이것만은 알아야 할 네트워크 보안 이야기

Part 11. APT 4. APT 공격 가상시나리오, APT 공격 방어장비

글. 이선응 아이크래프트 수석
ka3211a@gmail.com

이번 호에서는 다양한 단계를 통해 수행되는 APT 공격에서 조직 내 침투단계부터 침투 후 내부확산단계에 이르는 과정을 가상시나리오를 통해 설명하고 어떻게 공격을 탐지하여 방어할 것인가에 대해 알아보도록 하겠다.

연재 목차

지난 호에서 설명한 APT 공격방식을 기반으로 방송국에서 일어날 수 있는 APT 공격을 통한 방송시스템 가상공격 시나리오를 예상해 보았다. 공격자는 인터넷을 검색하던 중 방송국의 전산실 엔지니어로 재직 중인 사람의 블로그를 검색하다가 회사 이메일을 알게 되었다. 해당 엔지니어가 개인 블로그 게시글 중에 PC 화면을 캡처해서 올렸는데 화면 가장자리에 작게 보이지만 이메일이 같이 노출된 것이다. 공격자는 '택배 배송조회'라는 이름으로 URL을 첨부하여 이메일을 보냈으나, 엔지니어는 해킹 메일인 것을 인지하고 이메일을 바로 삭제하였다. 공격자는 다시 한번 '방송시스템 최신 공격 동향'이라는 이름의 이메일에 '5G 시대의 방송시스템 보안위협실태'라는 제목의 워드 파일에 악성코드를 삽입시켜 전송하였다. 평상시 같으면 무시했을 이메일이었지만, 마침 그때 전산팀에서 보안강화를 주제로 세미나를 준비 중이라 관련 자료를 수집 중이던 엔지니어는 자기도 모르게 해당 파일을 열어보게 되었다. 나름 참고할 만한 내용이 포함되어 있어 만족하며 데이터 폴더에 저장도 해 두었다. 그런데 워드 파일을 열어보면서 같이 첨부되어 있던 익스플로잇이 작동하면서, 악성코드가 엔지니어의 노트북에 설치되고 말았다.

악성코드는 사전에 설정된 공격자의 서버로 침투 성공 메시지를 보내게 되고, 공격자는 악성코드를 통해 감염된 PC의 화면뿐만 아니라 저장장치에 접근이 가능하게 되었다. 바탕화면을 보니 '패스워드 리스트-2007'이란 이름의 텍스트문서가 보여 클릭해 보니 전산실에서 직접 관리하는 각종 네트워크 장비와 주요 서버에 대한 계정정보를 확인할 수 있었

다. 공격자는 AD(계정관리서버 : Active Directory) 서버의 관리자 계정정보를 확인하고 감염된 PC를 통해 AD 서버에 접속하여, 사내업무망뿐만 아니라 방송제작망, 송출망에 있는 주요 서버의 IP 주소와 접속계정정보를 확보하게 되었다.

먼저 방송제작망에 있는 서버를 확인해 보니 영상편집서버가 눈에 띄어 AD 서버를 통해 접근해 보니 다량의 편집본과 원본 방송데이터가 보관되어 있는 것을 확인하였다. 한 달에 걸쳐 꼼꼼히 방송데이터를 검색해 보니 최근에 인기가 높은 리얼리티 연애방송의 데이터가 눈에 들어왔다. 공격자도 평상시 즐겨 보고 있던 프로그램인데, 아직 방송도 되지 않은 편집본이 있어 공격자는 방송 전 영상을 미리 확보할 수 있었다. 그뿐만 아니라 편집되기 전의 미방영 영상도 찾아볼 수 있었다. 공격자는 확보한 영상의 추적을 피하고자 토렌트를 통해 조금씩 공유하여 유출하기 시작하였다.

한편 공격자는 송출망의 송출 서버에도 접근할 수 있게 되었다. 송출서버가 어떻게 작동하는지 배경지식이 없어서 3개월 동안 서버의 동작 방식도 확인하고 프로그램 이름을 확인하여, 인터넷을 통해 프로그램 매뉴얼을 확보하고, 송출프로그램이 어떻게 작동하는지 익숙해지게 되었다. 그러던 중 평소 다크웹을 통해 해킹툴을 찾다가 새로운 게시글을 보게 되었다. 내용은 공중파 방송국, 대기업 전산실, 은행의 운영시스템에 대한 접근 권한을 제공해 주면 중요도에 따라 최고 1억 원을 주겠다는 제안이었다. 마침 공격자는 평소에 봐두었던 새로 나온 외제차가 생각이 났다. 이 정도 금액이면 충분히 새 차를 장만할 수 있겠다는 생각이 들었다. 고민을 거듭하다가 해당 게시글에 있는 이메일로 송출서버에 대한 접근정보를 제공해 주는 대가로 1억을 요구하였다. 협상을 통해 8천만 원을 비트코인으로 받기로 하고, 방송국의 송출서버 접근정보 및 송출프로그램의 동작 방식을 정리한 문서를 전달하였다. 우선 송출 서버 한 대에 대한 접근정보를 받은 구매자는 송출 서버의 구조와 동작 상태를 확인한 후 비트코인을 전달하고 나머지 송출 서버의 접근정보와 동작 방식을 정리한 문서를 전달받게 된다.

송출 서버의 접근정보를 획득한 구매자는 이웃 국가의 정보기관과 관련이 있는 해커집단이었다. 이 해커집단은 송출시스템에 접근하여 송출 서비스를 중단시킬 방법을 확인하고, 정보기관에 보고하게 된다. 마침 이웃 국가는 우리나라와 여러 가지 문제로 마찰을 빚고 있는 와중이었다. 이웃 국가의 최고의사 결정자는 이번 봄에 있을 대통령선거에 개입하여, 영향력을 과시해야겠다고 결정하고 가능한 수단을 강구하라고 지시했다. 마침 정보기관은 확보하고 있던 방송국 송출시스템을 이용하여 대통령 선거개표방송을 중단시키는 방식으로 개입이 가능하다고 보고했고, 해당 계획은 실행에 옮겨지게 된다. 선거개표방송 시작 시각인 18:00가 되자 송출시스템 서버 5대의 저장장치를 모두 포맷하고 재부팅 시켜 송출을 중단시킨 것이다.

송출담당자는 갑자기 송출이 중단된 것을 확인하고 송출 서버에 접근을 시도했지만 접근이 되지 않았다. 서버실에서 직접 콘솔에 접속해 보았지만 서버는 흑백화면만 표시할 뿐이었다. 다행스럽게도 선거개표방송을 준비하면서 만일의 사태에 대비해 전날에 송출 서버를 백업해 두었던 것이 희망이었다. 백업시스템 담당자가 급히 송출 서버의 복구를 시작하였으나, 복구에는 1시간이 소요되었다. 복구된 이후에도 연계시스템과의 테스트 및 설정 확인해 1시간이 소요되었다. 최초 원인파악에 1시간을 포함해서 개표방송이 복구되는데 3시간이 걸린 것이다. 사후대응팀이 확인해 보니 공격자는 전 세계 15개 국가의 20개 시스템을 경유하여 송출 서버에 접근한 것으로 밝혀져 정확한 공격자의 신원파악은 실패하였다. 단지 최근 여러 가지 문제로 대립 중인 이웃 국가가 후원하는 공격집단이 공격자가 아닌지 심증을 가질 뿐이었다.

다음 페이지의 [그림 1]은 위에서 설명한 가상공격 시나리오를 간략하게 정리하여 표시한 내용이다.

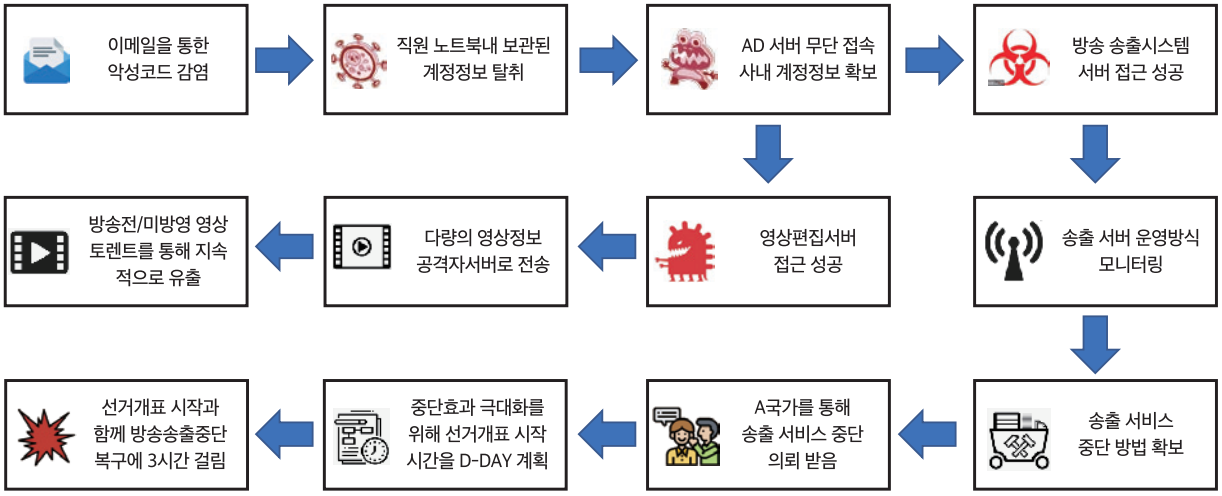


그림 1. APT 공격을 통한 방송시스템 가상공격 시나리오

업무에서의 인터넷과 이메일 사용이 활성화되면서, 조직 내에 있는 단말을 아주 쉽게 감염시켜 공격에 사용할 수 있게 되었고 인터넷 구간에 집중되어 운영 중인 방화벽, IPS 등의 다양한 보안 장비들만 가지고는 완벽한 보안이 불가능하게 되었다. 대부분의 공격이 애플리케이션 레벨의 웹이나 이메일에 첨부된 파일 또는 URL 클릭을 유도하여 감염시키기 때문에 악성코드 및 URL 등의 정보(공격침해지표 : IOC)가 없는 상황에서는 공격에 대한 탐지와 차단이 불가능한 상황이 되었다. IOC 정보를 공유받아 방화벽과 IPS를 통해 알려진 공격을 막는다고 하더라도 공격그룹에서 새로운 공격인프라(공격하기 위해 이용하는 해킹한 서버, 경유지로 활용되는 해킹된 단말 PC, 사용한 악성코드 등)를 사용하면 공유받은 IOC는 효용 가치가 떨어지게 된다.

그래서 알려지지 않은 악성코드나 URL 등의 공격 인프라에 대해 악성 여부를 사후에 인력이 분석하는 것이 아니고, 방어 장비 내에서 실시간으로 확인할 수 있는 탐지체계가 필요하였고 이를 위해 동적 분석방식이 개발되었다. 동적 분석방법이란 악성코드의 파일 패턴 분석을 통해 알려진 악성코드인지 여부를 판별하는 정적 분석방식에 비해, 가상화 시스템에 직접 악성코드를 다운로드하여 악성 행위를 모니터링하고 악성 여부를 판별하는 방식을 사용하기 때문에 변종 악성코드 같이 알려지지 않은 검사대상에 대해 악성 여부 판단이 가능한 장점이 있다. 이러한 기술 방식을 통상 샌드박스(Sandbox)라고 불린다. 우측 [그림 2]와 같이 모래 상자(샌드박스)는 모래로 채워진 상자를 방벽으로 테스트를 할 경우 폭발하더라도 실험자의 안전을 지키기 위해 사용하는 장치이다. 즉, 악성코드로 의심되는 파일을 가상시스템에서 검사를 수행하여 주위의 시스템에는 감염의 위험이 없도록 격리된 환경 내에서 악성 여부를 확인하는 장비를 샌드박스 방식이라고 한다. 처음에는 바이러스 백신 업체에서 백신에 대한 테스트 목적으로 시작된 체계였으나, 자동화 기능이 추가되면서 하나의 독립된 보안기술로 발전하였다.

그림 2. 폭발물의 위험으로부터 안전을 지키기 위한 모래방벽(Sandbox)

아래 [그림 3]은 실제 샌드박스 가상화시스템에 악성코드를 다운로드 시켜 악성코드가 동작하는 행위를 분석한 다이어그램이다. 익스플로러 웹브라우저를 통해서 파일을 생성하거나 기존 파일을 변경, 복사하고 특정 URL에서 파일을 다운로드하는 등 다양한 행위가 모니터링되어 악성 동작 여부를 판단하는 기준으로 활용된다. 기존에 알려진 악성코드는 파일의 패턴을 통해 인지가 가능하지만 신규로 만들어진 변종 악성코드의 경우 이런 식으로 동작시켜 보지 않으면 악성 여부를 판단하기가 어려워 이러한 검사를 통해 확실한 악성 여부 탐지가 가능하다.

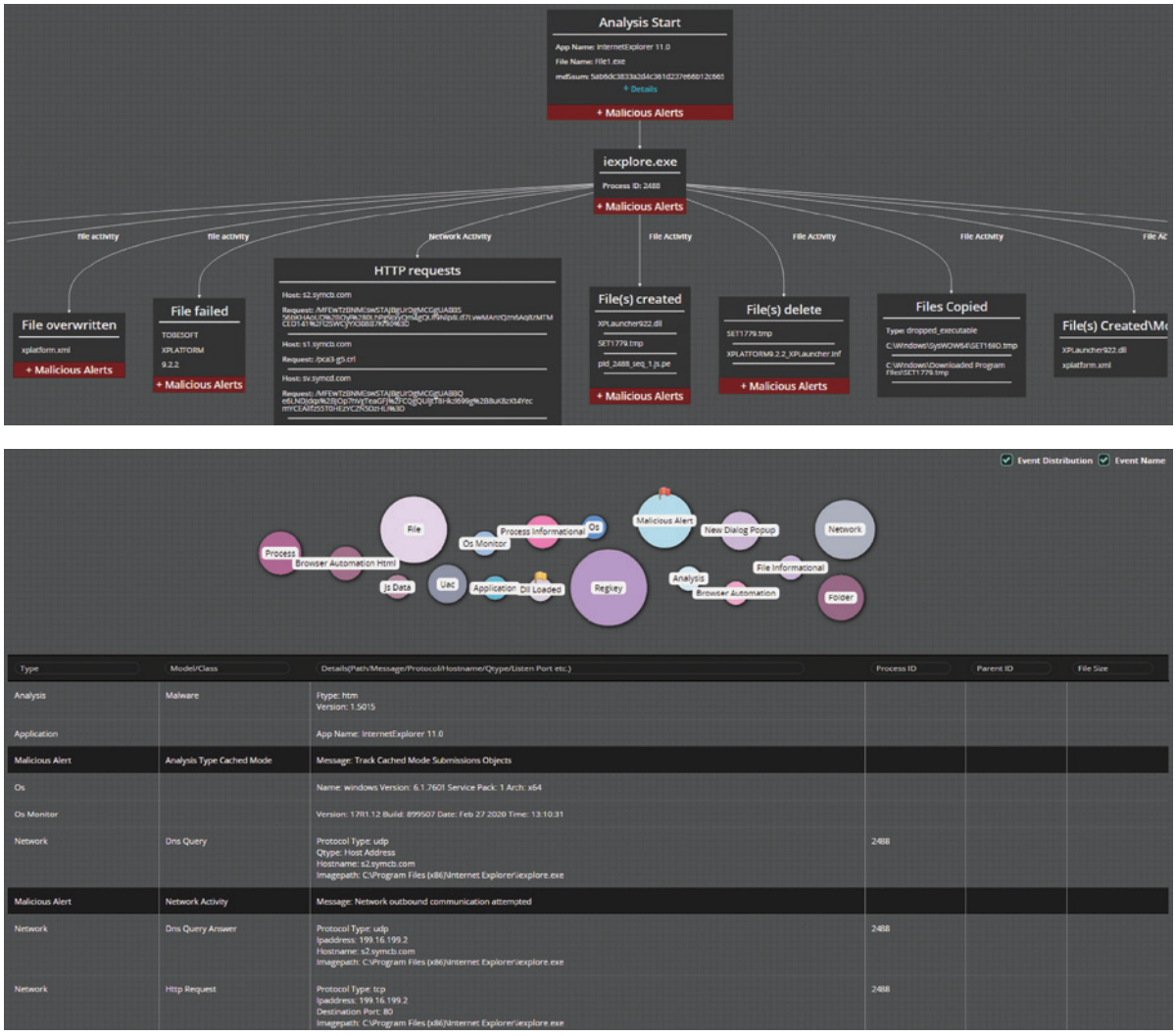


그림 3. 샌드박스 가상시스템에 분석한 악성코드 행위 분석 결과 / 출처 : FireEye

문제는 이러한 샌드박스 기반의 탐지방식이 만능이 아니라는 점이다. 악성코드를 개발하는 공격그룹에서 동작하는 환경이 샌드박스의 가상시스템인지를 확인하여 악성 행위를 하지 않는 방식으로 탐지를 우회하는 기능을 추가하기 시작하면서 악성코드 탐지율이 떨어지게 되었다. 더욱이 이러한 가상시스템을 동시에 여러 개를 동작시킬 경우 장비의 CPU, 메모리 등의 자원소모량이 기하급수적으로 늘어나 장비의 운영비가 늘어나는 문제가 발생한다.

이러한 문제를 보완하기 위해서 결국은 기존의 공격침해지표(IOC) 기반의 정보를 활용할 수밖에 없게 되었다. 기존의 방화벽, IPS 장비에 알려진 공격침해지표를 입력하는 방식은 관리자가 일일이 수작업으로 수행하고, 이러한 IOC 정보도 실시간으로 공유되는 것이 아니어서 효용 가치가 떨어졌었다. 그러나 실제 현장에서 사용되고 있는 전 세계 고객의

샌드박스에서 수집된 다양한 악성코드의 정보와 모니터링된 악성 행위들(접속 URL 정보, 다운로드 파일 정보, 파일변경정보)에 대한 데이터를 실시간으로 공유하면 샌드박스 방식에만 의존하여 생기는 문제를 어느 정도 해결할 수 있다. 수집된 악성코드 정보를 중앙서버에 저장하고 고객에 설치된 장비에서는 실시간으로 저장된 악성코드 정보를 공유받아 악성코드 판별에 활용할 수 있게 되면서, 기존과 같이 일일이 샌드박스에서 동작시키지 않아도 좀 더 시스템의 부하 없이 신속하고 정확하게 탐지가 가능하게 되었다.

APT 공격은 DDoS 공격과 같이 네트워크에서만 방어한다고 차단이 가능한 공격이 아니다. 대부분의 공격이 단말을 통해서 이루어지고, 웹브라우저뿐만 아니라 이메일을 통해서 공격이 시작되기 때문에 모니터링해야 하는 대상이 다양하다. 아래 [그림 4]와 같이 웹브라우저를 통해 다운로드되는 다양한 파일들, 내부로 유입되는 첨부파일이 포함된 다양한 이메일, 업무에 이용되는 다양한 단말 기기들이 모두가 APT 공격을 탐지하기 위해 필요한 모니터링 대상이다. 네트워크를 통해 주고받는 패킷을 모니터링하여야 악성코드 및 C&C 서버의 통신 내역을 모니터링 가능하고, 이메일을 모니터링하여야 첨부되는 파일의 악성코드 여부와 메일 본문에 포함된 URL 검사가 가능하며, 단말기기를 통해 공격이 시작되므로 단말기기를 직접 모니터링하고 악성 행위를 차단시켜야 완벽한 공격 탐지 및 방어가 가능하다.

그림 4. APT 공격 방어를 위한 모니터링 대상

최근 가장 빈번하게 발생하는 공격은 악성코드뿐만 아니라 랜섬웨어를 첨부파일에 포함해, 파일을 열어보도록 유도하는 스피어피싱 공격이다. 기업의 이메일은 공개되어 있어 수집이 비교적 쉽고, 대량의 이메일을 전송하는데도 전산 자원이 많이 필요하지 않으며, 목표를 공격자가 지정해서 수신자의 상황에 맞게 메일 내용을 작성하여 공격 성공률을 높일 수 있어 이메일을 통한 공격이 가장 활발하게 이루어지고 있다. [그림 5]와 같이 공격대상의 선정이 쉽고 공격에 소요되는 자원이 적고, 공격 성공률이 비교적 높아 이메일을 통한 공격이 선호된다.

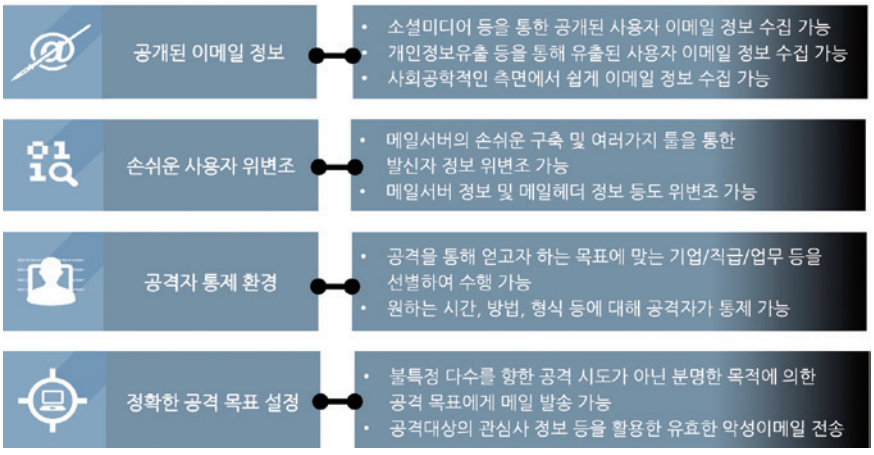


그림 5. 이메일을 통한 공격이 위협적인 이유

이제 이러한 이메일을 통한 공격을 탐지 및 차단하기 위한 방법을 알아보자. 아래 [그림 6]과 같이 이메일이 들어오면 메일에 첨부파일과 본문에 URL이 포함되어 있는지 검사한다. 이때 첨부파일이 포함되어 있으면 첨부파일에 대해 알려진 악성코드가 포함되어 있는지 파일에 대한 패턴분석을 시작한다. 이를 정적분석이라고 한다. 만약에 정적분석에서 악성코드가 검출되지 않는다면 동적분석 단계로 넘어가 다양한 OS가 포함된 가상시스템에 악성코드를 다운로드하여 동작을 모니터링한다. 파일을 생성하거나, 인터넷에서 특정 파일을 다운로드하여 설치하거나, 특정 서비스를 레지스트리에 등록하는 등 악성으로 판단되는 행위가 관찰되면 이메일을 차단하게 되고, 별다른 문제가 없으면 통과시킨다. 첨부파일 이외에 메일 본문에 URL이 포함되어 있다면, 해당 URL이 악성으로 등록되어 있는지 URL DB를 확인하고, 실제 URL을 통해 다운로드되는 파일을 분석하여 악성 여부를 검사하게 된다.

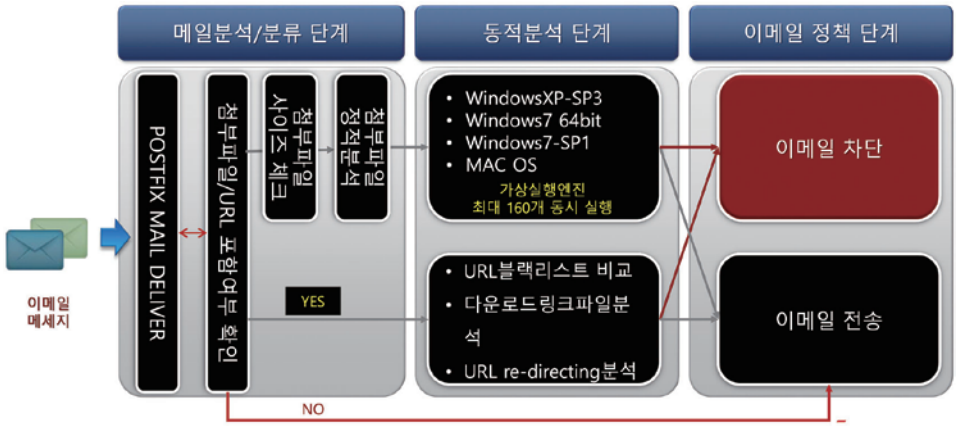
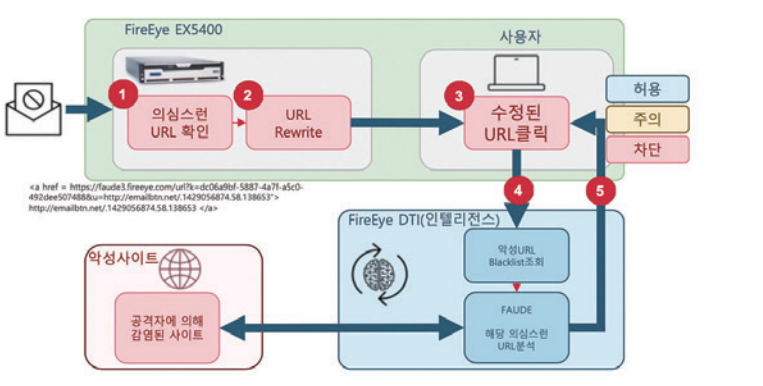
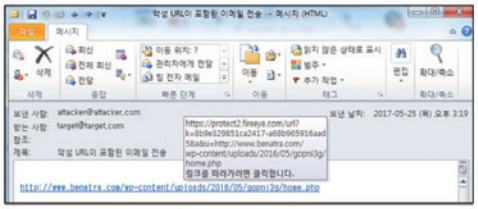


그림 6. 메일 분석 아키텍처 / 출처 : FireEye

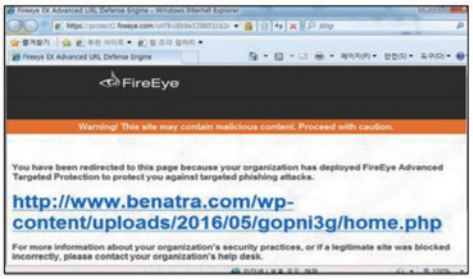
이제, 실제로 탐지된 악성이메일을 확인해 보자. 아래 [그림 7]과 같이 메일 본문에 있는 URL 링크된 파일을 실제로 다운로드하여 분석을 수행하고 문제가 있는 URL은 악성으로 등록하고 해당 이메일은 차단하는 방식을 사용한다.



1. EX에서 의심되는 URL을 추출하여서, DTI에 실시간 쿼리를 통해 확인
2. 만약, 해당 URL이 DTI상에 Unknown이라면, FAUD 엔진으로 보내져서 심층 분석 실행
3. URL은 수정되어서, 사용자에게 전달
4. 사용자가 실제 클릭할 때, DTI의 악성 URL DB를 통하도록 설정됨 :
   a. 만약, 악성이 맞다면, '차단' 페이지가 전송
   b. 정상이라고 판단된다면, 원래 URL로 전송
   c. 클릭 당시에도, Unknown인 경우에는 '경고' 페이지를 보여주고, 원래 URL로 전송



[실제 유입된 이메일]



[Fireeye DTI에서 분석된 화면]

그림 7. 이메일에 포함된 URL을 검사하는 절차 / 출처 : FireEye

다음으로 네트워크를 통해 트래픽을 검사하면 단말(호스트)에 감염되는 단계와 감염이 이루어진 이후 C&C 서버와 통신(Call back)을 하는 두 가지 단계의 탐지가 가능하다. [그림 8]과 같이 먼저 단말에서 웹브라우저를 통해 악성코드가 포함된 웹서버에 방문할 경우 악성코드가 단말에 도달하기 전에 네트워크를 통해 APT 탐지 장비에서 먼저 악성코드를 탐지할 수 있다. 그리고 이미 악성코드를 유포하고 있는 URL이 다른 사용자의 장비에서 탐지된 경우 중앙서버를 통해 해당 URL 정보는 공유를 통해 차단이 가능하다. 단말이 이미 악성코드에 감염된 이후라도 Callback(C&C 서버와의 통신) 단계를 통해 감염된 단말의 탐지가 가능하다. 이미 알려진 C&C 서버 리스트를 이용하여 통신 여부를 모니터링하고 트래픽 내에서 C&C 서버와의 통신에서 자주 사용하는 패턴을 확인하여 감염 여부를 파악할 수 있다.

	호스트 감염(Infection) 단계	감염 후 C&C와 통신(Call-back) 단계
발생 이벤트	**Web Infection** • 브라우저 취약성을 이용하여 악성코드가 침투 • 비정상 TCP 세션 생성 여부 모니터링	**Malware Callback** • C&C 서버와 통신하는 경우
	Malware Object • 웹 접속을 통해 악성코드가 다운로드되는 경우 • 해커는 사회공학적으로 악성코드 다운로드를 유도	**Domain Match** • C&C 서버 리스트에 포함된 도메인에 대한 DNS Query가 발생하는 경우
	Infection Match • 악성 URL 리스트에 포함된 도메인에 대한 접근 시도가 있는 경우	
위험등급	**Major** • 해커에 의해 공격을 당하는 초기단계	**Critical** • 해커의 공격으로 시스템의 제어권이 손상되어 정보 유출 또는 시스템 파괴가 가능한 상태
탐지방법	• 실제 다운로드 파일(MD5 Hash) 검사 • VXE에 의한 실제 행위 모니터링 • 악성 URL 리스트에 의한 탐지	• 사용 포트, 메시지 내용 등의 검사 • 알려진 C&C 서버 리스트와 통신 여부 검사

그림 8. 네트워크에서 APT 공격을 탐지하는 방식 / 출처 : FireEye

여기에서 악성코드 여부를 확인하는 방법도 정적분석과 동적분석방식을 모두 활용한다. 네트워크 트래픽으로 유입되는 HTML, JPG, EXE, ZIP 등을 파일 단위로 추출하고 재조립해서 우선 알려진 악성코드인지 확인해 보고 다음으로

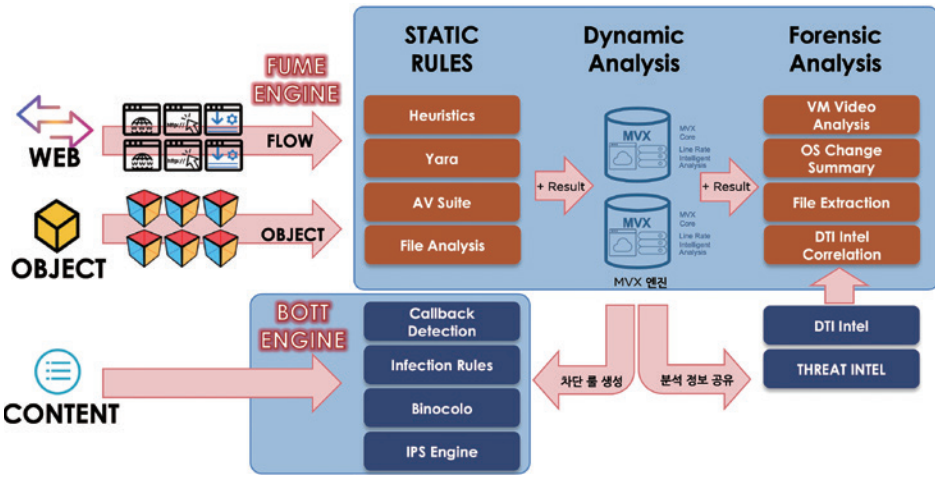


그림 9. 네트워크에서 APT 공격 분석 아키텍처 / 출처 : FireEye

가상시스템에 올려서 악성동작 여부를 확인하는데 악성코드로 판별되면 분석 결과를 중앙서버로 보내 다른 장비에서도 활용할 수 있도록 공유된다. 그리고 내부 단말에서 외부로 통신하는 내용을 모니터링하고 있다가 알려진 C&C 서버와 통신하는지, 통신내용 중에 C&C 서버와 통신 시 나타나는 특정 패턴이 있는지를 확인하여 악성코드에 감염되었는지 여부를 판단하게 된다. [그림 9]는 네트워크 레벨에서 트래픽이 들어올 경우 패킷을 재조립하고 파일을 분리하여 다양한 검사를 통해 악성코드 여부를 판별하고, 이미 감염된 단말을 식별하는 방식을 설명한 그림이다.

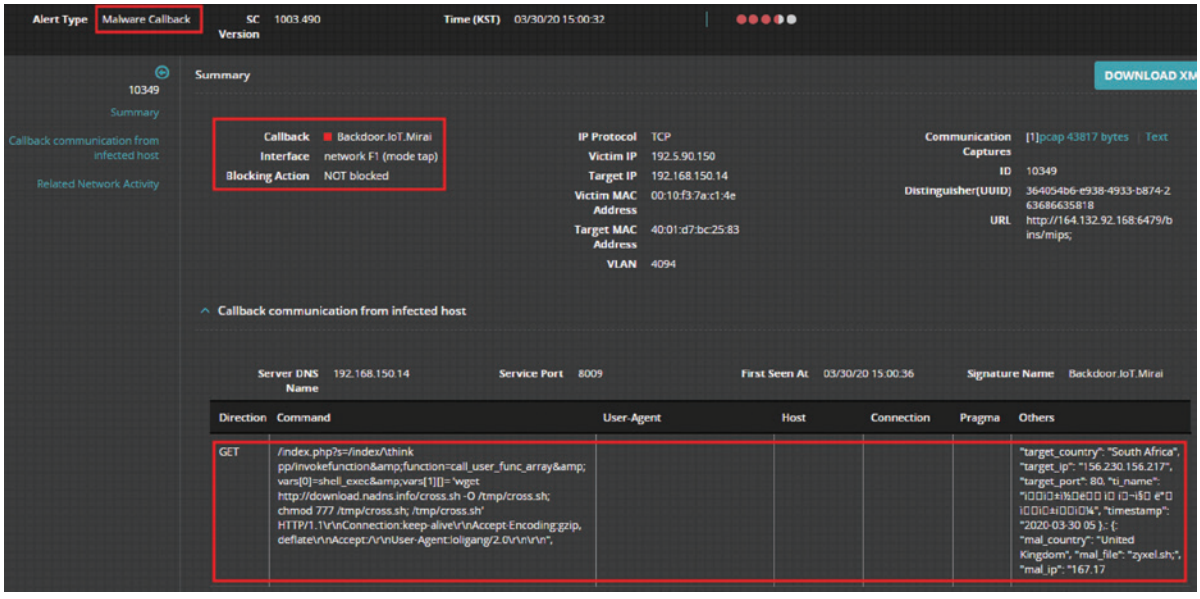


그림 10. 단말과 외부 C&C 서버가 통신탐지 내역 / 출처 : FireEye

[그림 10]은 실제로 악성코드에 감염되어 인터넷을 통해 C&C 서버와의 통신 내역이 탐지된 경보를 캡처한 그림이다. 미라이(Mirai)라는 악성코드에 감염된 단말(192.5.90.150)이 지정된 C&C 서버(192.168.150.14)와 통신되는 HTTP 방식의 통신내용을 네트워크 탐지 장비가 확인하여 해당 트래픽을 차단한 경보 내용이다.

IOC 종류	Custom IOC	IOC 설명	예상 탐지 범위 및 기대 효과
Process Event		E드라이브 부터 Z드라이브의 경로에서 파일이 실행 될 경우 탐지	• 이동식 디스크에 의해 유입되는 악성코드 탐지 가능 • 이동식 디스크에서 실행되는 Exploit 탐지 가능
File Write Event		E드라이브 부터 Z드라이브의 경로에서 파일이 생성될 경우 탐지	• 악성코드에 의해 이동식 디스크에 파일 생성시 탐지 • 내부인원에 의해 자료 유출을 위해 복사시 탐지
File Write Event & Process Event		hwp.exe(한컴오피스)에 의해 exe 파일이 생성될 경우 탐지	• 자주 사용되는 문서 형태의 exploit 실행 과정 탐지 • 스피어피싱을 통해 유입되는 악성문서 감염 과정 탐지 가능
Registry Key Event		Run 레지스트리에 키가 쓰여질 경우 탐지	• 악성코드가 자동실행을 위해서 등록하는 과정 탐지 가능
DNS Lookup Event		윈도우 정상 프로세스(svchost.exe, explorer.exe)에 의해 DNS query 발생시 탐지	• 윈도우 정상 프로세스로 위장한 악성코드 탐지 가능 • 윈도우 정상 프로세스가 변조되어 동작하는 행위 탐지 가능
IPv4 Network Event		특정 대역(192.168.0.x) 이외에 접속 시도시 탐지	• 사용하는 IP 대역 외의 대역에 접속 시도시 탐지

그림 11. IOC(공격침해지표)를 이용한 단말 PC에서의 APT 공격 탐지 / 출처 : FireEye

마지막으로 단말에서의 APT 탐지방식을 알아보자. 기존의 바이러스 백신의 경우 알려진 악성코드는 탐지가 가능하지만 알려지지 않은 악성코드는 탐지가 불가능하였다. 이런 단점을 보완하기 위해 단말에 악성 여부를 검사할 수 있는 기능을 추가하여, 알려지지 않은 악성코드도 탐지가 가능하게 되었다. 그뿐만 아니라 네트워크와 이메일에서 탐지된 악성코드의 다양한 정보(IOC : 공격침해지표)를 공유받아 다른 단말 기기에서 발생하는 공격행위를 탐지할 수도 있다. 아래 [그림 11]과 같이 단말 PC에 생성되는 파일, 레지스트리, 프로세스, 네트워크 행위 정보를 공유받아 별도의 정적, 동적 분석이 없더라도 공격 탐지가 가능한데, 이렇게 공격이 탐지된 이후에 생성된 파일을 삭제하거나, 변경된 레지스트리를 복구하거나, 악성코드의 프로세스를 중단시키고, C&C 서버와 통신하는 네트워크 트래픽을 차단하는 등의 방법을 통해 공격 차단이 가능하다.

기존에는 공격을 탐지하고 차단하는 것으로 대응이 끝났지만, APT 공격의 경우 침투한 단말을 통해 주위의 다른 단말과 서버에 악성코드를 확산시키는 특성을 가지기에 추가적인 대응이 필요하다. 그래서 아래 [그림 12]와 같이 확인된 공격행위의 전 과정을 별도로 수집할 수 있는 기능을 제공하여 어떻게 단말의 파일을 생성하고 레지스트리를 수정하고, 서비스를 등록했는지에 대한 내역을 시간대별로 정보를 저장할 수가 있으며, 이렇게 분석된 결과를 통해 다른 단말을 검사하여 동일한 침해지표를 있는지 검사를 수행할 수 있다. 기존에는 공격행위가 있어야 공격을 탐지할 수 있었다면 보안담당자의 탐지행위를 피하기 위해 악성코드만 설치되어 있고 공격행위를 하지 않고 잠복하고 있는 단말이 있는 경우에도 공격이 시작되기 전에 조사하여 악성코드가 설치된 단말을 탐지할 수 있는데 이러한 방식을 위협 사냥(Threat Hunting)이라고 부른다. 기존의 공격 방어가 수세적인 입장에서 공격이 이루어져야만 대응을 하는 개념이었다면, 이제는 공세적인 방식을 통해 공격을 일어나기 전이라도 사전에 대응하는 개념이 나오기 시작하였다.

그림 12. 침해지표(IOC)를 통한 단말의 침해 여부 조사 (Threat Hunting)

지금까지 설명한 APT 공격에 대한 대응을 위해 사내보안팀이 파악해야 하는 사항에 대해 [그림 13]과 같이 정리하였다. 최초 공격자가 이메일을 통해 악성코드를 사내 엔드포인트(단말)에 설치를 성공시키면, 내부 전파를 통해 여러 단말을 감염시켜 단말을 모니터링하면서 계정정보와 사내 서버 접속정보를 수집한다. 이후 AD(계정관리서버 : Active Directory) 서버의 계정을 탈취하여 사내 중요 데이터에 대한 접근에 성공하여 데이터를 외부 서버로 유출하거나 파괴하는 행위를 통해 원하는 목적을 달성하게 된다. 이때 이러한 공격에 대응하는 보안팀의 입장에서는 공격이 어떤 경로를 통해 이루어졌는지, 감염된 호스트는 무엇이며 감염 규모는 얼마인지, 사내 중요 데이터에 접근이 이루어졌는지, 데이터에 대한 유출이 이루어졌는지에 대한 사실을 파악하여야 공격에 대한 대응이 가능하다.
모든 공격이 단말을 통해 시작되고, 대부분의 공격 기간 단말을 중심으로 공격이 수행되기 때문에 단말을 모니터링하

고 대응을 하는 것이 무엇보다 중요하게 되었다. 아쉽게도 대부분의 조직에서는 바이러스 백신 정도의 방어수단만 존재하는 상황에서 이러한 APT 공격에 대한 방어가 여러모로 힘든 점이 존재하지만, 지속적인 방어수단에 대한 투자와 보안담당자의 교육을 통해 대응이 필요하다.

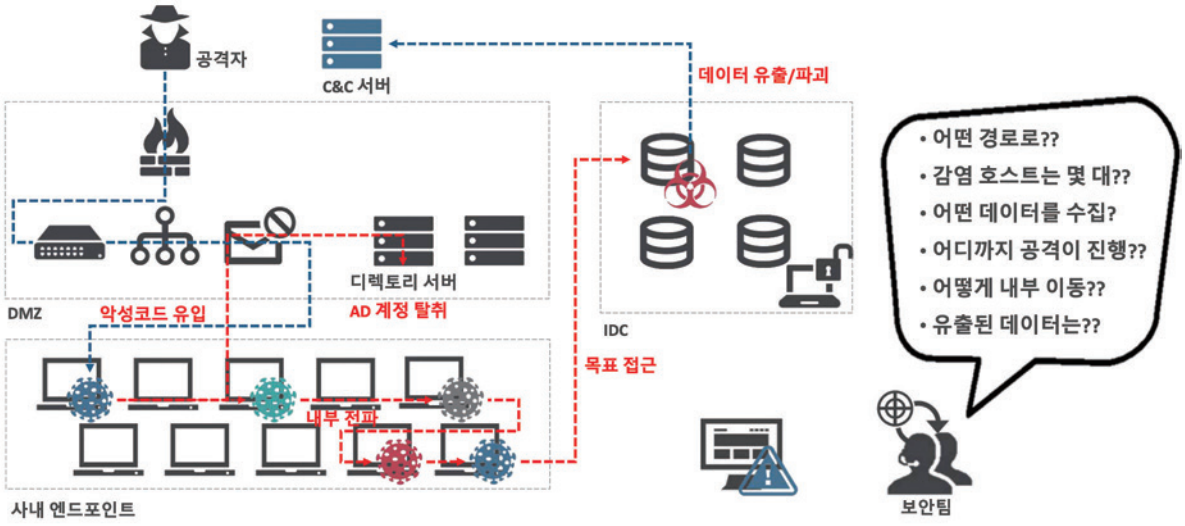


그림 13. APT 공격 시나리오와 보안팀 확인사항

이상으로 11회 걸친 네트워크 보안 이야기를 마무리하려고 한다. 방화벽을 시작으로 VPN, DDoS, APT 공격에 대해 나름대로 풀어서 설명을 한다고 했는데, 독자에게 네트워크 보안에 대해 조금이라도 이해가 되었으면 한다.
끝까지 읽어 주신 독자분들에게 고마움을 표하며, 기회가 된다면 새로운 정보보안 트렌드에 대해 소개하는 시간이 있기를 기대하며 글을 마치도록 하겠다.