기업의 백신 잠금 정책 미사용으로 인한 Lockis 랜섬웨어 감염 사례

asec.ahnlab.com/ko/30284/

2021년 12월 28일

지난 11월경 안랩의 한 고객사에서 다수의 서버가 Lockis 랜섬웨어에 감염된 사고가 발생했다. 피해 업체는 V3 백신을 사용하고 있었음에도 불구하고 랜섬웨어에 감염되어 감염 원인을 파악하기 위해 안랩 A-FIRST가 투입돼 포렌식 분석을 수행했다.

Lockis 랜섬웨어는 “ASEC 블로그 : Lockis 랜섬웨어와 함께 사용된 해킹 툴” 포스팅에서 언급한 바와 같이 GlobImposter 랜섬웨어의 변종으로, 9월 16일에 최초 발견됐다.

안랩에서는 2018년 5월경부터 GlobImposter 류의 랜섬웨어를 진단명 Trojan/Win32.FileCoder로 진단하고 있었고, 9월 16일 등장한 Lockis 랜섬웨어도 진단이 가능한 상황이었다.

피해 시스템에서 확인된 공격자의 공격 순서는 다음과 같다.

- 1. RDP 연결 (로컬 Administrator 계정)
- 2. 백신 언인스톨
  V3 Uninstall

- 3. 해킹 툴 및 랜섬웨어 복사
  - ProcessHacker.exee
  - Netscan.Chs.exe
  - dControl.exe
  - lockisdog.exe
- 4. 해킹 툴 및 랜섬웨어 실행
  - dControl.exe 실행
  - Netscan.Chs.exe 실행
  - ProcessHacker.exe 실행
  - lockisdog.exe 실행 (랜섬웨어)

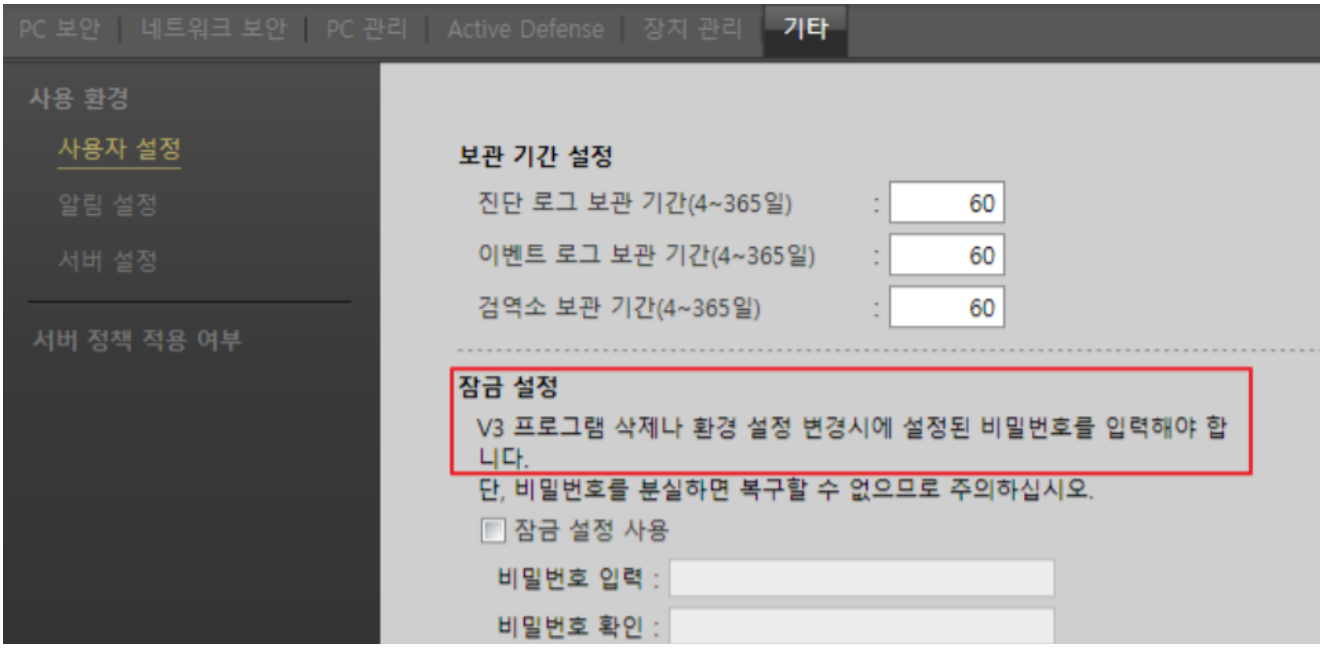
공격자는 랜섬웨어가 OS의 보안 기능이나, 보안 제품에 탐지돼 차단되는 것을 우회하기 위해 랜섬웨어를 실행하기 전 V3 백신을 언인스톨 하고, Windows Defender를 비활성화 했으며, 방해되는 프로세스를 종료시키기 위해 ProcessHacker를 사용했다.

즉, 랜섬웨어가 안전(?)하게 실행될 수 있도록 철저히 준비 후 랜섬웨어를 실행시킨 것이다.

이러한 방식의 공격이 가능한 이유는 우선 Administrator 계정으로 RDP 접속해 관리자 권한으로 시스템을 GUI 제어할 수 있었던 것이 1차적인 원인이며, 보안 제품의 임의 삭제가 가능한 것이 2차적인 원인일 것이다. 관리자 권한을 가진 사용자는 시스템에서 거의 모든일을 수행할 수 있는 관리자이므로 당연히 백신을 언인스톨 하는 것이 가능하다.

따라서, 기업 환경에서는 이와 같이 IT 인프라 부서에서 설치 혹은 설정한 보안 기능들이 무력화되지 않도록 보안 제품의 언인스톨 혹은 설정 등을 사용자가 임의로 변경하지 못하도록 해야 한다.

안랩 APC는 V3 제품의 삭제나 설정 변경 등을 제한하기 위해 '잠금 설정' 기능을 제공하고 있으나, 아쉽게도 해당 업체에는 잠금 정책을 사용하고 있지 않았다.



[그림] 안랩 APC의 잠금 설정 적용 화면

결론

- 백신을 사용 중임에도 백신의 보호를 받지 못한 이유는 백신의 '잠금 설정' 정책이 적용돼 있지 않았기 때문이다.
- 기업 보안 담당자는 자사에 적용된 보안 제품이 임의로 삭제되거나, 설정이 변경되지 않도록 해당 제조사에서 제공되는 잠금 기능을 반드시 활성화 하도록 하자.

[파일 진단]

- Trojan/Win32.FileCoder
- HackTool/Win.NetScan
- HackTool/Win.Disabler
- Trojan/BAT.Delete

[IOC 정보]

- 58c8c8c3038a5fbca2202248a1101da0
- 48755f2d10f7ff1050fbd081f630aaa3
- 230c143d283842061b14967d4df972d0
- 0a50081a6cd37aea0945c91de91c5d97
- 116e1e7a0c8d3ff9175b87927d188835

관련글

동일한 패스워드가 설정된 Local Administrator 계정을 사용하는 기업의 랜섬웨어 감염 사례 – ASEC BLOG

ASEC 분석팀은 최근 Lockis 랜섬웨어 감염 피해를 입은 업체의 피해 시스템들을 분석한 결과, 공격자가 피해 시스템들에 로컬 Administrator 계정으로 RDP 접속 후 랜섬웨어를 실행시킨 것

을 확인했다. 피해 시스템들의 로컬 Administrator 정보를 조사한 결과, 1~2년동안 패스워드를 변경하지 않았으며, 모두 동일한 패스워드가 설정돼 있는 것으로 확인됐다. 게다가 해당 NTLM 해시를 복호화한 결과 Administrator 계정의 평문 패스워드는 `1qazxcv 인 것으로 확인됐다. 이 패스워드 문자열은 영…

Lockis 랜섬웨어와 함께 사용된 해킹 툴 – ASEC BLOG

안랩 A-FIRST는 지난 11월경 Lockis 랜섬웨어에 감염된 피해 시스템을 대상으로 포렌식 분석을 수행했다. Lockis 랜섬웨어는 러시아 공격 그룹인 TA505가 사용하는 GlobeImposter 랜섬웨어의 변종으로, 지난 9월 16일 처음 등장했다. GlobeImposter 랜섬웨어는 2017년 2월에 처음 등장한 이래로 꾸준히 변종이 증가해 현재까지 총 192개의 변종이 발견됐다. 공격자는 랜섬웨어 감염을 위해 악성 스팸 메일 발송, 익스플로잇 공격, RDP 접속 등의 공격 기법을 사용하는 것으로 알려져 있다. 현재 Lo…

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:미분류, 악성코드 정보, 침해사고 분석 사례

Tagged as:Forensics, 침해사고, Lockis