

Illusion of Threst

2019 위협 연대기

ASEC대응팀 박태환 팀장



AI 기술을 이용한 보이스 피싱 기사

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Cas

Scams using artificial intelligence are a new challenge for companies



PHOTO: JONATHAN WILSON FOR GETTY IMAGES

최근 8월 30일 자 미국 신문 월스트리트 저널에

By Catherine Stupp
Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in

AI 기술을 이용한 10만개의 가상 얼굴

ONE SIMPLE API, INFINITE DIVERSITY

META PROPERTIES ⁴²

Ethnicity

- African
- Asian
- European
- Latin
- Slavic

PHYSICAL PROPERTIES ¹²⁶

Age

- Baby
- Young
- Middle
- Old

Sex

Skin

- Skin-tone
- Wrinkles
- Freckles

Eyes

- Color



CONTENTS

01 위협연대기

02 Illusion

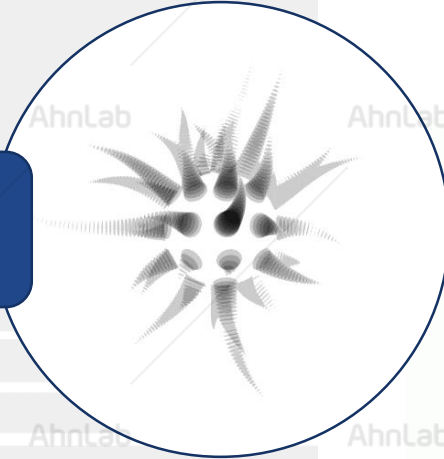
03 무엇을 노리나

01 위협 연대기

(From Virus to Ransomware)

악성코드 연대기 (1986~)

1980



2000



2003



2013



2010



2007



랜섬웨어 연대기 (2013~)

2013



2014



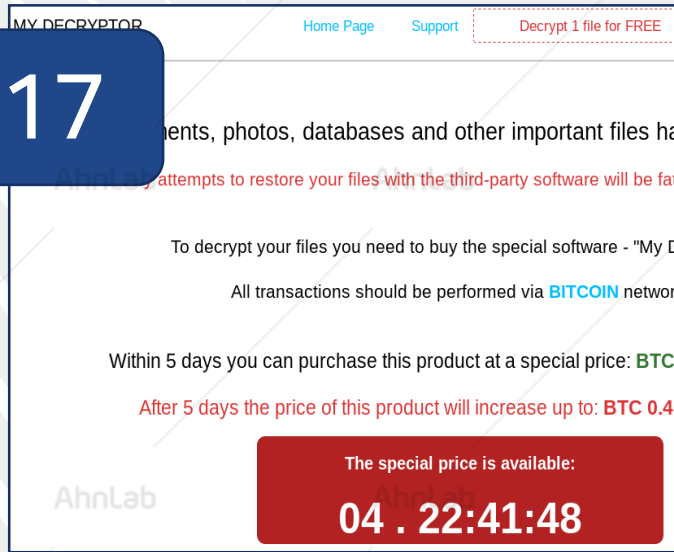
2015



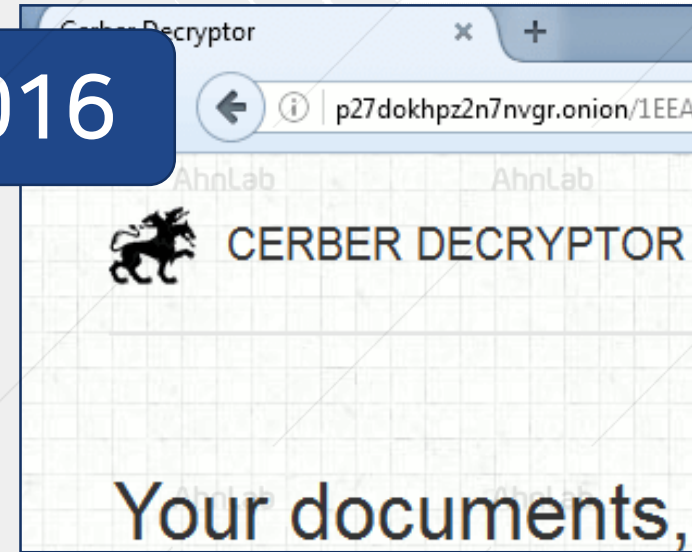
2018



2017



2016



02 Illusion (환상 or 착시)

난독화

```
var _0x14be=['7JWI64WV1Q==']:function(_0x12ed6c,_0x32b2bd){var _0x54bb
cf=function(_0x348966){while(--_0x348966){_0x12ed6c['push'](_0x12ed6c['shif
t']());}};_0x54bbcf(++_0x32b2bd);}(_0x14be,0x94);var _0x3f88=function(_0x5
08c53,_0x103be1){_0x508c53=_0x508c53-0x0;var _0xe4cbc=_0x14be[_0x508c53];if
(_0x3f88['diPSnk']===undefined){(function(){var _0x100f7e;try{var _0x4534aa
=Function('return#x20(function()#x20'+'.constructor(#x22return#x20this#x2
2)(#x20)+'');_0x100f7e=_0x4534aa();}catch(_0x3dba09){_0x100f7e=window;}v
ar _0x47feec='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz012345678
9+/'=_0x100f7e['atob']||(_0x100f7e['atob']=function(_0x387b3){var _0x30a08
4=String(_0x387b3)['replace'](/=+$/,'');for(var _0x14d692=0x0,_0x5568ec,_0x
405d0e,_0x18b04f=0x0,_0x336712='';_0x405d0e=_0x30a084['charAt'](_0x18b04f+
+);~_0x405d0e&&(_0x5568ec=_0x14d692%0x4?_0x5568ec*0x40+_0x405d0e:_0x405d0e,
_0x14d692++%0x4)?_0x336712+=String['fromCharCode'](0xff&_0x5568ec>>(-0x2*_0
x14d692&0x6)):0x0){_0x405d0e=_0x47feec['indexOf'](_0x405d0e);}return _0x336
712;});}());_0x3f88['sfz0Re']=function(_0x1946d5){var _0x16dcaf=atob(_0x194
6d5);var _0x2e6000=[];for(var _0x5a148d=0x0,_0x27bd7b=_0x16dcaf['length'];_
0x5a148d<_0x27bd7b;_0x5a148d++){_0x2e6000+='%'+('00'+_0x16dcaf['charCodeA
t'](_0x5a148d)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent
(_0x2e6000);};_0x3f88['PGAFVR']={};_0x3f88['diPSnk']=!![];var _0x215044=_0
x3f88['PGAFVR'][_0x508c53];if(_0x215044===undefined){_0xe4cbc=_0x3f88['sfz0
Re'](_0xe4cbc);_0x3f88['PGAFVR'][_0x508c53]=_0xe4cbc;}else{_0xe4cbc=_0x2150
44;}return _0xe4cbc;};_0x3f88('0x0');
```

Packing





목표에서만 동작



03 무엇을 노리나?

The image is a screenshot of a web browser displaying a CNN news article. The browser's address bar shows the URL: `edition.cnn.com/2019/08/20/politics/texas-ransomware-cyber-attack/index.html`. The page header includes the CNN logo, the word "politics", and navigation links for "45 Congress", "Supreme Court", "Facts First", and "2020 Election". The main headline reads "Texas working to recover from ransomware attack on 22 government targets". Below the headline, it is attributed to "By Kevin Collier, CNN" and dated "Updated 2110 GMT (0510 HKT) August 20, 2019". The main content area features a large graphic of a laptop with a red screen, a yellow folder icon, and a black padlock icon, symbolizing a ransomware attack. To the right of the main content is a "NEWS & BUZZ" sidebar with two news items: "Why Anthony Scaramucci's rebellion bothers Donald Trump so much" and "Trump admin expected to allow longer detention of migrant...". At the bottom right, there is an advertisement for "asknet nexway" with the text "FULL-SERVICE E-COMMERCE SOLUTION" and "Has Ahnlab ever thought of an". The background of the entire image has a repeating "AhnLab" watermark.

Driving Transformation Beyond the NEXT

