ESET Endpoint Solution 을 통한 RANSOMWARE 예방 가이드

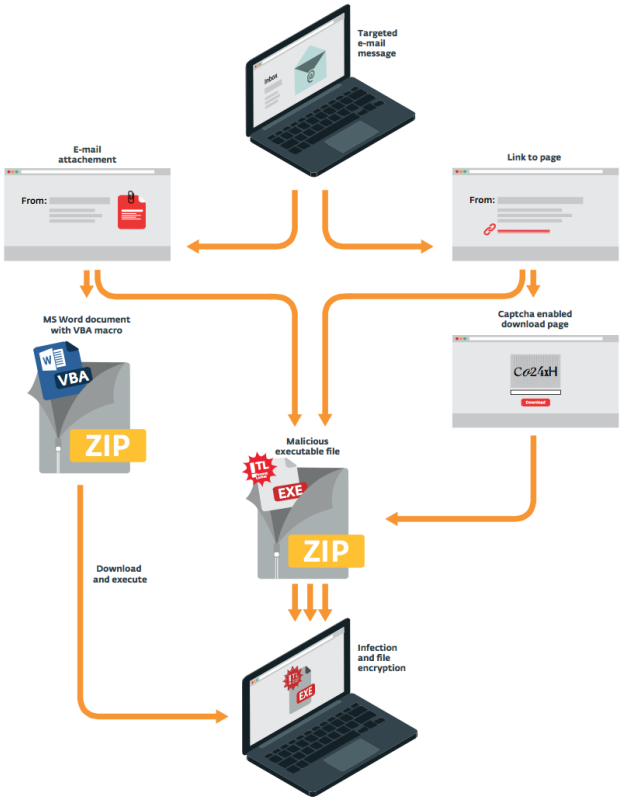
㈜이셋코리아

1. 랜섬웨어란 무엇인가?

랜섬웨어는 사용자의 정상적인 PC 사용을 방해 또는 중단하는 것으로 PC 를 잠그거나 파일을 암호화한 후 몸값(ransome)을(돈 또는 설문) 요구합니다.

1) 랜섬웨어 감염 증상
   - 윈도우 접근을 방해하거나 파일을 사용할 수 없도록 암호화
   - 특정 애플리케이션의 실행을 중지 (웹 브라우저 등)

2) 랜섬웨어 감염 경로
   - Exploit 을 포함한 웹 페이지
   - Fake 사이트
   - 신뢰를 주기 위해 captcha 사용
   - 이메일
   - VBA 매크로가 포함된 오피스 문서 첨부



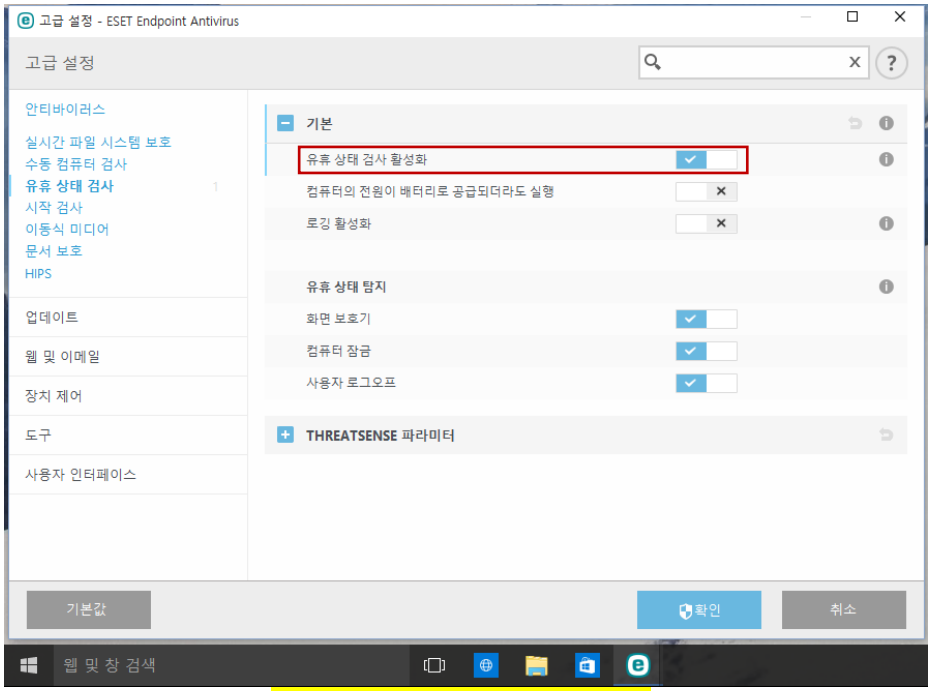
3) 암호화된 파일의 복구 가능성은?
   - 랜섬웨어가 주로 사용하는 암호화 알고리즘
     - AES-256: 안전한 대칭키 암호화 알고리즘, 파일 암호화에 사용
     - RSA-2048: 안전한 공개키 암호화 알고리즘, 대칭키 암호화에 사용
   - 암호를 풀기 위해서는 2048 비트 키를 모두 대입해야 함
     - 2^{2048} 가지 경우의 수가 발생하며 현재의 컴퓨팅 능력으로 수십 년의 시간이 필요
       => 현실적으로 불가능
   - 몸값을 지불하면 복호화가 가능한가?
     - 50% 정도가 암호 해독이 가능한 프로그램 전달 받음
     - 몸값을 지불한다 해도 암호 해독을 보장받을 수 없음
   - 랜섬웨어에 의해 암호화된 파일의 복구가 가능하니 비용을 지불하라는 업체의 말에 현혹되지 말 것
     -> **암호 키를 찾아내어 복구하는 것은 불가능!!!**

2. 랜섬웨어 예방

1) **ESET Endpoint Solution 으로 랜섬웨어를 예방할 수 있습니다.**

- 유휴 상태일 때 수동 검사 설정

  : ESET Endpoint Solution 은 자동으로 PC 의 유휴상태를 감지하여 PC 의 바이러스 검사를 진행합니다. 화면 보호기 작동, 컴퓨터 잠금, 사용자 로그오프 상태를 감지하여 PC 자원을 효율적으로 활용합니다.



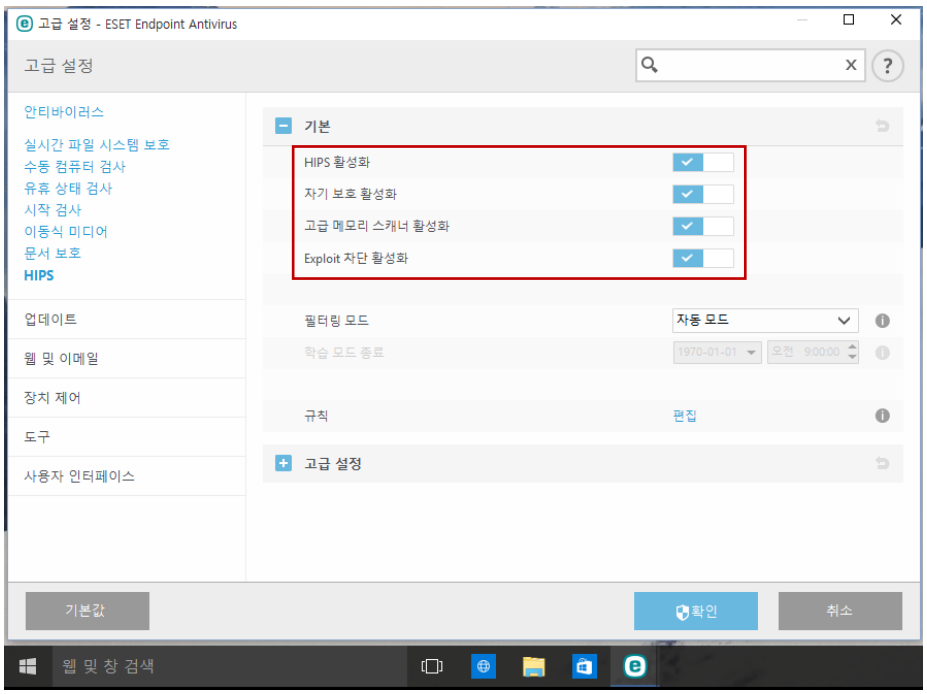
[Windows10 설치 운영 화면]

- HIPS, 고급 메모리 스캐너, Exploit 차단 활성화

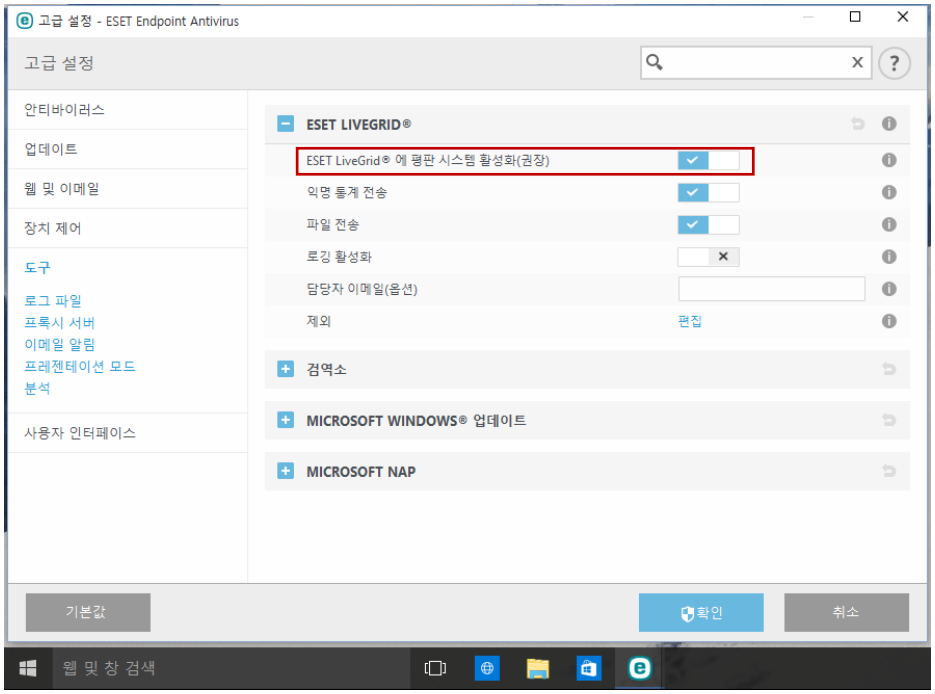
  HIPS: 호스트 기반 침입방어 시스템으로, 행위 기반의 휴리스틱 기술을 이용하여 알려지지 않은 악성코드를 차단

  고급 메모리 스캐너: Exploit Blocker 와 함께 프로세스 동작을 감시하며 난독화된 악성코드 대응

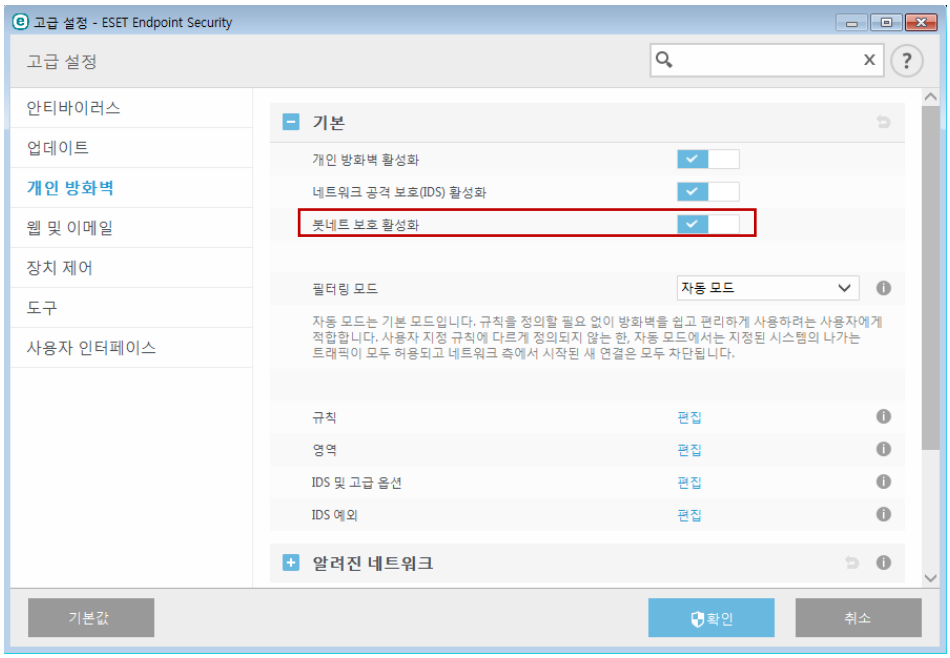
  Exploit 차단: 웹브라우저, 이메일, MS 오피스 등의 취약점을 이용한 익스플로잇 공격 대응하며, 프로세스 동작을 분석하여 익스플로잇 공격으로 의심되는 활동을 감지하고 차단



- ESET LiveGrid® 평판 시스템 활성화
  : ESET Endpoint Solution 은 여러 클라우드 기반 기술로 구성된 고급 조기 경보 시스템으로, 최근 발생한 위협을 감지하고 허용 목록을 통해 검사 성능을 향상시킵니다.
  새 위협 정보는 클라우드에 실시간으로 스트리밍되기 때문에 ESET 맬웨어 연구소에서 적절한 조치와 일관된 보호를 항상 제공할 수 있습니다.

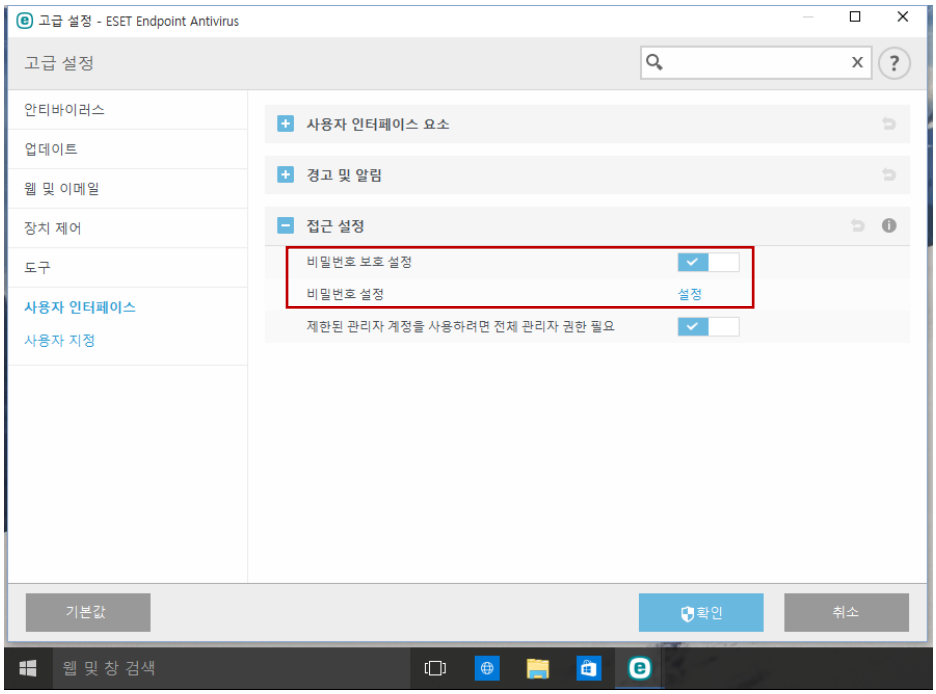


- 봇네트 보호 (상위버전 제품 기능)
  : Command & Control 서버 등을 향한 악의적인 네트워크 통신을 차단합니다.



- 비밀번호 설정

  : ESET Endpoint Solution 을 통해 시스템의 보안을 극대화하려면 ESET Endpoint Antivirus 를 올바르게 구성해야 합니다. 구성을 잘못 변경하면 중요한 데이터가 손실될 수 있습니다. 무단 수정을 방지하기 위해 ESET Endpoint Antivirus 의 설정 파라미터를 비밀번호로 보호할 수 있습니다.



2) ESET 의 랜섬웨어 경고

ESET 은 2013 년도부터 수차례 변종 랜섬웨어 확산에 대하여 경고 및 대응하였습니다.

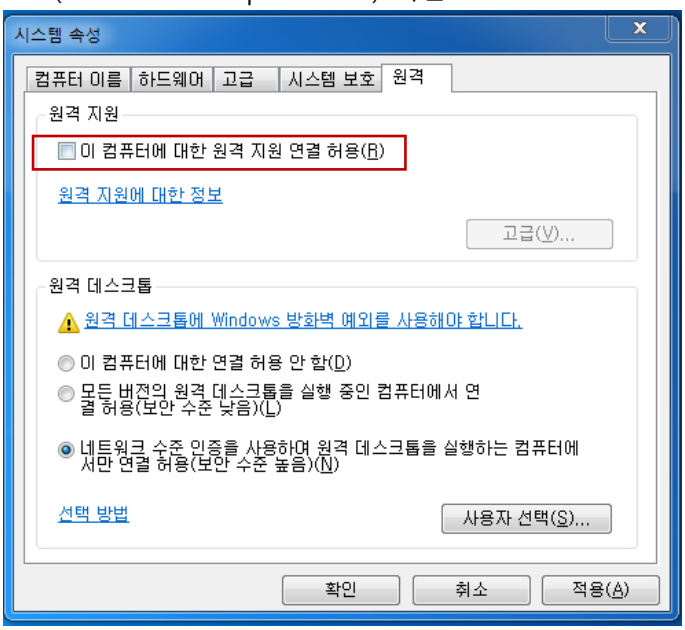
날짜	매체	제목	기사 링크
2013-12-23	보안뉴스	ESET 2014 년 위협 동향 리포트 발표	원문보기
2013-12-24	아이티데일리	2014 년 보안 트렌드, "개인정보보호, 안드로이드, 랜섬웨어"	원문보기
2014-07-24	데이터넷	이셋, 랜섬웨어 변종 확산 경고	원문보기
2014-12-19	데일리시큐	악명 높은 TorrentLocker 랜섬웨어 피해 주의	원문보기
2015-01-27	데이터넷	노드 32 "표적공격.결제시스템 공격 주의" 당부	원문보기
2015-01-29	CCTV 뉴스	새로운 범주 디지털 기기 2015 년도 사이버범죄 원흉	원문보기
2016-03-23	데이터넷	[긴급진단: 랜섬웨어①] '록키' 랜섬웨어 비상	원문보기
2016-06-15	CCTV 뉴스	이셋코리아, 크라이시스·변종 램섬웨어 확산 '경고'	원문보기

3) 랜섬웨어 피해 예방을 위한 개인행동 수칙: **각 사용자의 보안 인식이 중요**

- 출처가 불분명한 메일, 웹 사이트를 열지 않는다.
- 윈도우를 최신 버전으로 업데이트한다. (윈도우 XP 사용 지양)
- 안티바이러스를 최신 버전으로 업데이트하고 사전방역 기능을 활성화한다.
- 중요한 파일이나 문서는 주기적으로 백업해 놓는다.

  => 랜섬웨어를 진단하고 치료한다는 것이 암호화된 파일을 복구한다는 의미는 아니랍니다!!!

4) RDP(Remote Desktop Protocol) 차단



3. 결론

랜섬웨어도 악성코드가 감염되는 경로와 같은 방법으로 사용자 PC 를 감염시켜 결과적으로 암호화 해서 금전을 요구하는 형태의 변종입니다.

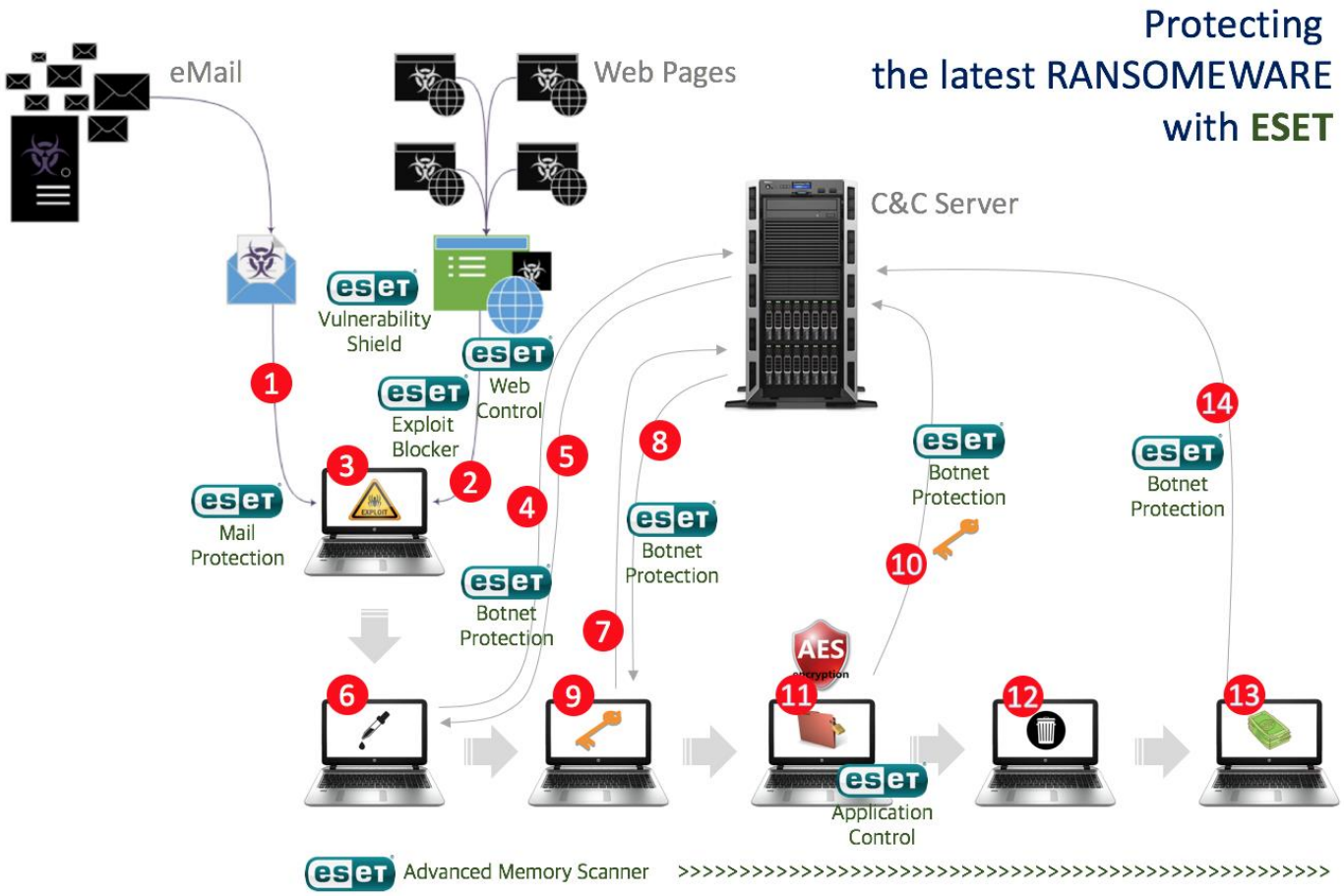
신종 및 변종 악성코드(랜섬웨어도 악성코드 중 하나)에 대한 대응 방법은 휴리스틱 기술에 근간한 사전방어 기능을 이용하는 것입니다. 각 백신업체가 사전방역 기능의 진단율을 높이고 오진율을 제로로 만들기 위해 노력을 하고 있지만, 아쉽게도 진단율 100%, 오진율 0%를 기록하는 제품은 없습니다. 이는 http://av-comparatives.org 의 사전방역 테스트 결과를 보시면 알 수 있습니다.

상식적으로도, 아직 존재하지 않는 모든 공격을 다 막을 수 있다고 공언하는 것 자체가 넌센스입니다. 모든 질병을 다 막을 수 있는 백신이 존재하지 않는 것과 같은 논리입니다. (독감예방 접종도 올해 유행할 것으로 예측되는 바이러스에 대한 저항력을 갖도록 하는 것)

결론적으로 랜섬웨어를 100% 방어할 수 있는 백신업체는 없습니다.

ESET Endpoint Solution 은 이미 HIPS(호스트기반 침입방지 시스템) 관련 기능들이 모두 활성화 되어 공급이 이루어지고 있으며, HIPS 기능이 활성화 되어 있음에도 업무에 지장 없이 가볍게 사용가능 합니다. ESET 의 HIPS 기능, 고급 메모리 스캐너, Exploit 차단, 봇네트 보호 활성화 설정으로 랜섬웨어를 적극적으로 대응하고 있습니다.

※ 랜섬웨어 유입 흐름에 따른 ESET 의 대응



① 이메일을 통한 익스플로잇 유입
② 웹페이지 방문을 통한 익스플로잇 유입
③ 익스플로잇 실행
④ 드로퍼/다운로더 감염
⑤ C&C 서버 접속
⑥ 랜섬웨어 다운로드 후 감염
⑦ C&C 서버로 IP 주소 등 감염 시스템 정보 전송
⑧ C&C 서버로부터 랜섬 페이지 다운로드
⑨ AES 암호화키 생성
⑩ AES 암호화키를 RSA 공개키로 암호화하여 C&C 서버로 전송
⑪ AES 암호화키로 문서 암호화
⑫ AES 암호화키 삭제
⑬ 랜섬 페이지 표시
⑭ 암호화된 문서 갯수를 C&C 서버로 전송