정 보 보 호 학 회 지
제26권 제1호, 2016. 2

은닉형 악성코드를 활용한 공격 사례 분석과 대응방안에 대한 고찰

지 선 학*, 박 지 윤**, 이 재 우***

요 약

IT기술이 발달함에 따라서 데이터는 대량화, 다양화 되었다. 그에 따라서 이를 침해하려는 다양한 공격기술들이 등장하고 있다. 특히, 지능형 타깃 지속 공격이라는 APT(Advanced Persistent Threat) 공격은 날로 발전하고 있다. APT공격 중에서도 특히 은닉형 악성코드를 이용한 공격들이 많이 등장하고 있다.

은닉형 악성코드는 사용자가 인식하지 못하도록 보안시스템을 우회하고, 중요 데이터의 수집 및 유출을 위하여 교묘하게 시스템에 숨어들어 악의적인 행위를 하는 형태의 악성코드를 말한다. 이러한 고도화된 악의적인 행위를 하는 악성코드를 탐지하고, 대응하기 위한 기술들은 아직까지 부족한 것이 현실이다. 본 논문에서 대표적인 은닉형 악성코드와 공격사례를 분석하여 이를 대응할 수 있는 방안을 고찰해본다. 또한 이를 통하여 고도화된 공격기술들에 대해 예방하고 대응하는 자료로 활용 가능하다.

Ⅰ. 서 론

최근 각종 공공기관, 금융기관 등에서 많은 정보보안 사고가 발생하고 있다. 이는 현대 기술이 발달함에 따라서 데이터의 가치성은 크게 증가하였고, 이를 통하여 이득을 보기위한 악의적인 공격자들의 숫자도 증가하였다. 또한 악의적인 공격행위에 이용되는 기술들도 하루가 다르게 지능화 되고 있다.

이러한 공격자들의 공격기술 중 최근 가장 화두가 되고 있는 것이 APT공격기술이다. 장기간에 걸쳐 특정 데이터를 목표로 잠입하여 공격이 이루어지기 때문에 쉽게 탐지를 하거나 예방하는 것에는 한계가 있다. 이러한 APT 공격기술들에 핵심은 피해 시스템에 장기간 동안 잠입하는 은닉형 악성코드 기술이다. 은닉형 악성코드는 일반적인 백신소프트웨어나 IDS, IPS, Firewall 등의 장비로는 예방 및 탐지하기 어렵도록 지능화되어 보안시스템을 우회하여 시스템에 침입한다. 또한 일부 은닉형 악성코드는 이란 원전 공격에 사용된 스턱스넷(Stuxnet)이라고 하는 웜 바이러스의 파괴력과 비슷한 수준이다. 즉, 이러한 은닉형 악성코드에 대비해야할 필요성이 존재한다.

본 지에서는 이러한 공격기술에 핵심이 되는 은닉형 악성코드의 분석을 통하여 APT공격에 대비하고 은닉형 악성코드를 통한 보안사고의 사례분석을 통하여 대응방안에 대하여 고찰해본다.

Ⅱ. 은닉형 악성코드

은닉형 악성코드의 특징은 공격 대상 시스템이 공격자의 침입을 눈치 채지 못하게 잠입하는 것이 가장 큰 특징이다. 이는 APT공격에 있어서 가장 핵심이 되는 기술이 된다. 본 부분에서는 가장 대표적인 은닉형 악성코드들을 분석하고 이를 이해하도록 한다.

2.1 두쿠 1.0(Duqu 1.0)

2.1.1. 개요

2011년 부다페스트 대학의 보안 연구실인 CrySyS는 이 위협의 파일이름의 접두사가 DQ로 시작하는 파일을

* 동국대학교 정보보호학과
** 동국대학교 정보보호학과
*** 동국대학교 국제정보대학원

생성한다고 하여 두쿠(Duqu)라는 명칭으로 지정했다. 두쿠의 목적은 제조 시스템과 산업 시설의 기밀 데이터를 수집하는 것이다. 수집되는 데이터에는 산업 통제 시스템의 설계 정보도 포함하기 때문에 앞으로의 추가적인 공격을 수행하는데 중요한 정보가 된다.

공격자들은 시스템 정보 수집과 키 입력 정보를 얻을 수 있는 인포스틸러(Inforstealer) 설치를 위해서 두쿠를 사용하여 앞으로의 공격에 사용할 수 있는 정보 자산을 검색하거나 유출시킨다.

두쿠는 드라이버 파일, DLL파일(임베디드 파일 포함), 구성파일(configuration file)로 되어 있다. 이 파일들은 프로세스 등록의 과정을 통하여 두쿠의 활동을 숨기고, 보안 제품들을 우회 할 수 있도록 한다.

두쿠는 하나 혹은 그 이상의 다른 C&C 서버(Command & Control Server)들을 사용한다. C&C 서버를 통해서 공격자들은 추가적인 실행 파일을 다운받고, 연결된 네트워크 정보, 키 입력 정보를 수집한다. 또한, 시스템 정보 수집을 하기 위한 인포스틸러를 포함시킨다.

두쿠는 스턱스넷과 많은 코드들이 유사하지만, 페이로드(Payload)는 완벽하게 다르다. 여기서 말하는 페이로드란 악성코드가 수행하는 악의적인 작업을 일으키는 데이터의 일부분을 말하는데 두쿠는 산업 제어 시스템을 파괴하기 위한 스턱스넷의 페이로드보다는 일반적인 원격 접근을 위한 페이로드를 가지고 있다.[1]

추가적으로 2015년 중순, 카스퍼스키(kaspersky)에서는 두쿠 1.0의 발전된 버전인 두쿠 2.0의 등장을 보고했다. 두쿠 2.0은 두쿠 1.0과 같은 제로데이 취약점(CVE-2014-4148)을 이용하며, 두쿠 1.0만의 로그 생성 방식과 독특한 문자열 역시 공유하고 있다. 진화된 두쿠 2.0은 감염된 시스템의 커널 메모리 안에서만 작동하며 어떠한 파일이나 기록을 남기지 않기 때문에 안티 바이러스 프로그램이 탐지하거나 분석하기 어렵다. 두쿠 2.0은 최근 서양, 중앙아시아, 동아시아 등 다양한 지역에서 발견되었으며 현재까지 두쿠 2.0의 최초 감염경로는 밝혀지지 않았다.[2]

2.1.2. 감염 경로

두쿠는 특별히 조작된 MS워드문서를 공격 대상에게 전송한다. 이 문서는 공격 대상 시스템의 제로데이 커널 취약점을 이용해서 공격대상이 모르는 사이에 공격대상 PC에 두쿠를 설치시킨다. 이후 두쿠는 쉘코드(shellcode) 취약점을 통하여 설치가 진행되며 최종적으로 자신의 흔적을 지우는 구조를 가지고 있다.[1]

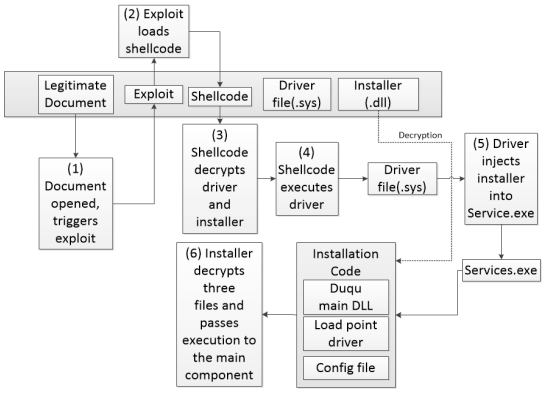
2.1.3. 설치 과정

다음은 그림은 W32.Duqu의 설치 과정이다.

(1) 워드 문서를 열었을 때 쉘코드 취약점을 이용하여 동작을 수행한다. (2) 이 취약점은 디렉토리의 레지스트리 값(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\“CF1D”)으로부터 컴퓨터가 손상되었는지를 확인한다. 만약 컴퓨터가 이미 손상되었다면 쉘코드는 정상적으로 종료된다. 만약 손상되지 않았다면, (3)쉘 코드는 워드 문서 내부의 드라이버 파일과 DLL 설치 파일의 정보를 추출한다. (4) 쉘 코드는 추출된 드라이버 파일을 실행시키기 위해서 (5)services.exe 파일에 코드를 등록한다. 이 쉘코드는 DLL 설치 파일을 실행하고, 자기 자신을 제로 값으로 대체하며 메모리로부터 스스로 삭제된다.

이후에 DLL 설치의 제어를 전달하게 되고, 내부 스스로 세 개 파일(Duqu’s main DLL,.sys driver file, configuration file)로 구성된다. 드라이버 파일은 재부팅 이후에 두쿠가 동작하는 로드 포인트이다. 설치 설정 파일은 두 개의 타임스탬프(timestamps)를 이용하여 설치를 진행한다. (6) 인스톨러(Installer)는 주요 컴포넌트를 실행시키고 세 개의 파일을 추출한다.

두쿠는 이러한 복잡한 설치 과정을 통해서 디스크에



〔그림 1〕 W32.Duqu 설치과정

서 흔적을 최소화 하도록 설계되었다.[1]

2.2. 레긴(Regin)

2.2.1. 개요

레긴은 공격 목표에 따라서 다른 기능으로 동작하는 정교한 악성코드이다. 레긴의 주요 목적은 정부 조직, 인프라 운영, 비즈니스, 학교, 개개인의 데이터에서 정보를 수집하는 것이다. 레긴은 여러 단계를 거쳐서 공격이 이루어지며, 모듈러 접근을 통하여 공격 목표에 따라서 유연하게 동작한다. 특히, 여러 단계로 로딩(loading)되는 아키텍처는 두쿠(Duqu)/스턱스넷(Stuxnet)과 유사한 컴포넌트를 가진다.

레긴은 전형적인 APT공격과 그 목적이 다르다. 전형적인 APT 공격들은 특정 정보나 일반적인 지적 재산을 획득하는 것이라면, 레긴은 목표 대상인 조직이나 개개인의 데이터 수집과 지속적인 모니터링을 위해서 사용한다.

레긴을 통하여 추가적인 페이로드 설치를 하거나, 또는 공격 대상에 맞추어서 페이로드를 제작한다. 기본 기능은 RAT(Remote Access Trojan)형태로 마우스 커서를 조정하는 기능과 스크린 샷 캡쳐 기능을 가진다. 또한, 대상 PC의 패스워드 도용과 네트워크 트래픽 모니터링을 수행하며, 프로세스와 메모리 정보를 훔친다.

레긴은 특히 모듈 형태로 제작되기 때문에 목표대상에 따라 다른 모듈이 제작된다. 예를 들면, 한 모듈은 마이크로소프트의 IIS(Internet Information Service) 웹 서버의 네트워크 트래픽을 모니터하기 위해 설계되거나, 다른 모듈은 모바일 기지국 컨트롤러를 관리하는 트래픽을 수집한다. 또한, Exchange 데이터베이스의 메일을 파싱(parsing)하기 위해서 모듈이 만들어지기도 한다.

레긴은 대규모 데이터 수집을 위한 매우 정교하고 복잡한 위협이다. 이 위협의 개발 및 운영은 특별한 자원과 시간의 투자가 필요하며, 레긴의 많은 컴포넌트들은 여전히 발견되지 않았고, 추가적인 기능과 버전들이 존재한다고 본다.[3]

2.2.2. 감염 경로

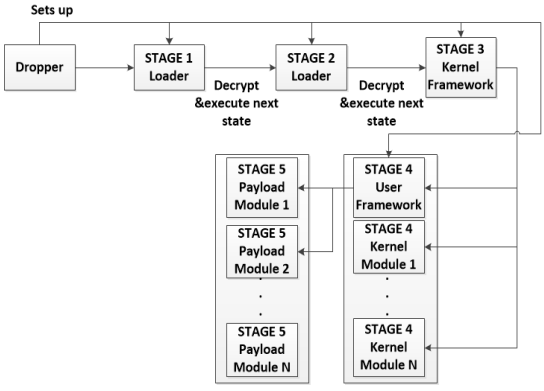
공격자는 공격 대상을 많이 알려진 웹 사이트의 스푸핑(Spoofing)을 통하여 속인다. 이후에 공격대상의 시스템에 웹 브라우저를 통하거나 어플리케이션의 취약점을 이용하여 레긴을 설치시킨다. 한 예로, 유명 메신저 어플리케이션의 취약점을 통해서 공격대상 시스템에 레긴을 설치시킨 것이 로그 파일을 통해서 확인되었다.[3]

2.2.3. 설치 과정

다음 그림은 레긴이 설치되는 과정이다.

레긴은 6단계의 아키텍쳐를 가진다. 초기단계인 0단계에서는 드롭퍼(dropper)의해서 1차적으로 공격 대상 시스템에 레긴이 넘어가게 된다. 여기서 말하는 드롭퍼란 컴퓨터 사용자가 인지하지 못하는 순간에 바이러스 혹은 트로이 목마 프로그램을 사용자의 컴퓨터에 설치하는 프로그램을 말하는데 이를 통해서 레긴을 넘겨주게 되는 것이다. 이후에 1단계로 넘어가게 된다.

1단계에서는 위협을 위하여 커널 드라이버 파일을 이용한다. 여기서는 커널 드라이버 파일이 로드가 되면 레지스트리 키나 시스템 서비스로 등록하여 로드 포인트를 초기화 한다. 2단계에서는 커널 드라이버를 추출하고, 확장된 속성과 레지스트리 키 정보가 암호화한다. 또한 1단계의 인스턴스를 숨겨서 실행할 수 있다. 3단계에서는 압축, 암호, 네트워크 루틴을 제공하고, 암호화된 가상파일 시스템을 다루는 과정을 한다. 3단계에서는 모듈 프레임 워크를 기반으로 하는 코드 모듈을 가지는데 이 모듈은 사용자 인터페이스를 통해서 기능들을 제공한다. 4단계에서는 암호화된 가상파일 시스템을 처리한다. 또한 사용자 정보를 유출시키기 위한 기술이 제공된다. 5단계에서는 메인 페이로드들로 구성되어 있다. 4단계에서의 파일들은 service.exe파일에 등록되어 있어서 5단



〔그림 2〕 Regin 설치 과정

계의 동작을 돕는다. 레긴의 페이로드는 SystemLog.evt EVFS 컨테이너에 포함 된 DLL파일을 포함하게 되는데 이는 대상 시스템에 따라 페이로드 기능이 다르게 동작하게 해준다.

즉, 공격 대상의 환경에 맞추어 사용자 페이로드의 전송이 이루어진다.[3]

2.3. 다이어(Dyre)

2.3.1. 개요

다이어는 전 세계 수많은 금융기관 고객들의 돈을 사취할 수 있는 가장 위험한 인터넷뱅킹 정보 탈취형 악성바이러스로 부상하고 있다.[7]

다이어는 세 개의 메이저 웹 브라우저(Internet Explorer, Chrome, Firefox) 모두 하이재킹(Hijacking) 할 수 있으며 피해자의 로그인 정보를 탈취하고 공격자에게 해당 정보를 보내기 위해 인터넷 뱅킹 세션을 가로채는 등의 공격을 할 수 있는 매우 발달된 악성 바이러스이다. 다이어는 로그인 정보를 탈취하기 위해서 정상 웹 페이지와 똑같은 가짜 웹페이지를 만들거나, 정상 URL에 악성코드를 삽입해 사용자의 개인정보를 탈취하는 man-in-the-browser(MITB) 공격 기술을 사용한다.

다이어는 크게 어퍼트리(Upatre), C&C서버, 다이어 악성코드에 의해 동작한다. 어퍼트리는 다이어 악성코드를 다운로드 하고 설치하는 32Kb의 초경량 다운로더이다. 주로 스팸 전자메일에 첨부되어 피해자 PC에 설치된다. 다이어는 C&C서버와 I2P(Invisible Internet Project)통신을 하며 모듈 및 파일을 다운로드 하거나 특정한 설정을 바꾼다.

다이어 악성코드는 모듈 형태로 제작된 악성코드로, 다양한 모듈 기능을 바탕으로 하여 다음과 같은 여러 작업을 수행한다. 유효한 C&C서버의 리스트와 설정 및 모듈을 다운로드하고 특정 DLL파일(nw9vbe8cc4.dll)에 저장한다. 다운로드 된 모듈을 로드시키거나 MITB 공격을 수행하기 위해서 다른 프로세스에 특정 리소스(0y2hgif34, 4qvndmku0)을 삽입한다. 원격 서버로부터 명령을 받고, 추가적인 악성코드를 다운로드 받고 실행한다. 또한 다이어는 피해자의 정보 및 해당 시스템 정보를 모으고 공격자에게 전송하여, 공격자가 원격으로 피해자의 시스템을 운영할 수 있다. 이외에도 널리 위협을 전파하기 위해 봇넷(Botnet)으로 추가 된 피해자의 PC를 이용하여 수 천통의 스팸 메일을 보내는 등의 수많은 기능을 갖고 있어 매우 위협적이다.[4]

2.3.2. 감염 경로

다이어의 주요 감염경로는 스팸 전자메일이다. 일반적으로 전자메일은 구조가 간단하며 비즈니스 문서로 위장하기 쉽다. 악성코드가 포함 된 첨부파일 또는 악성 프로그램이 삽입 된 호스팅 링크가 첨부된 메일을 피해자가 열었을 때, 그 즉시 어퍼트리 다운로더가 피해자의 컴퓨터에 설치되게 된다.[5]

2.3.3. 설치과정

공격자는 일상적인 압축 파일로 위장한 어퍼트리 다운로더를 첨부하여 스팸메일을 피해자에게 전송한다. 피해자가 첨부 된 파일이나 악성링크를 클릭하면 어퍼트리 다운로더가 피해자의 PC에 설치된다. 설치 된 어퍼트리는 다양한 활동을 수행한다. PC에 보안 소프트웨어가 동작하고 있다면 탐지를 피하기 위해 URL과 페이로드를 동적으로 변경한다. 또한 “google.com”을 접속하여 인터넷 연결 상태를 체크하고, 연결이 되어 있다면 C&C서버와 최초로 연결한다. C&C서버는 원격 서버로부터 바이너리 형태의 다이어를 피해자의 PC에 다운로드하고 실행시켜 설치한다. 다이어가 설치되면 어퍼트리는 자동으로 삭제된다.

다이어는 지속적으로 감염된 PC에서 활동하기 위해 서비스명을 “Google Update Service"와 같은 내용으로 변경하고 컴퓨터 부팅 시 자동으로 동작할 수 있도록 설정한다. 그 후에 정상적인 SVCHOST.EXE에 악성코드를 삽입한다.

다이어는 peer-to-peer 터널링 네트워크를 연결하기 위해 I2P 노드들을 연결한다. 이 작업은 피해자의 PC에서 전송되는 정보들을 최종 목적지 및 내용들을 드러내지 않고 전송하기 위함이다. 동시에 다이어는 피해자의 PC에 설치되어 있는 Internet Explorer, Chrome, Firefox와 같은 브라우저를 후킹한다. 위와 같은 작업을 통해 공격자는 피해자가 은행 등 금융과 관련된 사이트에 개인정보를 기입했을 때 그 정보들을 가로챌 수 있다.[4]

Ⅲ. 은닉형 악성코드를 활용한 공격 사례 분석

은닉형 악성코드는 흔적을 남기지 않는 기능을 가지고 있어 악성코드의 유포지를 찾기가 쉽지가 않으며 이를 탐지하기도 쉽지 않다. 많은 국가와 기관들이 파악한 내용에 따르면, 이미 알려진 시스템 감염 통계보다 많은 악성코드들이 침입하여 잠입해있을 것으로 예상한다. 본 부분에서 은닉형 악성코드 공격 사례의 분석을 통하여 그 위험성을 인식하도록 한다.

3.1. 주요 8개 나라의 두쿠 감염

시만텍(symantec) 측에서 두쿠의 감염이 지리적 분포에 따라서 6개 조직과 8개 나라에서 확인되었다고 밝혔다. 6개 조직의 조직 A는 프랑스, 네덜란드, 스위스, 우크라이나이며 조직 B는 인도, 조직 C, D는 이란, 조직 E는 수단, 조직 F는 베트남으로 이루어져 있으며, 감염을 보고한 벤더사들은 호주, 헝가리, 인도네시아, 영국, 이란 등에 걸쳐서 확인되었다. 또한, 일부 조직들만이 조직에 따라서 ISP(Internet Service Provider)로만 추적 할 수 있다고 알렸지만, IP 주소가 그룹화 되었기 때문에 명확하게 조직을 식별 할 수 없다고 한다.[1]

지리적인 감염 분포를 보면 특정 지역에 집중적으로 감염된 것이 아니라 아시아, 유럽, 아프리카 대륙전반에 걸쳐 감염 된 것으로 보인다. 또한, 아직 확인 되지 않은 두쿠 감염이 있을 것으로 예상되며 어딘가에서 은닉 활동을 하고 있을 것으로 본다. 이러한 분포 사례를 통하여 두쿠의 악의적인 특징을 인식할 수 있다.

3.2. 다양한 감염 대상을 갖는 레긴

시만텍 측에서는 레긴은 특별한 산업 분야에 초점을 두지 않고, 다양한 조직, 회사, 정부 기관 및 연구소 등에서 감염이 관찰되었다고 한다. 또한 감염은 10개의 다른 지역에서 식별되었고 지리학적으로 다양했다.[3]

특히 레긴은 스푸핑 된 웹 사이트를 이용하는 방식이기 때문에 공격자에 의해서 스푸핑 된 웹 사이트에 어떤 사용자가 접속을 하냐에 따라서 감염이 결정된다. 이로 인하여 다양한 감염대상이 발생한다.

3.3. 금융기관 고객을 노리는 다이어

다이어는 금융 쪽으로 특화 된 악성코드로서, 2014년 6월부터 활동하기 시작했다. 2015년 초엔 다이어로 인해 4000대 이상의 시스템이 감염되어 피해가 큰 폭으로 증가되었다.[4] 다이어의 주요 공격 대상은 전 세계적으로 유명한 은행을 이용하는 고객들이며, 특히 영국과 미국의 주요 은행을 포함한 영어권 국가에 초점이 맞춰졌다.

이외에도 전자 거래 서비스 이용 고객은 물론이고 HR과 같은 개인정보가 많은 웹 사이트, 웹 호스팅 서비스를 제공하는 업체 등 수 다양한 사이트들이 다이어의 공격 목표가 된다. 다이어 공격의 주목적은 재정적인 이익이지만, 이외에도 C&C 서버의 인프라를 키우기 위해서도 공격한다.[5]

Ⅳ. 대응방안에 대한 고찰

은닉형 악성코드로부터 발생되는 위협을 대응하기 위해 개인 또는 기관들은 여러 가지 보안대책을 세울 수 있다. 본 장에서는 이러한 공격기술에 대비할 수 있는 대응책에 대하여 고찰해본다.

4.1. 관리적 보안방안

· 웹페이지 개발 시 보안 인식 및 시큐어코딩

은닉형 악성코드는 웹 취약점을 이용하여 공격대상 PC 침입을 하는 경우가 있다. 개인 혹은 기업에서는 웹페이지 개발 시 개발자의 보안 인식 확립과 시큐어 코딩을 통하여 취약점 요소를 최소한으로 줄이고, 관리자는 주기적으로 취약점 점검 및 패치를 통하여 웹 서버가 해킹되지 않도록 해야 한다.[6]

즉, 기업이나 기관에서 프로젝트를 진행할 경우에 개발 및 구현 단계에서부터 보안을 인식하고 이를 적용하려는 노력이 필요하다고 생각한다.

· 관리자 보안 교육

관리자 사전교육과 보안인식 훈련은 보안 사고를 예방하는데 중요하므로 지속적으로 수행해야 한다. 특히, 어떤 시스템 또는 사이버 위협이 발생했을 경우, 관리자들이 취해야 하는 행동 또는 하지 말아야 할 행동들을

사전교육을 통해 배워야 한다.

관리자는 공격자, 스팸 그리고 피싱 공격 등에서 사용되는 일반적인 기술을 숙지하고 있어야하며 시스템이 비정상적일 경우 어떻게 그리고 누구에게 보고해야 하는지 또한 알고 있어야 한다.[4]

4.2. 기술적 보안 방안

· 전자메일의 첨부파일 중 실행 가능한 파일 제거

대부분의 공격자들은 은닉형 악성코드를 압축파일로 만들어 전자메일에 첨부하여 보낸다. 기관들은 대게 메일서버의 게이트웨이에서 메일에 첨부 된 실행파일은 제거하지만 압축파일은 스캔만 할 뿐 제거하지 않는다. 결국 그 파일은 사용자의 메일함이나 단말기까지 도달하게 된다.

따라서 기관들은 악성파일이 사용자의 메일함에 도달하지 않도록, EXE, COM 또는 SCR 등의 확장파일이 포함 된 압축파일 역시 메일 서버가 제거할 수 있도록 설정해야 한다.[4]

· 악성코드 탐지 후 시스템 재시작

바이러스 스캐너는 파일 시스템에서 은닉형 악성코드를 발견하면 삭제하거나 격리한다. 하지만 은닉형 악성코드의 대부분이 악성코드를 삽입 한 메모리에서만 보통 동작한다. 그렇기 때문에 시스템을 재시작할 때까지 은닉형 악성코드가 탐지되고 시스템에서 삭제되더라도, 악성코드가 메모리에 존재하면 피해자의 정보 등을 가로채거나 훔칠 수 있다.

이에 따라 관리자들은 은닉형 악성코드가 탐지되었을 경우 악성코드를 삭제할 뿐만 아니라, 시스템 역시 다시 부팅해야한다.[4]

· 임시폴더(temp folder)에서 프로그램 실행 제한

대부분의 시스템 감염경로의 시작은 임시폴더이다. 악성코드가 다운로드 되면 주로 임시폴더에서 처음 실행된다. 또한 악성코드는 실행만을 유지하기 위해 임시폴더에 악성코드파일을 복제한다.

이러한 행위들을 방지하기 위해서 가능하다면 임시폴더에서 어떠한 프로그램도 실행할 수 없도록 그룹 정책 개체(Group Policy Objects; GPO) 또는 소프트웨어 제한 정책(Software Restriction Policies; SRP)을 수립하는 것이 좋다.[4]

· 개인 및 기관의 보안점검 및 패치

대부분 사용자들은 단말기에 설치 된 백신프로그램을 설치했을 때의 버전 그대로 사용한다. 은닉형 악성코드는 백신프로그램의 탐지를 우회하기 위해 지속적으로 발전한다. 진화된 악성코드를 방어하기 위해선 항상 백신프로그램을 최신 상태로 유지해야 한다.

또한, 공격자는 개인이나 기관이 사용하는 운영체제나 어플리케이션의 취약점을 노리는 제로데이 공격을 일으킬 수 있다. 이 또한 공격 방어를 위해서 항상 최신의 업데이트를 유지해야한다.[4]

즉, 개인이나 기관에서는 지속적으로 보안점검 및 보안 패치를 함으로써 공격에 대응하려는 노력이 필요하다.

Ⅴ. 결 론

본 고에서는 APT 공격의 핵심 기술 중에 하나인 은닉형 악성코드에 대해서 살펴보고, 공격사례를 통하여 이를 대비할 수 있는 대응방안에 대해 고찰해 보았다.

은닉형 악성코드는 변종을 일으키거나, 스스로 자신의 흔적을 지우는 기능들을 가지는 아키텍쳐를 가지고 있다. 이로 인해서 시스템의 백신, 방화벽, IDS/IPS가 탐지하지 못하고 우회를 하게 되는 결과를 가지게 된다. 이러한 공격을 대비하기 위해서는 1차적으로 보안 장비와 시스템의 취약점을 지속적으로 관리하고 업데이트를 해줘야한다. 하지만 이러한 대비책은 사고가 발생하였을 때 해당 문제만 해결하는 단기적인 대비책일 뿐이며 보안시스템을 우회하고 숨어드는 은닉형 악성코드의 원천적인 문제를 해결하진 못한다.

최근 국내외로 은닉형 악성코드를 이용한 APT공격으로 많은 피해를 입었다. 하지만 이러한 사고에 대한 대비책은 대부분 일시적인 대응책일 뿐이다. 이를 해결하기 위해서는 기술적 접근뿐만 아니라 보안인식 훈련과 같은 교육적 입장과 관리적 보안까지 고려해야 한다. 또한 원천적인 문제를 해결하려는 전략적인 보안관리 체계가 필요하다.

향후에는 지금보다 지속화, 지능화되는 APT 공격으로 인한 보안사고가 발생할 것이다. 이에 따라 장기적인 관점으로 보안사고가 발생하였을 때 피해를 최소한으로 줄이고 원천적인 문제를 고려하는 대응방안에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] Symantec Security Response, “W32.Duqu The precursor to the next Stuxnet Version1.4”, November 2011.

[2] kasperskylab, "THE DUQU 2.0 Technical Details Version2.1", June 2015.

[3] Symantec Security Response, "Regin: Top-tier espionage tool enables stealthy surveillance Version1.0", November 2014.

[4] IBM MSS, "THE DYRE WOLF:ATTACKS ON CORPORATE BANKING ACCOUNTS", April 2015.

[5] Symantec Security Response, "Dyre:Emerging threat on financial fraud landscape Version1.0", June 2015.

[6] 침해사고 대응단, “월간 악성코드 은닉사이트 동향 보고서[11월]”, December 2013.

[7] 안랩, “금융정보 탈취 악성코드 '다이어(Dyre)'”, July, 2015.

[8] F5SOC “Dyre Malware Analysis”, November 2014.

[9] 이현목, “은닉형 악성코드, 대체 뭐길래?”, 안랩(AhnLab) 보안 이슈, December 2014.

[10] 박형근, “스턱스넷(Stuxnet) 상세 분석 보고서”, IBM Security, December 2010

〈저자소개〉

지 선 학 (Seon-Hak Ji)
학생회원

2015년 2월 : 강원대학교 정보통신공학과 졸업
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 모바일보안, S/W보안, 악성코드

박 지 윤 (Ji-Yun Park)
학생회원

2014년 8월 : 서울여자대학교 정보보호학과 졸업
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> ISMS, 시스템보안, 네트워크보안

이 재 우 (Jae-Woo Lee)
동국대학교 국제정보대학원 석좌교수(현)
한국포렌식조사전문가협회 회장(현)
ISC2 Fellow, Asia Board 의장(현)
한국 CSO 협회 자문위원장(현)
한국정보보호진흥원 초대 원장