EQST insight

지능형 이메일 해킹 공격 시나리오 및 대응 방안

개요

오늘날 기업 보안 강화로 악성코드가 내부로 쉽게 침입하기 어려워지면서 이메일이 대표적인 사이버 공격 경로가 되었다. 한국인터넷진흥원(KISA)에 따르면, 2020년 국내에서 발생한 사이버 공격의 약 91%가 이메일을 통해 이루어지고 있으며, 당사 침해 사고 대응 조사 결과에서도 85%가 이메일이 사이버 공격의 주요 대상으로 지목했다. 이메일은 손쉽게 사용자에게 접근할 수 있어 해킹 공격의 주요 수단으로 활용되고 있으며, 특히 이메일에 첨부된 문서파일의 경우 악성코드가 삽입되어 알아채기 어렵기 때문에 사용자들이 이를 구분하기는 불가능에 가깝다.

지난달에는 일반적인 “이메일을 이용한 공격 사례”에 대해서 살펴보았다.

※ 참고 : [EQST insight] 이메일을 이용한 지능형 APT 공격 사례 및 대응 방안

본 포스팅에서는 최근 이메일 보안 사고 발생률이 높은 공격 방식에 대해 알아보고, 그에 따른 대응 방안과 함께 이메일 사고에 대한 경각심을 일깨우고자 한다.

공격 목적

이메일을 통한 사이버 공격의 주된 목적은 금전 취득이다. 그 대표적인 수단으로 랜섬웨어 공격이 있으며, 정보 탈취(개인 정보, 산업기밀정보 등) 및 신용 사기(SCAM) 외 다양한 공격을 시도하고 있다. 이로 인해 기업에 금전적인 손실과 이미지 실추 등의 피해가 발생되고 있다. 최근 해커 집단 랩서스에 의한 삼성전자, LG전자의 해킹 사고도 이메일이 원인인 것으로 밝혀졌다.

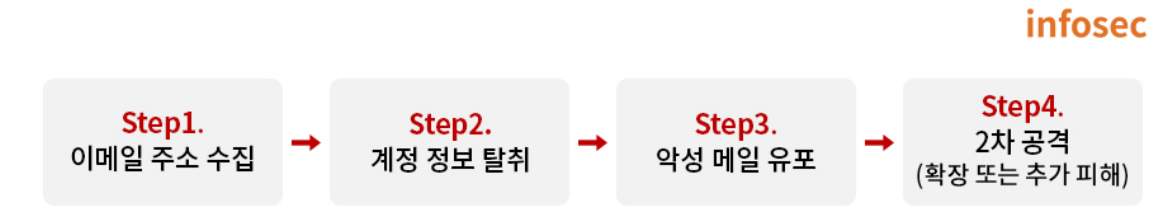
IDC의 보안이 강화되면서 악성코드가 내부로 침투하기 어려워지고 있는 반면, 이메일에 대한 보안은 상대적으로 취약한 경우가 많다. 악성코드 변종과 같이 지속적으로 탐지를 우회하는 악성 메일의 시도가 발생되고 있다.

공격자는 최초에 공격 대상에 대한 정보가 필요하며, 취약점 및 보안 Hole 등을 스캔하기보다는 수집이 용이한 이메일 주소를 수집하여 불특정 다수의 이메일 주소를 대상으로 피싱/악성메일을 발송하고 계정 및 시스템 정보를 탈취를 시도한다. 탈취한 정보에 따라서 개인 또는 특정 기업이 공격 대상이 되기도 하며, 2차 공격을 통해 공격 대상을 확장하거나 특정 대상에 더 큰 피해를 발생시키기도 한다.

해당 공격 방식은 최근 모든 기업을 대상으로 공격을 시도하고 있다고 해도 과언이 아니다.

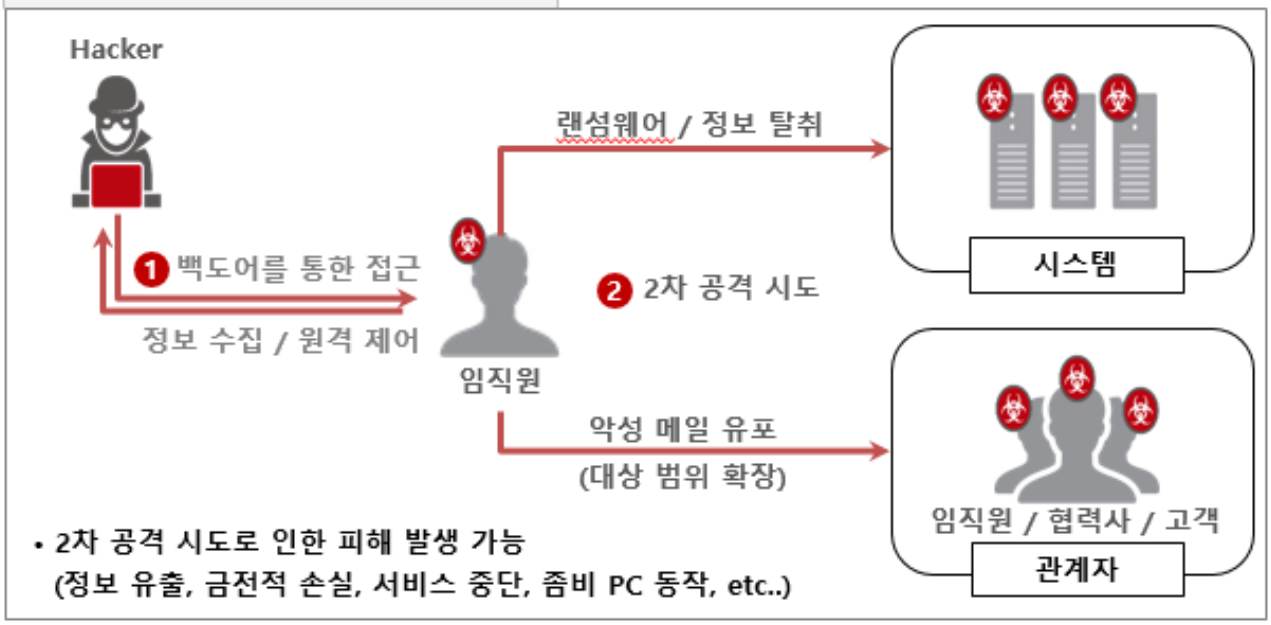
공격 흐름

위에서 설명한 공격 방식에 대한 실제 사례를 기반으로 한 시나리오는 다음과 같다.

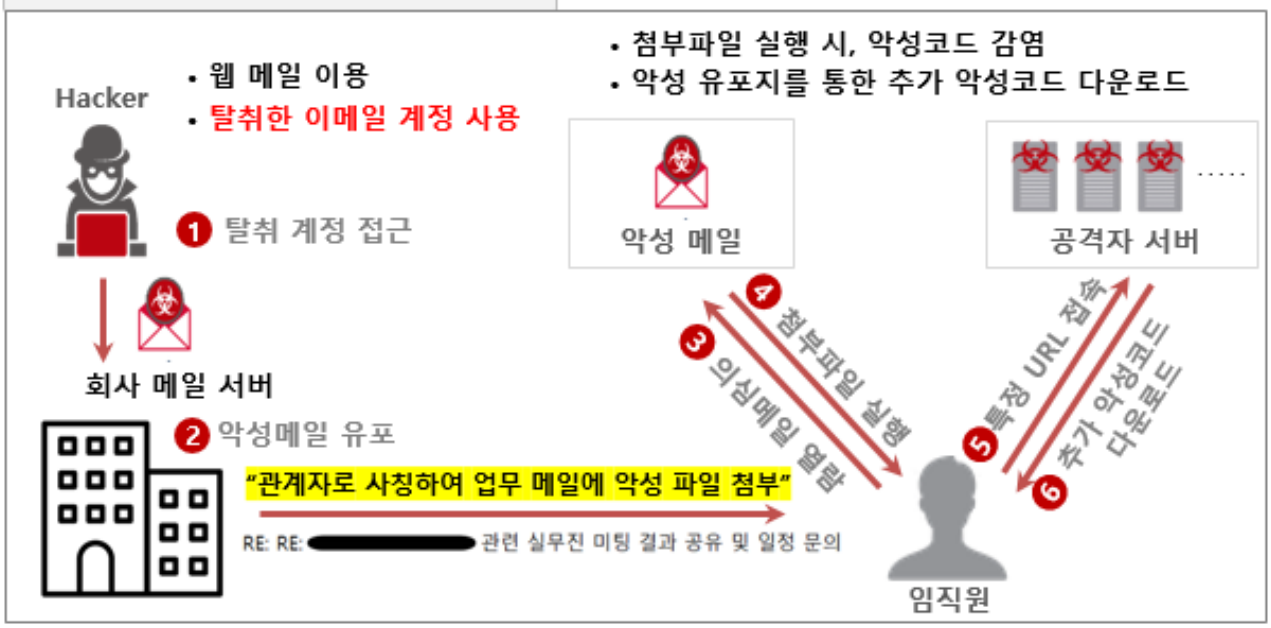


[공격 시나리오 구성]

3 2차 공격 시도



2 악성 메일 유포



공격 방식 (단계별 상세 공격 내용)

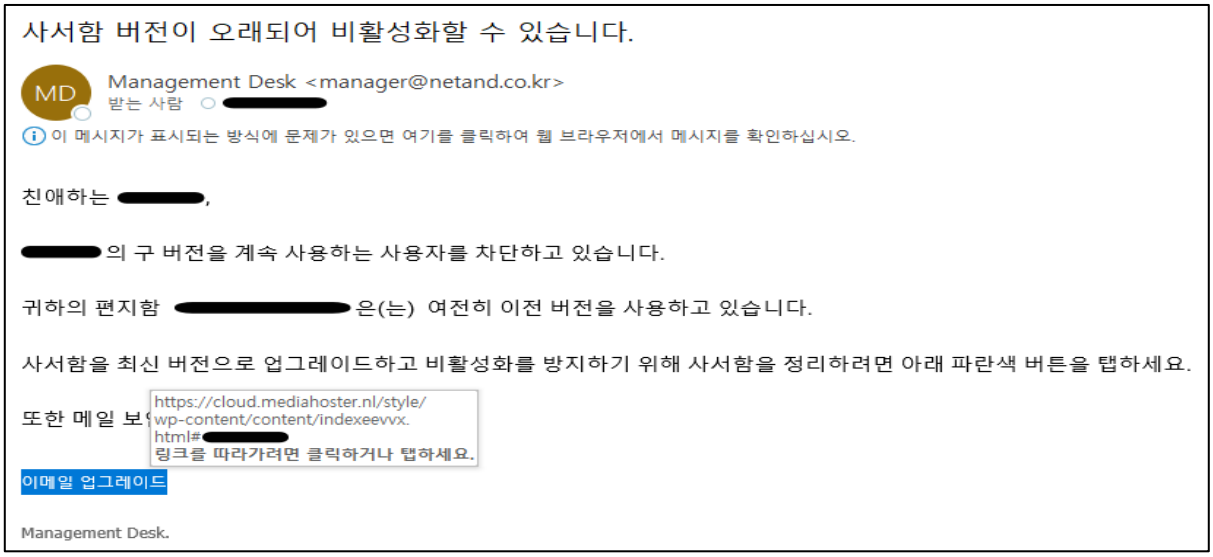
Step1. 이메일 주소 수집

기업 임직원의 이메일 주소를 인터넷 검색(구글, 바이러스토탈 등)과 다크웹 등을 통해 손쉽게 수집할 수 있으며, 피싱/악성 메일을 발송한다. 일반적으로 이메일 열람만으로 자동 실행되는 악성 행위는 없으며, 링크 클릭 및 첨부파일 실행을 유도한다.

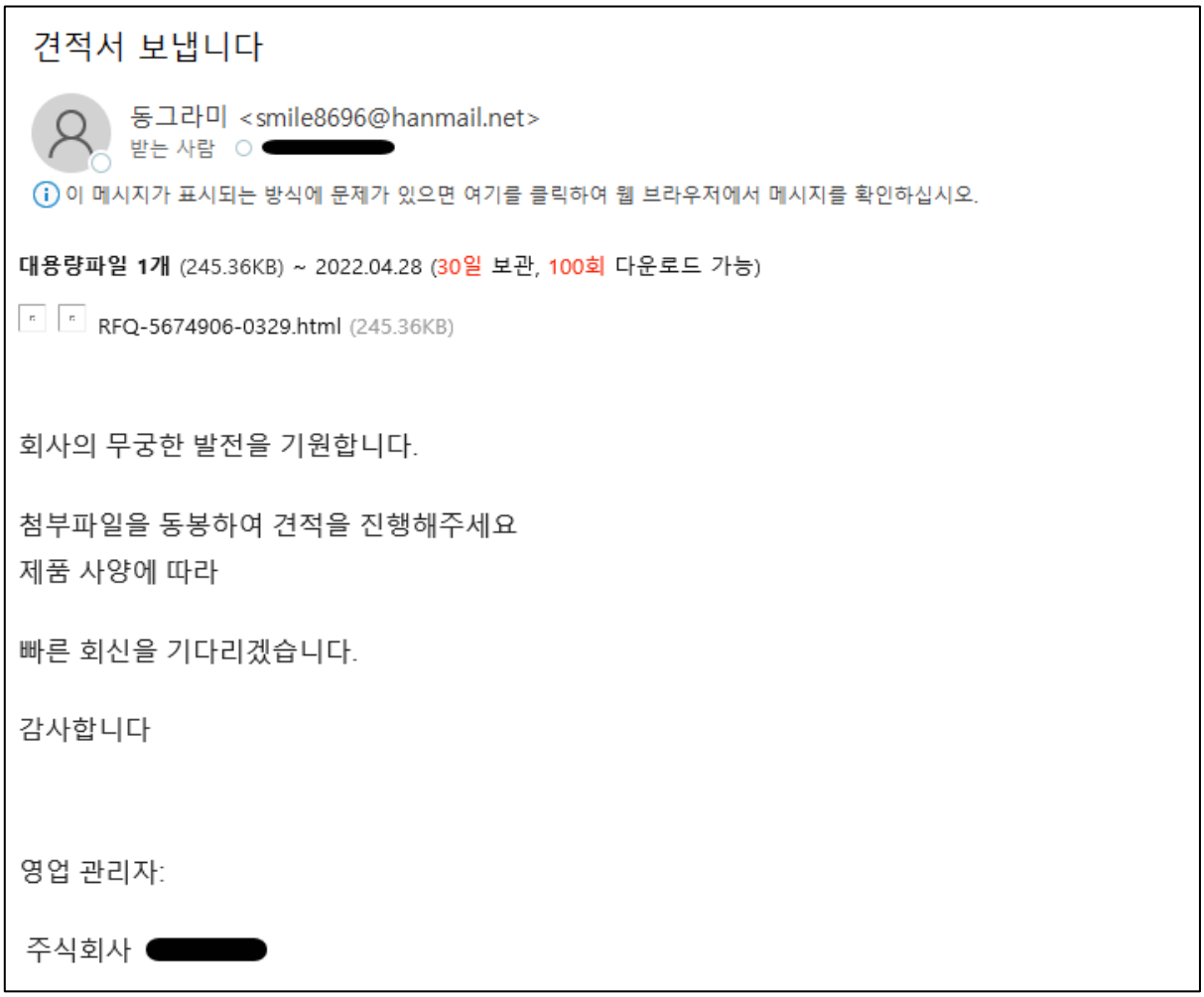
Step2. 계정 정보 탈취

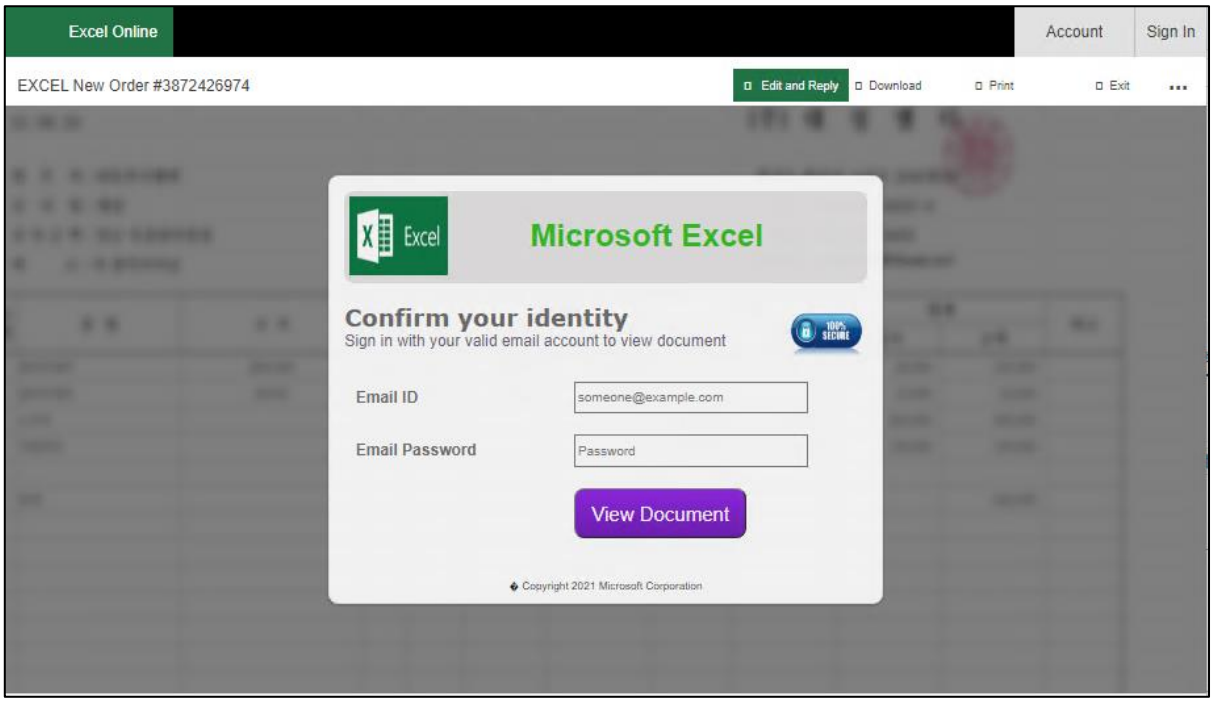
계정 정보 탈취를 위한 피싱 메일은 메일 본문 내 URL 링크를 포함하거나, HTML 파일을 첨부하는 형태로 나눌 수 있다.

Case 1. 메일 본문 내 링크(URL)가 피싱 페이지인 경우



Case2. HTML 파일이 피싱 페이지인 경우 (직접 첨부 또는 대용량 링크)





악성 첨부파일 메일은 압축을 하거나, 파일명에 공백을 길게 하여 실제 확장자를 인지하지 못하게 하는 경우가 있다. 이외에 오피스 문서에 악성 매크로를 사용하거나, 취약점을 악용하는 등의 다양한 형태로도 계정 정보 탈취가 가능하다.

메일 내 첨부파일이 정보 탈취 악성코드인 경우, 아래와 같은 단계를 거쳐 계정 정보 탈취 동작(브라우저, 키로거 등)을 수행한다.

Step. 1) 브라우저 계정 정보 검색

```
0040C236 PUSH    00414D08                UNICODE "₩Google₩Chrome₩User Data₩Local State"
0040C23B PUSH    00414D58                UNICODE "₩Google₩Chrome₩User Data₩Default₩Login Data"

0040C26C PUSH    00414E70                UNICODE "₩Microsoft₩Edge₩User Data₩Local State"
0040C271 PUSH    00414EC0                UNICODE "₩Microsoft₩Edge₩User Data₩Default₩Login Data"

00407F25   68 14544100   PUSH    00415414                ASCII "password_value"
00407F2A   68 24544100   PUSH    00415424                ASCII "username_value"
```

Step. 2) 키로거를 통한 계정 정보 수집

```
0040904A   BF 78E945   MOV     EDI, 0045E978           ASCII "Online Keylogger Started"
```

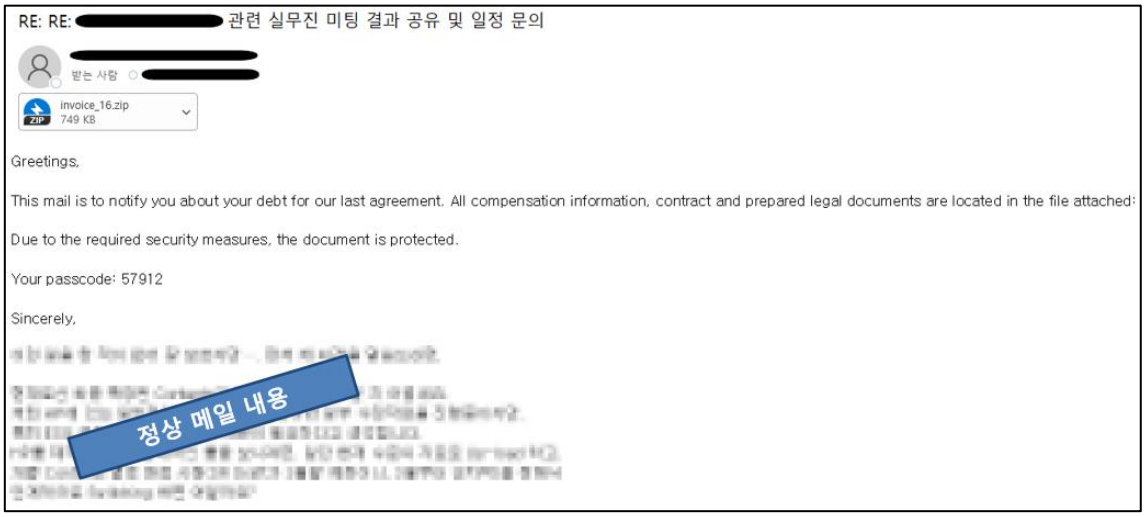
Step. 3) 공격자에게 전송

Proc...	PID	Protocol	Local Address	Local Port	Remote Add...	Remote Port	State
RegSvcs.exe	3796	TCP	192.168.28.137	49217	103.6.198.106	587	ESTABLISHED

Step3. 악성 메일 유포

위의 피싱/악성 메일을 통해서 탈취한 메일 계정으로 수·발신된 업무 메일들을 획득하여, 업무 메일 발신자/제목 등을 사칭하고, 메일 본문에 내용/첨부파일을 추가시킨 악성 메일을 수·발신된 다른 메일 주소들로 유포한다. 이를 통해서 사내 임직원 및 관계자의 계정을 추가로 획득하는 시도를 한다.

※ 업무 메일로 사칭 및 악성 파일을 첨부하여 악성 메일 유포



대부분의 악성코드가 기본적으로 시스템 정보를 스캔하는 기능이 있으며, 특히 Emotet 경우에는 추가로 악성코드를 다운로드하는 기능을 포함하여, 다운로드되는 악성코드에 따라서 추가 피해가 달라진다.

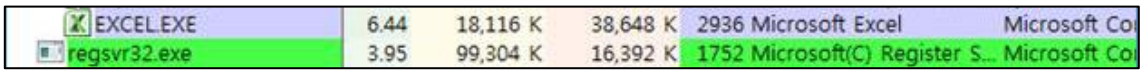
이전의 Emotet은 금융 정보 탈취형 악성코드를 다운로드하였으나, 최근에는 정보 탈취 및 추가 공격에 중점을 둔 것으로 보인다.

※ 계정 및 정보 탈취 악성코드는 아래와 같다. (최근 3월 간 조사 결과)

- 계정 및 정보 탈취 유형의 AgentTesla , Lokibot , Formbook 등 지속 유입
- 다운로더 유형의 Emotet 악성코드 유입이 급증 (Squirrelwaffle 악성코드와도 유사)

Step. 1) Emotet 악성코드 실행 시에 매크로를 통해 추가 악성코드 다운로드 및 실행

```
12  <si><t>"..\rfs.dll</t></si>
13  <si><t>regsvr32.exe</t></si>
14  <si><t>"http://henrysfreshroast.com/6cc4ts0bkrOlXq/",</t></si>
15  <si><t>"http://consejosdeorlando.com/wp-includes/jxTbRk2DgQOIOyokR/",</t></si>
16  <si><t>"http://blog.centerking.top/wp-includes/DBq5jx/",</t></si>
17  <si><t>"http://polarrefrigeracao.com.br/fontes/y7Qp0/",</t></si>
18  <si><t>"http://filmsetserie.dx.am/img/ghCY9J5KD1J/",</t></si>
19  <si><t>"https://vagbharati.in/wp-admin/nYBb/",</t></si>
20  <si><t>"http://advogadogoiania.com.br/wp-includes/O9Az4/",</t></si>
```



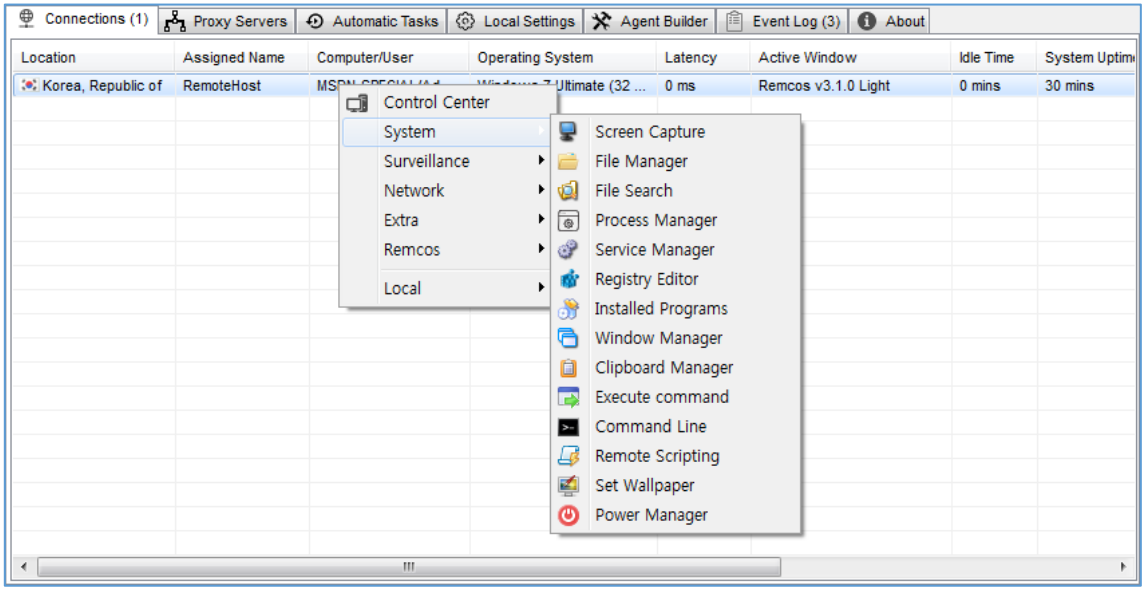
Step. 2) 공격자에게 전송

Proc...	PID	Protocol	Local Address	Local Port	Remote Add...	Remote Port	State
regsvr32.exe	1752	TCP	192.168.28.136	49176	165.22.61.235	443	SYN_SENT

Step4. 2차 공격(확장 또는 추가 피해)

사내 시스템 관리자 권한의 계정을 탈취한 경우 정보 탈취(개인 정보, 산업기밀정보 등) 및 랜섬웨어 배포 등을 통해서 기업에 추가적인 피해를 발생시키며, 관계자(협력사)에 유포된 메일은 업무에 혼선을 야기시키는 등 기업 이미지를 실추시키는 추가 피해도 발생한다. 이메일을 통하여 악성코드가 유입되면 공격자는 다양한 가능성을 갖고 공격하기 때문에 사실상 공격을 막기는 쉽지 않다

※ RAT 악성코드는 원격 명령 수행, 키로깅, 화면캡쳐, 웹브라우저 계정 정보 탈취 등 가능



대응 방안

악성 메일을 유포하는 수법이 날로 진화하면서 구글, M365 등 이메일 서비스 기업들도 이메일 작성 시 자바스크립트 파일을 첨부하지 못하도록 조치를 취하는 등 다양한 방안을 도입하고 있다. 그러나 악성코드나 랜섬웨어의 확산을 막기에는 역부족한 것이 사실이다.

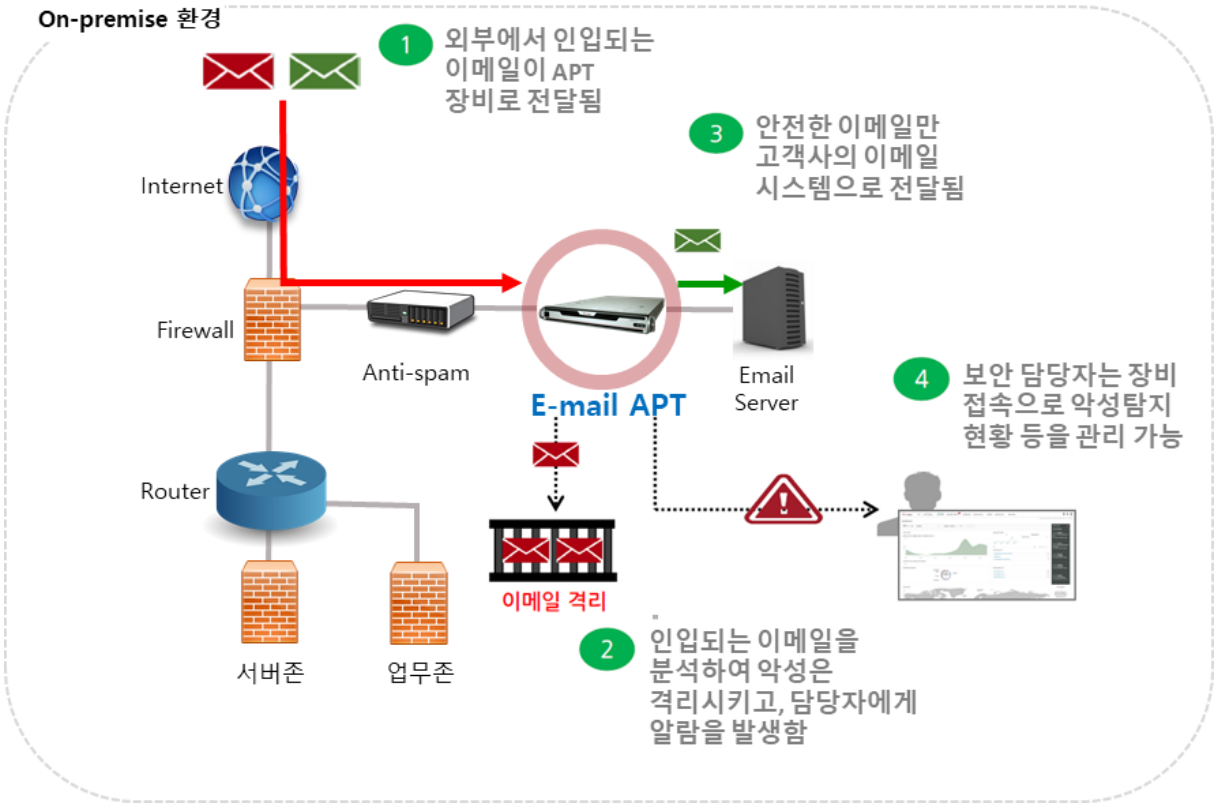
기업이 랜섬웨어를 비롯하여 개인 정보 탈취 목적으로 유포되는 악성 메일을 차단하고 피해를 예방하기 위한 방법을 인터넷에 검색해 보면 사용자의 주의를 요하는 방법론이 대부분이다. 악성 메일을 사용자가 클릭을 할 수밖에 없게끔 신뢰하는 사용자로 위장하여 악성 메일을 보낼 경우 사용자가 주의해서 구별하기가 결코 쉽지 않다.

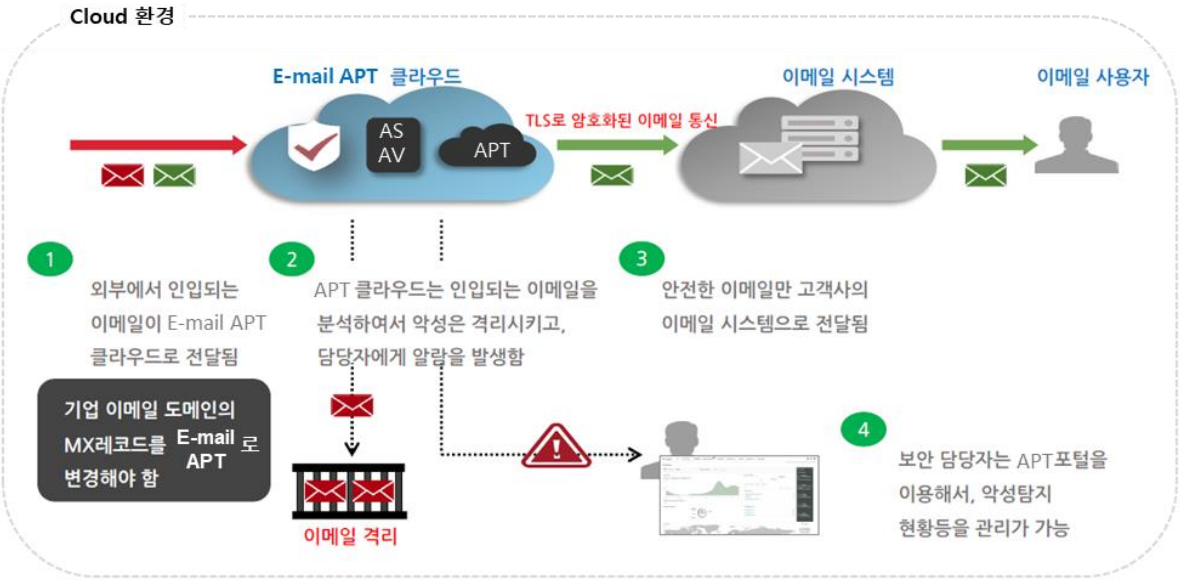
이메일 사용자가 보안 수칙을 준수하며 아래와 같은 보안 솔루션을 도입하여 복합적으로 탐지 및 차단하는 대응 방안을 구축하는 것이 최선책일 것으로 보인다.

- 스팸 차단
- 이메일 APT
- 네트워크 APT
- EDR/EPP
- DRM/DLP
- 접근제어 및 계정관리
- 2-Factor 인증 (모바일, 생체인증)
- 비인가 IP 추적 및 이력 관리 솔루션
- 분기별 악성메일 모의 훈련

하지만, 솔루션 도입 비용, 운영 방안, 전문 인력 등 기업의 상황을 고려하지 않을 수 없다. 현업에서 이메일 보안 사고 사례들과 다양한 솔루션들의 특장점들을 비교 분석했을 때 이메일 APT 솔루션만이라도 도입한다면 비용 대비 가장 효과적으로 대다수의 APT 공격을 탐지하고 차단할 수 있다. 그리고 중소기업을 포함 많은 기업들이 스팸차단 솔루션을 도입하여 운영하고 있으나 APT 공격은 스팸차단 솔루션에서 탐지하고 차단할 수 없다는 것을 인식해야 할 것이다.

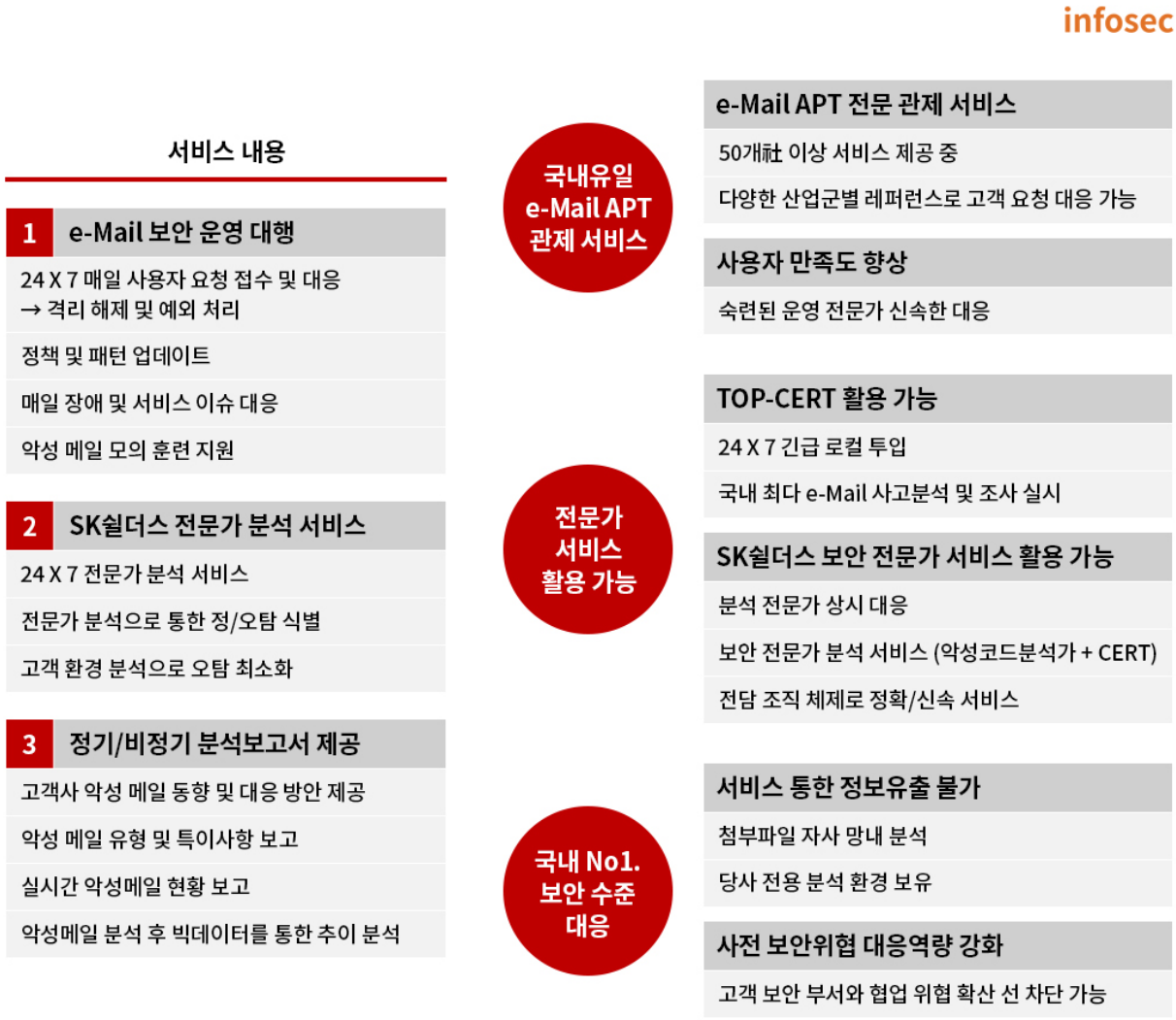
이메일 APT 솔루션은 아래와 같이 On-premise, Cloud 환경에 맞게 구성 가능하며, 실시간으로 정책이 업데이트되어 메일에 포함된 악성파일 및 URL을 차단 및 탐지할 수 있다.





SK쉴더스에서는 이메일 APT 솔루션의 운영 고도화 및 운영이 어려운 고객을 대상으로 아래와 같이 국내 유일 이메일 APT 관제 서비스도 제공해 주고 있다.

[e-mail APT 관제 서비스]



이메일을 통하여 악성코드가 유입되면 공격자는 다양한 가능성을 갖고 공격하기 때문에 사실상 이를 완벽하게 막기는 쉽지 않다. 이메일 APT 솔루션을 통하여 최대한 원천 공격을 차단하고 임직원에게 이메일, 문서 등을 이용한 공격에 주의할 것을 강조해야 한다. 또한, 주기적인 모의 훈련을 통해 보안 의식을 강화한다면 비용 대비 가장 효과적인 이메일 보안 방안을 구성할 수 있을 것이다.