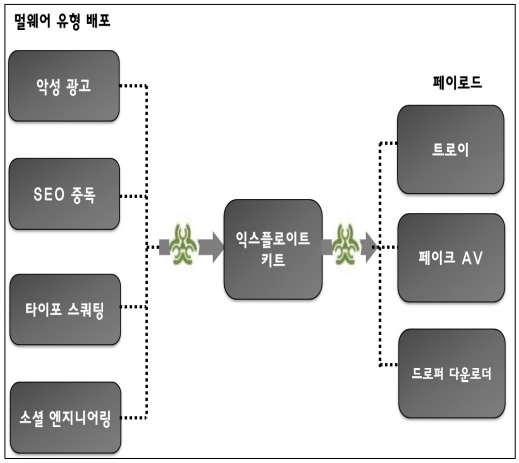

Fig. 2. Malware Procedure

웹사이트의 코드를 통해 배포될 수 있는 여러 종류의 멀웨어 (악성광고, SEO 중독, 타이포 스쿼팅 및 소셜 엔지니어링)들이 있다. 일단 공격에 노출되면 익스플로이트 키트를 통해 다운로드가 활성화된다. 그런 다음 다운로더는 사용자의 컴퓨터를 감염시켜 컴퓨터를 손상시키거나 정보를 도용한다.

멀웨어는 오래됐다고 해서 기능이 떨어지지 않는다. 아주 작고 사소한 변형이라도 새로운 공격이 될 수도 있다. 멀웨어는 4초마다 새로운 변종이 태어나고 있고, 지난해 새로운 멀웨어 변종 증가율이 77%로 집계되었다. 멀웨어는 계속해서 새로운 변화를 통해 활개를 칠 것이다.[3]

3. APT(Advanced Persistent Threats)

3.1 APT(Advanced Persistent Threats)[4]

APT 공격은 공격 대상이 눈치 채지 못하도록 은밀하게 침투한다. 때를 기다리면서 회사와 관련된 정보를 천천히 살펴본다. 흔적을 남기지 않고 활동하면서 회사 내 보안서비스를 무력화시키고 유유히 정보를 유출한다. 흔적을 지우면서 조심히 활동하기 때문에 정보가 유출된 시점이 바로 들어나지 않는다.

3.2 APT공격 방법

APT의 공격 방법은 제로 데이(Zero-day)와 루트킷(RootKit) 2가지 공격 방법이 있다.

제로 데이(Zero-day)는 특정 소프트웨어의 아직까지 공표되지 않았거나 공표되었지만 패치가 발표되기도 전에 취약점을 이용한 해킹을 말한다.

최근 사례를 보면, 안랩에서 '한글'의 '제로데이 취약점'을 이용한 악성코드 감염 시도를 발견했다고 한다. 21일 한글과 컴퓨터는 관련 취약점을 개선한 보안패치를 배포하였다.[5]

루트킷(RootKit)은 해커들이 컴퓨터나 또는 네트워크에 침입한 사실을 숨긴 채 관리자용 접근권한을 획득 하는데 사용하는 도구를 말한다. 공격자는 루트킷을 이용하여 시스템에 관한 관리자 수준 액세스 권한을 얻는다. 이 도구는 보통 탐지하기 쉽지 않으며, 암호를 크랙킹 하거나 알려진 취약점을 통하여 설치된다. 로컬 네트워크의 패킷들을 수집하여 아이디와 패스워드를 빼내고 공격자에게 루트 계정의 권한이나 특별한 접근권한을 제공한다.[6]

3.2 APT공격 과정[7]

APT의 공격은 크게 네 가지 단계로 구분된다. 침투 단계, 검색 단계, 수집 단계, 유출 단계가 있다. 침투를 하기 위해서 목표를 한 대상에 대한 조사를 하게 된다.

침투 단계에서는 그 대상이 어떤 소프트웨어를 사용하고, 소프트웨어의 버전은 어떻게 되며 어떠한 보안 장비를 사용하여 웹을 접속하는지, 그리고 자주 접속하는 웹 사이트는 어떻게 되는지 세세하게 모든 부분에 대해 조사를 한다. 이렇게 조사한 내용을 토대로 취약점을 찾아 침투를 하게 된다. 이러한 침투 방법에는 웹을 통한 워터링홀(Watering-Hole)과 스피어피싱(Spear Phshing)이 있다. 이렇게 침투를 시도해 대상이 웹 페이지 접속이나 이메일을 통해 악성 파일을 다운로드 받게 되고 실행하게 된다. 이 과정을 드랍퍼 단계라 한다. 이렇게 악성코드 실행까지 정상적으로 완료가 되고 나면, 우리가 흔히 아는 콜 백 통신, C&C 서버로의 콜 백 통신이 이루어지게 된다. 즉, 이 때부터 악성 파일을 다운로드 받은 PC에 대한 모든 제어권은 외부에 있는 해커에게 넘어간다.

검색 단계에서는 해커가 감염 된 PC를 통해 조직 내의 모든 인프라 구조와 시스템에 대해 검색 하게 된다. 이를테면 PMS 서버와 같은 업데이트 서버의 주소를 찾아내던지, 핵심 데이터를 가진 서버의 주소를 알아낸다던지 다음 단계를 계획을 하게 된다.

수집 단계에서는 PMS 서버에 접근해 제어권을 획득하고, 그 PMS 서버를 통해 모든 에이전트에게 악성 코드를 배포하게 된다. 결과적으로 목표로 하는 대상의 네트워크에 대한 모든 제어권이 해커에게 넘어가게 된 것이다. 해커는 무력화된 시스템 상의 데이터를 수집하게 된다.

마지막 유출 단계에서는 해커가 내부에 있는 데이터를 유출시킨다던지 시스템 운영을 방해하며 심한 경우에는 시스템의 핵심 데이터를 파괴하는 행위를 하게 된다.

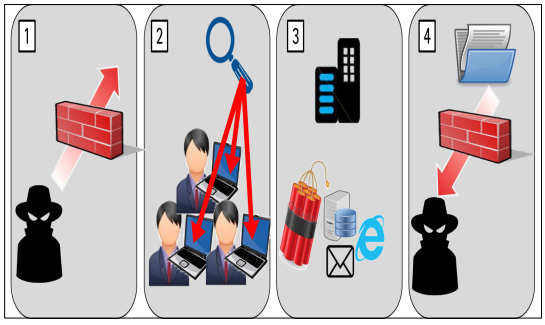

Fig. 3. APT Attack Processing

3.3 APT 침투 방법

3.3.1 스피어 피싱(Spear Phshing)

스피어 피싱이란 '창, 창으로 찌르다'라는 의미의 영어 단어 스피어(Spear)와 '사용자를 속이기 위한 사기 이메일 및 기타 행위'를 의미하는 용어인 피싱(Phishing)의 합성어이다.

개인이나 조직을 은밀히 염탐하고 해당 개인이나 조직의 기밀정보를 빼내기 위해 신뢰할 수 있는 내용처럼 위장한 악성 이메일을 관련자들에게 전송시켜 감염시킨다. 이후 원격제어 및 데이터 탈취 등을 시도한다.

Fig. 4. Spear Phshing Attack

스피어피싱 이메일에는 정상파일과 2중 확장명을 가지고 있는 악성파일이 함께 포함되어 있다. 2중 확장명을 가진 악성파일이 실행되면 동일 경로에 정상적인 문서파일을 생성하고 실행한다. 정상적인 문서파일을 실행함과 동시에 사용자가 눈치 채지 못하게 임시폴더 경로에 “conhost.exe” 이름의 추가 악성파일을 몰래 설치하고 자동으로 실행하게 한다. 해당 악성코드는184.164.81.5:80 원격지(C&C) 주소로 접속을 하여, 추가적인 명령을 무한 대기하게 된다. 이후 공격자의 원격제어 및 추가 명령에 따라 변종 악성코드가 추가로 설치되거나 정보가 유출되는 피해를 입을 수 있다.[8]

3.3.2 워터링홀(Watering-Hole) 공격

사자가 먹이를 습격하기 위해 물 웅덩이(Watering hole) 근처에 매복하고 있는 모습을 빗댄 말이다. 사용자가 덫에 걸리기를 기다리고 있다. 공격자가 타깃으로 정한 사용자의 정보를 수집해서 주로 방문하는 사이트에 제로 데이 취약점을 사용해 해당 사이트에 악성코드를 심어둔다.

3.3.3 APT 공격의 내부 확산(Lateral Movement)

위의 침투 방법 등으로 기업의 내부 네트워크에 침투에 성공하면 공격자는 공격 목표인 시스템으로 이동하려고 한다. 이 과정을 ‘Lateral Move ment‘라 한다. 이러한 이동을 위해서는 높은 권한을 가진 계정의 인증 정보가 필요하다.

계정의 인증 정보는 시스템의 레지스트리, 메모리 내에서 얻을 수 있다. 이때 대부분의 공격자들은 주로 gsecdump, WCE(Windows Credential Editor), mimikatz 등 기존의 툴을 이용하거나 공격 툴이 사용하는 wceaux.dll, sekuralsa.dll 등의 DLL을 악성코드에 삽입하여 이를 호출하는 방식을 사용한다.

위의 방법으로 획득한 도메인 관리자 계정 정보를 가지고 시스템과 네트워크 공유를 맺은 후 백도어를 복사한다. 원격 서비스, 또는 작업 스케줄러를 등록해 앞서 복사한 백도어를 실행한 후 이를 시스템 권한으로 동작하게 한다. 이렇게 실행된 백도어는 프록시 기능에 의해 C&C(Command and Control) 서버와의 연결을 중계함으로써 공격자는 해당 시스템에 접근할 수 있게 된다.

이렇듯 공격자는 치밀한 네트워킹 기술을 보유하고 있으며 목표 대상의 네트워크를 넘나들면 은밀히 네트워크를 장학하고 지속적으로 주요 기밀 정보를 유출하고 있다.

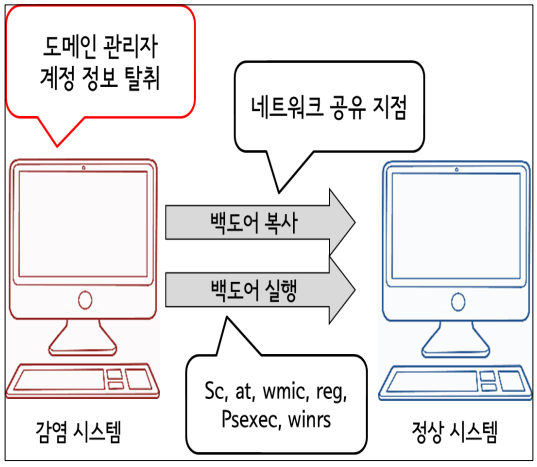

Fig. 5. Internal Diffusion Process

4. APT 공격 대응방안

기술을 통해서 악성코드 공격자의 공격 소요 시간을 지연시키는 방안과 공격에 대한 탐지 및 제거 할 수 있는 방법에 대하여 설명하겠다.

APT 공격자가 원하는 정보에 도달하기 까지 1개월에서 6개월 정도의 시간이 필요하다고 한다. APT 공격 소요 시간 지연을 위한 주요 보안 조치로 첫 번째 시스템 패치를 한다. 악성코드의 공격의 성공을 낮추어 내부 시스템 점령에 많은 시간을 필요하게 한다.

두 번째 내부 인증을 강화하는 것이다. OTP, Smart Card 등을 이용하여 인증 내부 시스템을 강화하여 관리자의 계정정보 획득을 어렵게 한다.

세 번째 네트워크 망을 분리시킨다.[9] 네트워크 망을 분리시키면 인터넷으로부터 보안 위협 자체를 차단할 수 있다. 이메일이나 매체 등 허용된 경로에 대한 보안 솔루션만 도입하여 운영해야 한다.

마지막으로 중요 정보를 암호화 한다. 중요 정보에 대해 암호화를 적용 하고 암호화 키를 관리한다.

APT 공격에 대한 탐지 및 제거를 할 수 있는 방법으로는 첫 번째, 샌드박스(SandBox) 기술을 사용하는 것이다. 샌드박스를 간단히 말하면 악성코드 분석에 유용한 환경을 제공하는 프로그램이다. 사용자 PC에 다운로드 되는 파일을 샌드박스 내에서 실행해보고 문제가 없을 경우에만 유입될 수 있게 하는 기술이다.

두 번째는 행위기반 탐지 기법(Behavior Detection Tech)이다. 행위기반 탐지는 각종파일이나 유입된 트래픽이 내부에서 허락되지 않은 시스템에 접근하거나 레지스트리를 변경하는 것을 모니터링해서 악성 코드를 탐지할 수 있다. [6]

마지막으로 분석과 감지에 빅데이터(BIG DATA) 기술을 이용해서 보안을 강화한다. 로그나 패킷을 모아서 분석해서 사이버 공격이나 데이터 유출 패턴을 찾을 수 있는데 이 기술을 통하여 APT 공격도 막을 수 있다. [10]

하지만 위의 기술을 모두 이용한다고 해도 공격을 완벽하게 막을 수 있는 방법은 없다. 계속하여 알려지지 않은 취약점을 이용하여 공격이 시도되고 있다.

기업은 기존에 보유하고 있는 솔루션을 재검토하여 새로운 솔루션을 마련해야 하고, 지속적인 관리가 필요하다. 내부 보안 교육을 강화하고 보안 업데이트는 항상 최신 상태로 유지해야 한다.

또한, 스스로가 보안에 대한 인식을 가져야 한다. 자신의 컴퓨터에 설치된 백신은 항상 최신 업데이트가 되도록 유지하고, 주기적인 바이러스 검사를 해줘야 한다. 발신인이 불분명하거나 수상한 첨부파일은 실행하지 말아야 한다.

5. 결론

본 연구에서 APT 공격을 자세하게 살펴본 뒤, APT 공격에 대한 대응방안을 제시 하였다. APT 공격은 지능적이며 지속적으로 이루어진다. 공격자들은 계속 IT 기술안의 취약점을 찾아 공격해올 것이다. 이에 대응하기 위해서 보안에 대한 투자와 APT에 대한 연구가 필요하고 꾸준한 보안 업데이트가 필요할 것으로 생각된다.

REFERENCES

[1] Huy Kang Kim, Soo-Kyun Kim, Seok-Hun Kim: Decision Support System for Zero-day Attack Response, An International Journal, Appl. Math. Inf. Sci. 6 No. 1S pp. 221S-241S (2012)

[2] Reshma R. Patel, Chirag S. Thaker: Zero-Day Attack Signatures Detection Using Honey-pot, International Conference on Computer Communication and Networks CSI- COMNET (2011)

[3] Zhang Wei, Wang Hao-yu: Intrusive Detection Systems Design based on BP Neural Net-work, Distributed Computing and Applications to Business Engineering and Science (DCABES), IEEE (2010)

[4] Pachghare V.K., Kulkarni P., Nikam D.M. : Intru-sion Detection System using Self OrganizingMaps, International Conference on Computing & Processing (Hardware/Software), IEEE (2009)

[5] Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung: Intrusion Detection: Support Vector Machines and Neural Networks, IEEE and Proceedings of the 2002 International Joint Conference on Neural Networks IJCNN02 Cat No 02 CH3 7290 (2002)

[6] Meijuan Gao, Jingwen Tian: Network Intrusion Detection Method Based on Improved Simulated Annealing Neural Network, IEEE and also at International Conference on Measur-ing Technology and Mechatronics Automation (2009)

[7] Paulo M. Mafra, Vinicius Moll, Joni da Silva Fraga: Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System, IEEE (2010)

[8] Song Guangjun, Zhang Jialin, Sun Zhenlong: The Research of Dynamic Change Learning Rate Strategy in BP Neural Network and Application in Network Intrusion Detection, IEEE and 3rd International Conference
on Innovative Computing Information and Control (ICICIC'08) (2008)

[9] Bhavin Shah, Bhushan H. Trivedi: Artificial Neural Network based Intrusion Detection System: A Survey,

International Journal of Computer Applications (0975 - 8887) Volume 39 - No.6 (2012)

[10] System Forensics. (2012, Nov.) APTish Attack via Metasploit-Par 2-Spunk. [Online]. Available: http://www.sysforensics.org/2012/11/aptishattack-via-metasploit-part-two.html 109-115, Aug. 2013. September

저 자 소 개

한 군 희(Kun-Hee Han) [종신회원]

- 2000년 2월 : 충북대학교 박사
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 정보보호 전공 교수

<관심분야> : 데이터베이스, 운영체제, 정보보호, Network Security, 이동통신보안