FireEye

SSL암호화를 활용한 보안위협 동향 및 대응 방안

박병하 차장

OPENBASE

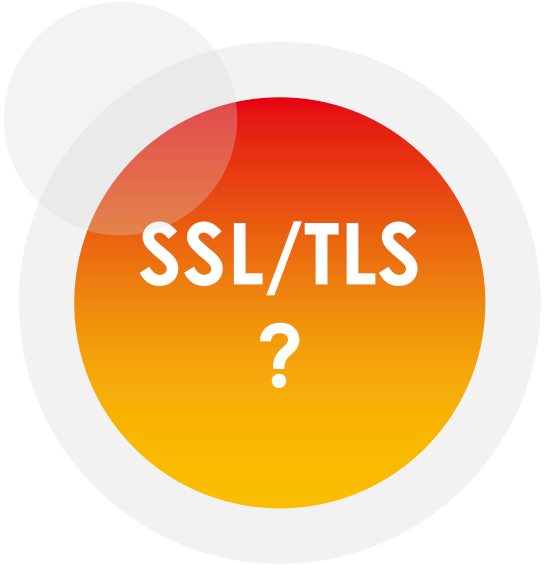
Agenda

- SSL Traffic 트랜드
- 암호화를 활용한 공격 유형
- SSL복호화 솔루션과의 결합
- SSL 복호화 솔루션 체크리스트

©2018 FireEye | Private & Confidential

FireEye

SSL Traffic 트랜드



$$SSL \cong TLS = \frac{\text{디지털 인증서 + 해쉬 함수}}{\text{공개키암호화 + 비밀키 암호화}}$$

= 네트워크 통신 보안 기법

©2018 FireEye | Private & Confidential

SSL 사용 이유

SSL/TLS 의 장점

- 기술적으로 쉽게 적용
- 접속하는 사이트가 안전함을 보장
- 전달하는 내용이 정확하고 안전하게 전달을 보장



서버 신뢰성 확보



Sniffing 방지



변경 방지

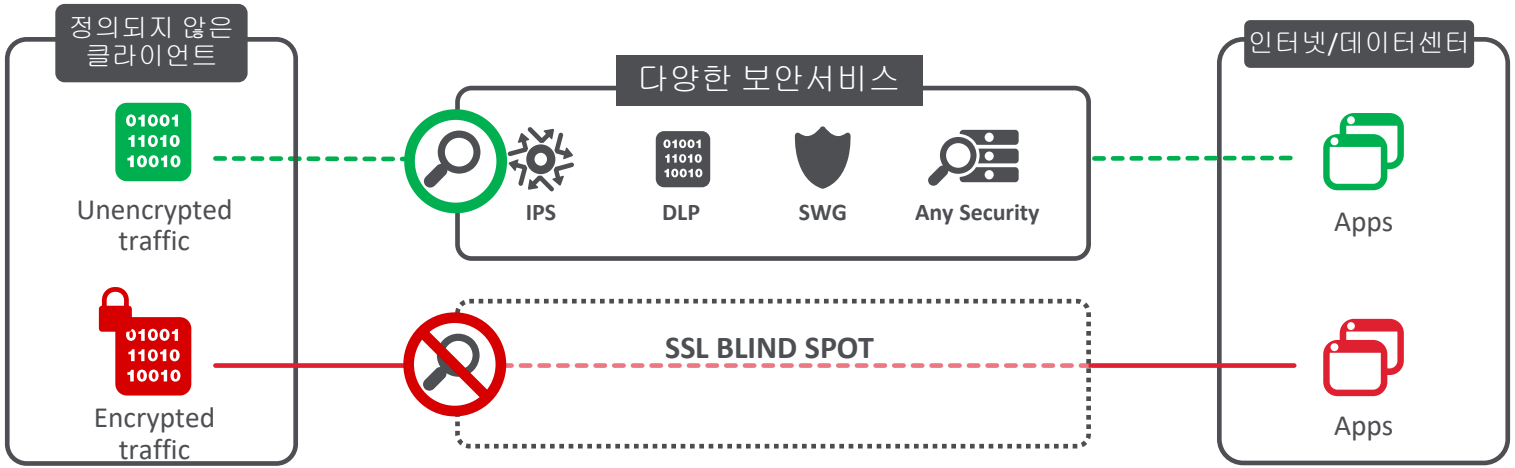


위장 방지

누구나 손쉽게 고수준의 네트워크 통신 보안 확보

©2018 FireEye | Private & Confidential

Blind Spot



암호화된 트래픽에 대해 복호화를 하지 않고 그대로 전달하여
Blind Spot을 생성함

©2018 FireEye | Private & Confidential

암호화 채널에 숨은 공격

- SSL은 안전하다는 고정관념

그러나

SSL은 공격자에게도 '안전한' 공격 경로



모든 국내 외 보안업체가 SSL을 이용한 숨겨진 공격 방식에 대해 경고!

FORTINET

THE RAPID GROWTH OF SSL ENCRYPTION

The Dark Side of SSL That Today's Enterprise Can't Ignore

- FORTINET (2017)-

The Rise in SSL-based Threats

Overview

The majority of Internet traffic is now encrypted. With the advent of free SSL

-Zscaler (2017.2)-

2016 Security Predictions

With the blurring of network boundaries and the increasing number of connected devices, we predict even more attacks and vulnerability disclosures next year. Take a look at our top 5 security predictions for 2016.

1 Attacks hidden in SSL traffic will exceed attacks in clear text

-A10 (2016년 5가지 주요 보안 예측)-

2015년 8대 보안 위협

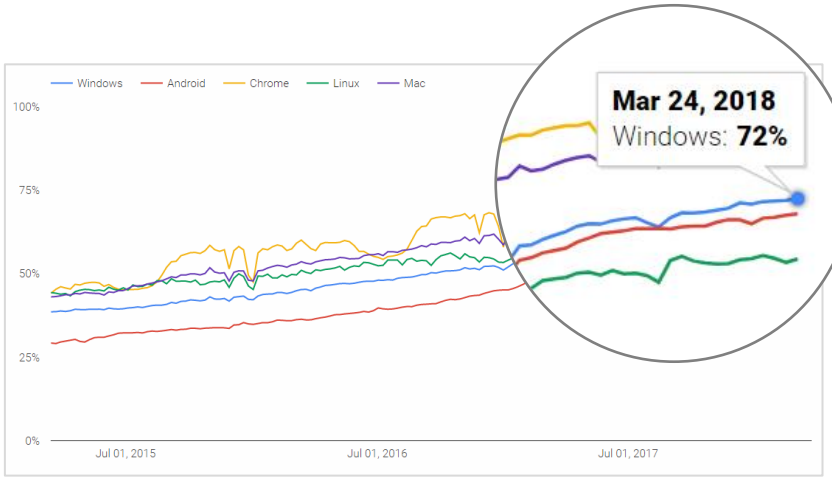
1 암호화를 이용한 공격과 기존 공격기법의 혼합 증가

- 이글루 시큐리티 (2015년 보안 위협 전망 보고서)-

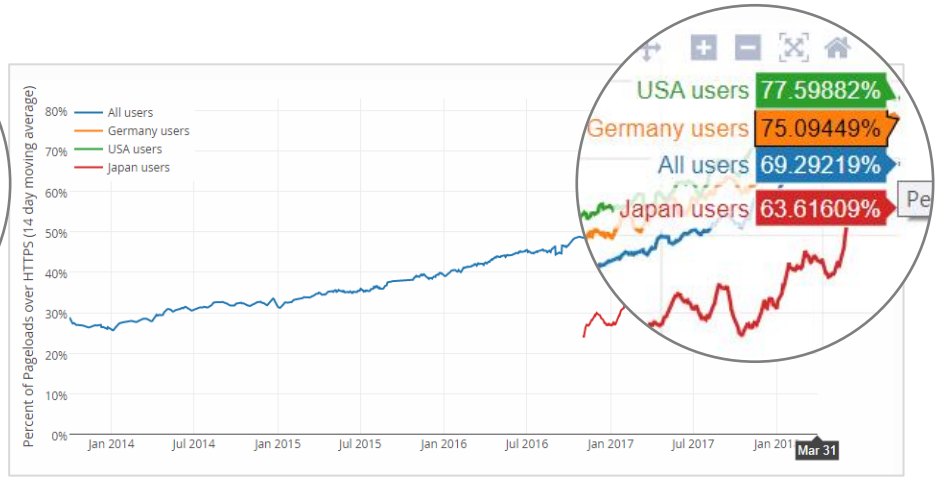
©2018 FireEye | Private & Confidential

SSL 사용 트랜드

HTTPS기반의 페이지 로딩 비율



https://transparencyreport.google.com/https/overview?hl=en



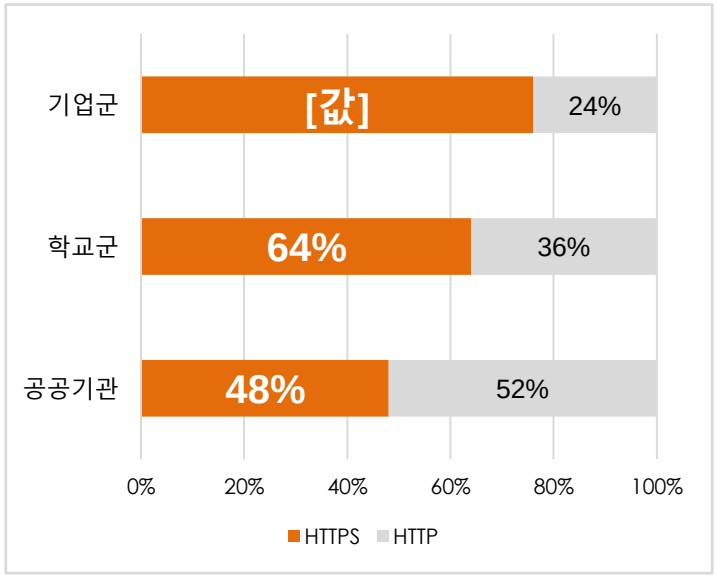
https://letsencrypt.org/stats/

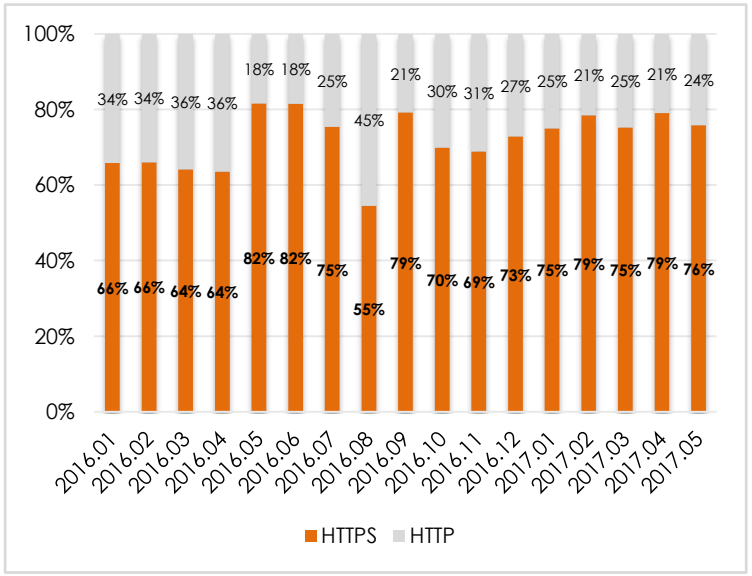
대부분의 플랫폼에서 70% 이상 사용 중

©2018 FireEye | Private & Confidential

SSL/TLS 현황

국내 트래픽 현황





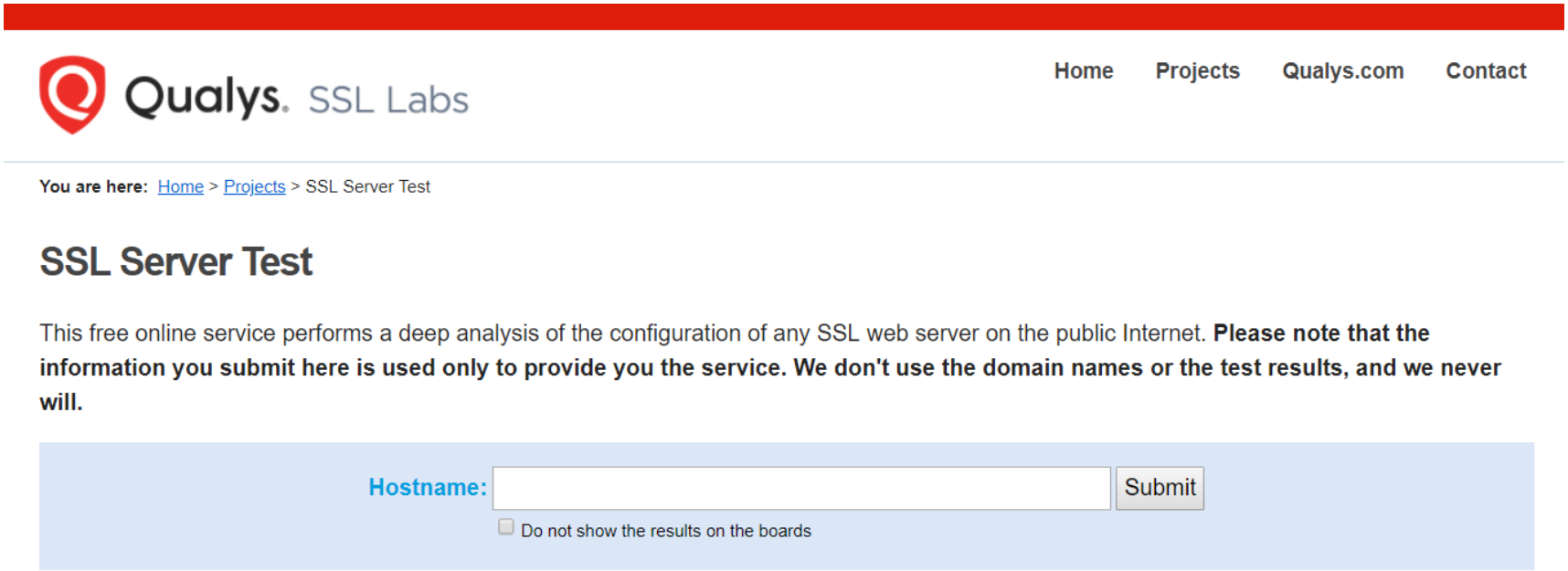
- **현 시점, HTTPS 비중 최소 50% 이상 사용 중**

<출처: SOOSAN INT Traffic Analysis Report 2017>

©2018 FireEye | Private & Confidential

SSL 안정성 확인

https://www.ssllabs.com



©2018 FireEye | Private & Confidential

SSL 안정성 확인

https://www.ssllabs.com

Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.google.com Fingerprint SHA256: 492a73666bf8e6f1cc38c250898126e69f4d74c0304226906fb2ca78a675fa34 Pin SHA256: ZhtZ5Sw7/fPEouYYutX3KifEE6hFtlAKVBU1iL+cNwU=
Common names	www.google.com
Alternative names	www.google.com
Serial Number	71e4224fff2d7f5f
Valid from	Tue, 20 Mar 2018 17:34:07 UTC
Valid until	Tue, 12 Jun 2018 16:55:00 UTC (expires in 2 months and 7 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	Google Internet Authority G3 AIA: http://pki.goog/gsr2/GTSGIAG3.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (TLS extension)

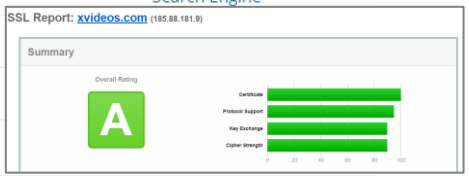
©2018 FireEye | Private & Confidential

SSL/TLS 현황

국내외 웹사이트 Top 10

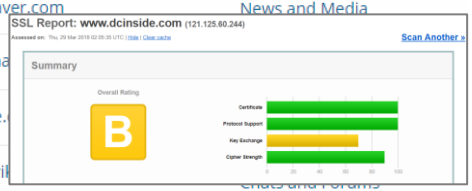
Rank	Website	Category
1	google.com	
2	facebook.com	
3	youtube.com	
4	baidu.com	Internet and Telecom > Search Engine
5	xvideos.com	
6	xnxx.com	
7	google.co.in	
8	yahoo.com	News and Media
9	vk.com	Internet and Telecom > Social Network
10	twitter.com	Internet and Telecom > Social Network





Rank	Website	Category
1	naver.com	News and Media
2	google.co	
3	daum.ne	
4	youtube.	TV and Video
5	google.com	Internet and Telecom > Search Engine
6	facebook.com	Internet and Telecom > Social Network
7	news.naver.com	News and Media
8	sports.na	
9	dcinside.	
10	namu.wi	



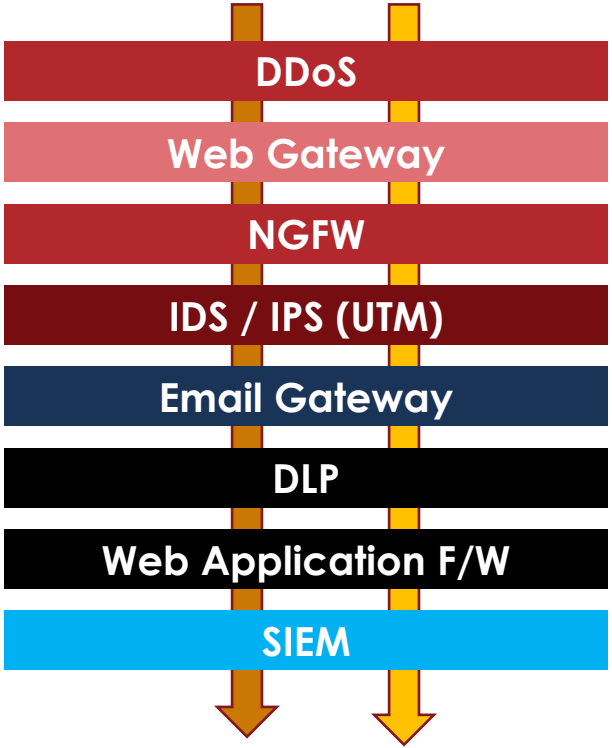


https://www.similarweb.com/top-websites
https://www.ssllabs.com/ssltest/

©2018 FireEye | Private & Confidential

새로운 우회 기법

암호화를 통한 Anti-Detection



- 기존의 보안솔루션 우회 기법

  Zero-Day Threats

  Anti-emulation

  Anti-VM (Human Interaction)

- 모든 Attack Cycle에 암호화된 트래픽 적용

  Exploit

  Malware Download

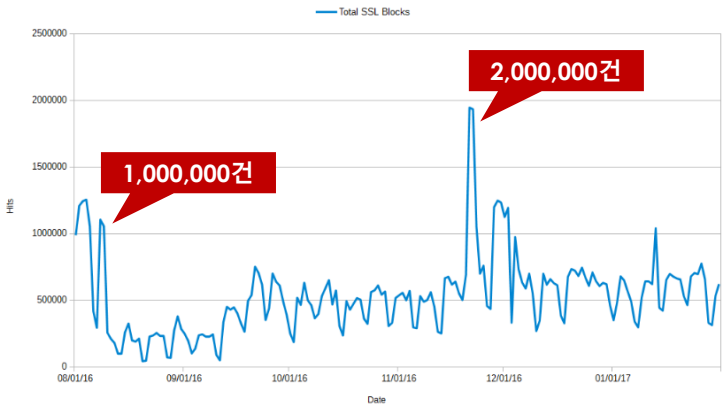
  Callback

©2018 FireEye | Private & Confidential

SSL기반 악성코드 글로벌 공격 현황

Malicious SSL Activity

During the six-month period, the ThreatLabZ research team observed that the Zscaler cloud blocked an average 600,000 malicious activities each day that used SSL, including exploit kit traffic, malware and adware distribution, malware callbacks, and other malicious traffic.



<2016년 8월 – 2017년 1월, Zscaler Cloud의 트래픽 분석>

유해 SSL Activity 공격 발생

1일 평균 60만회

- Exploit kit traffic
- Malware
- Adware Distribution
- Malware callback
- Malicious traffic
- Phishing
- C&C Communication

©2018 FireEye | Private & Confidential

FireEye

암호화를 활용한 공격 유형

암호화 채널에 숨은 공격

Attack Cycle



Exploit

Deliver the payload
Exploit



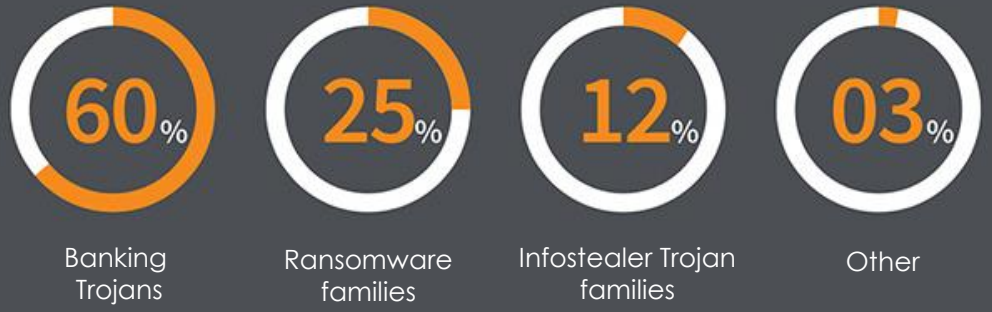
Malware Download

Malicious Sites
Phishing Page



Callback

SSL based C&C



암호화 채널에 숨은 공격 #1

Callback and Beacon



- **HTTPS 서버를 이용하면, SSL을 직접 구현할 필요가 없어 개발이 용이.**
- **초기 발견 어려움 -> 분석 이후 발견 가능**
- **특히, Google Docs와 같은 사이트를 이용하면 IP 및 Port 차단도 불가!!**

PCLOUD

```
push    23h
xor     edx, edx
push    offset aHttpsApiPcloud ; "https://api.pcloud.com/oauth2_token"
mov     [eax], dx
call    sub_1AB3280
```

.box.com/2.0/files/%s/conten"...

```
push    2Dh
xor     eax, eax
mov     [ebp+var_85C], 7
push    offset aHttpsContentDr ; "https://content.dropboxapi.com/2/files/"..
lea     ecx, [ebp+var_870]
```

YANDEX

```
push    eax
lea     eax, [ebp+var_2210]
push    offset aHttpsCloudApiY_0 ; "https://cloud-api.yandex.net/v1/disk/re"..
push    eax             ; int
call    sub_1AADBC0
```

http://ciscokrblog.com/1275

©2018 FireEye | Private & Confidential

암호화 채널에 숨은 공격 #2

SNS를 활용한 공격

Home 〉 전체기사

페이스북·인스타그램 등 SNS 위력 활용해 사이버 공격

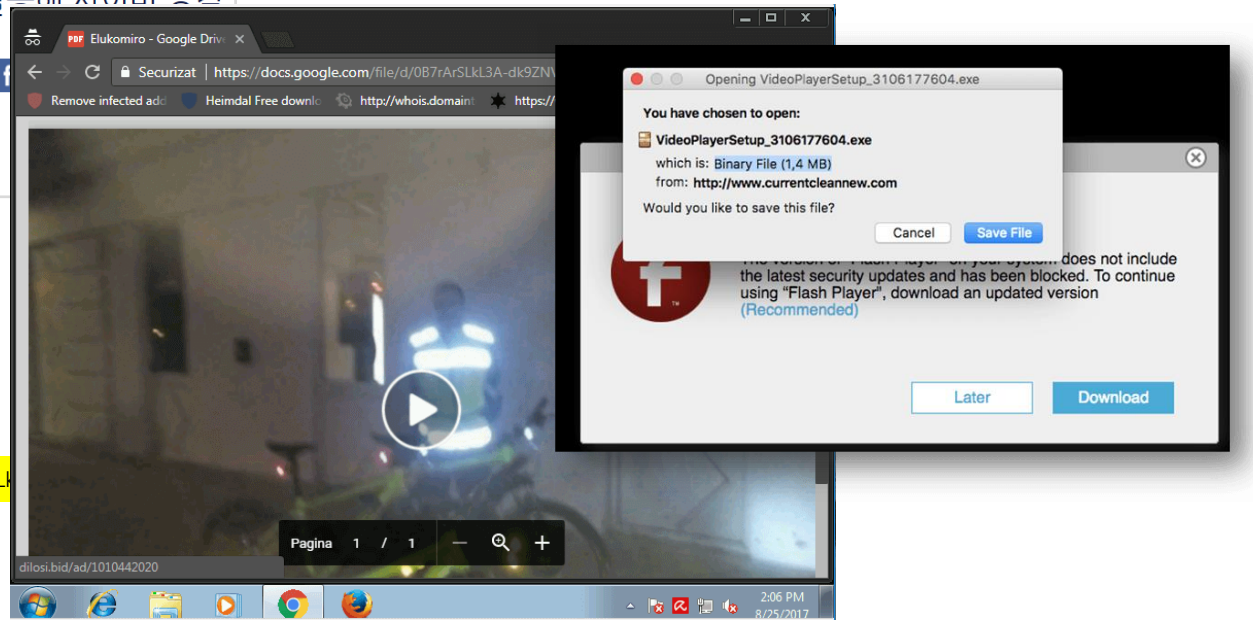
좋아요 16개 | 입력 : 2017-09-01 16:35 가 가

사이버 공격자, 인스타그램에선 유명인 크리덴셜 빼돌리고

페이스북 메신저로는 멀웨어 퍼뜨리고 악성 크롬 익스텐션 설치

Peter Video 😎
http://bitly.com
/2v8tlRs?Peter

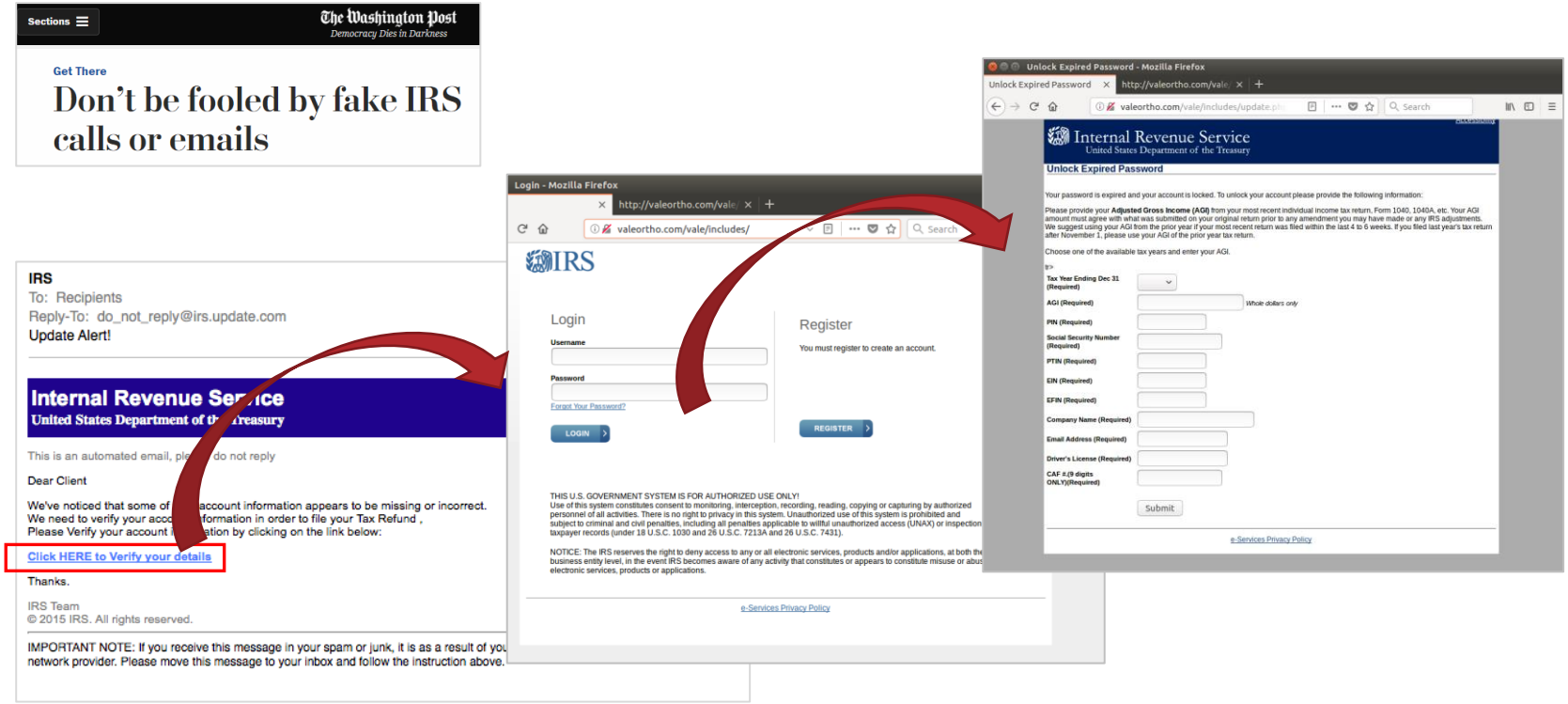
https [://] docs.google [.] com/file/d/0B7rArSL



©2018 FireEye | Private & Confidential

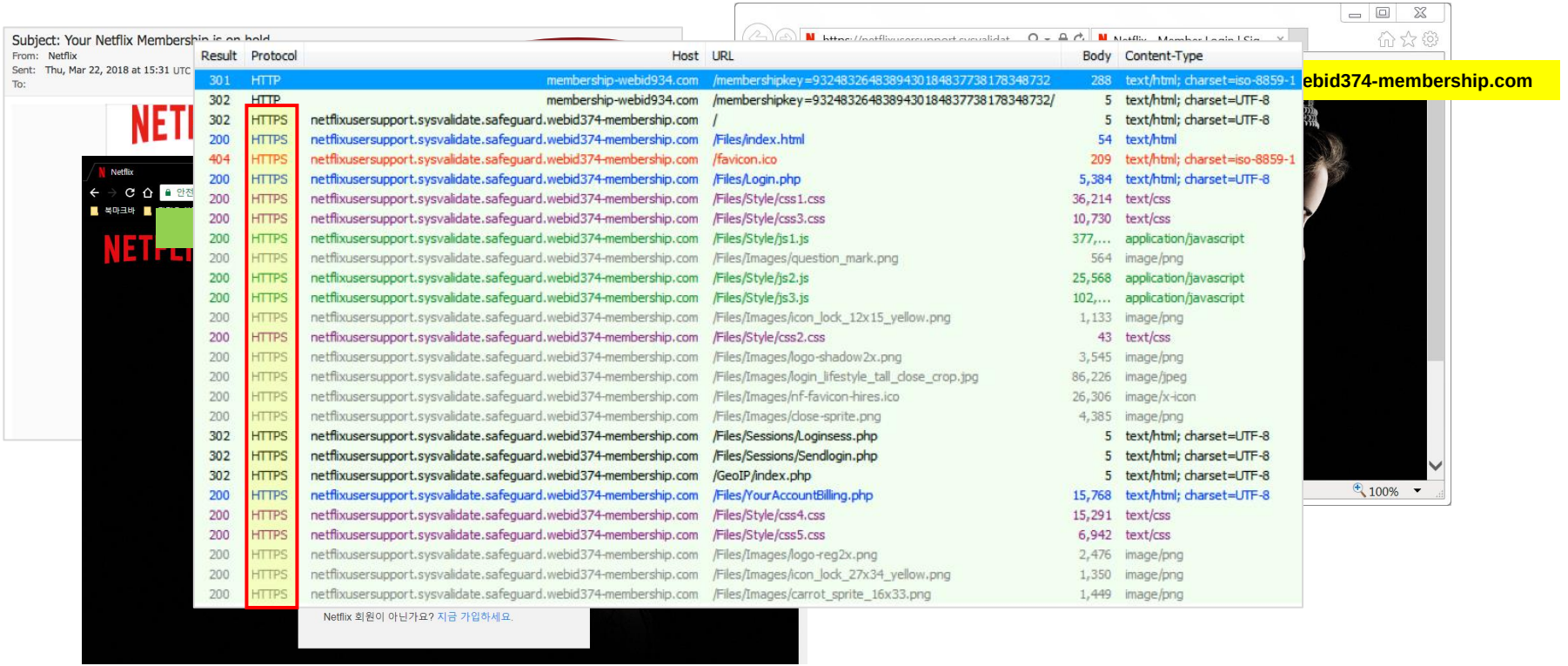
암호화 채널에 숨은 공격 #3

암호화된 페이지를 활용한 피싱 공격



암호화 채널에 숨은 공격 #4

스피어피싱 + 피싱 공격

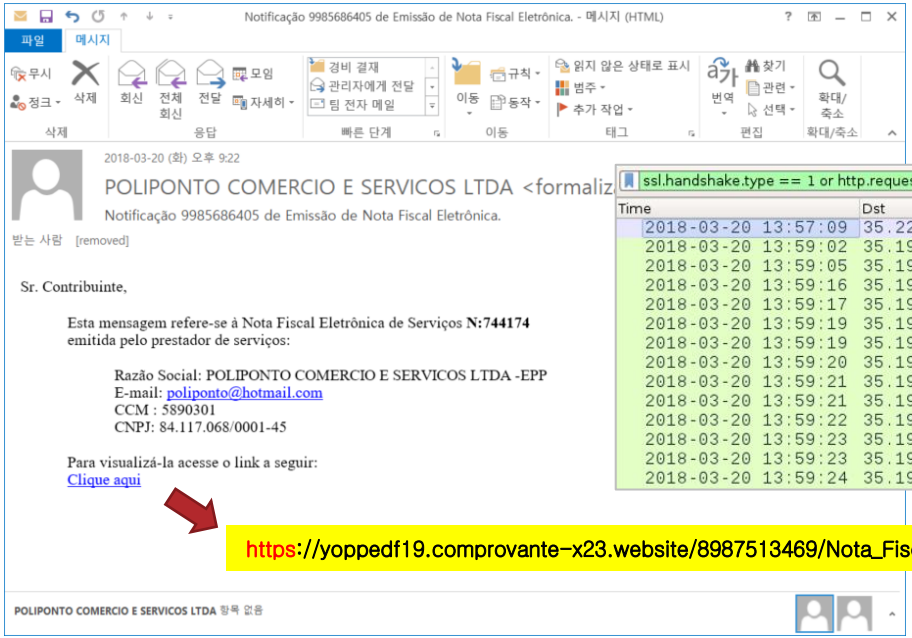


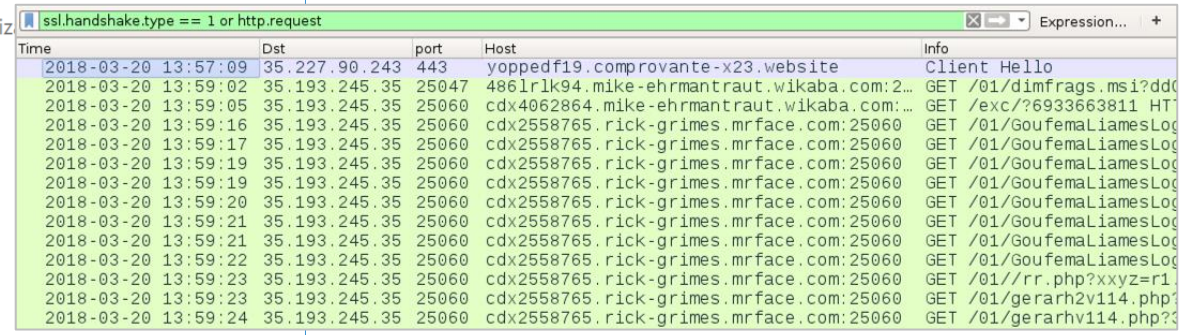
Result	Protocol	Host	URL	Body	Content-Type
301	HTTP	membership-webid934.com	/membershipkey=9324832648389430184837738178348732	288	text/html; charset=iso-8859-1
302	HTTP	membership-webid934.com	/membershipkey=9324832648389430184837738178348732/	5	text/html; charset=UTF-8
302	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/	5	text/html; charset=UTF-8
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/index.html	54	text/html
404	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/favicon.ico	209	text/html; charset=iso-8859-1
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Login.php	5,384	text/html; charset=UTF-8
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/css1.css	36,214	text/css
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/css3.css	10,730	text/css
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/js1.js	377,...	application/javascript
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/question_mark.png	564	image/png
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/js2.js	25,568	application/javascript
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/js3.js	102,...	application/javascript
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/icon_lock_12x15_yellow.png	1,133	image/png
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/css2.css	43	text/css
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/logo-shadow2x.png	3,545	image/png
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/login_lifestyle_tall_close_crop.jpg	86,226	image/jpeg
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/nf-favicon-hires.ico	26,306	image/x-icon
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/close-sprite.png	4,385	image/png
302	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Sessions/Loginsess.php	5	text/html; charset=UTF-8
302	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Sessions/Sendlogin.php	5	text/html; charset=UTF-8
302	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/GeoIP/index.php	5	text/html; charset=UTF-8
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/YourAccountBilling.php	15,768	text/html; charset=UTF-8
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/css4.css	15,291	text/css
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Style/css5.css	6,942	text/css
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/logo-reg2x.png	2,476	image/png
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/icon_lock_27x34_yellow.png	1,350	image/png
200	HTTPS	netflixusersupport.sysvalidate.safeguard.webid374-membership.com	/Files/Images/carrot_sprite_16x33.png	1,449	image/png

©2018 FireEye | Private & Confidential

암호화 채널에 숨은 공격 #5

암호화 다운로드 링크를 활용한 스피어피싱 공격





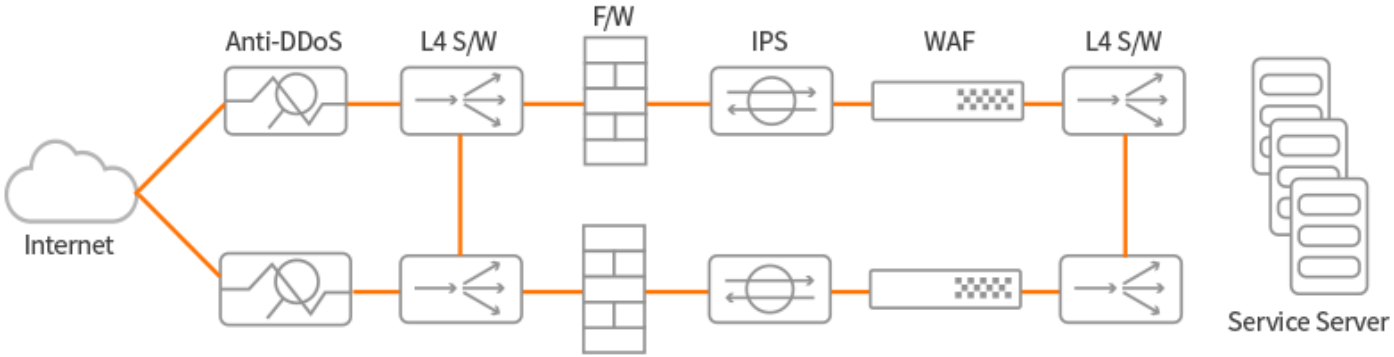
©2018 FireEye | Private & Confidential

FireEye

SSL복호화 솔루션과의 결합

SSL복호화 적용 방안

One Source Single Use



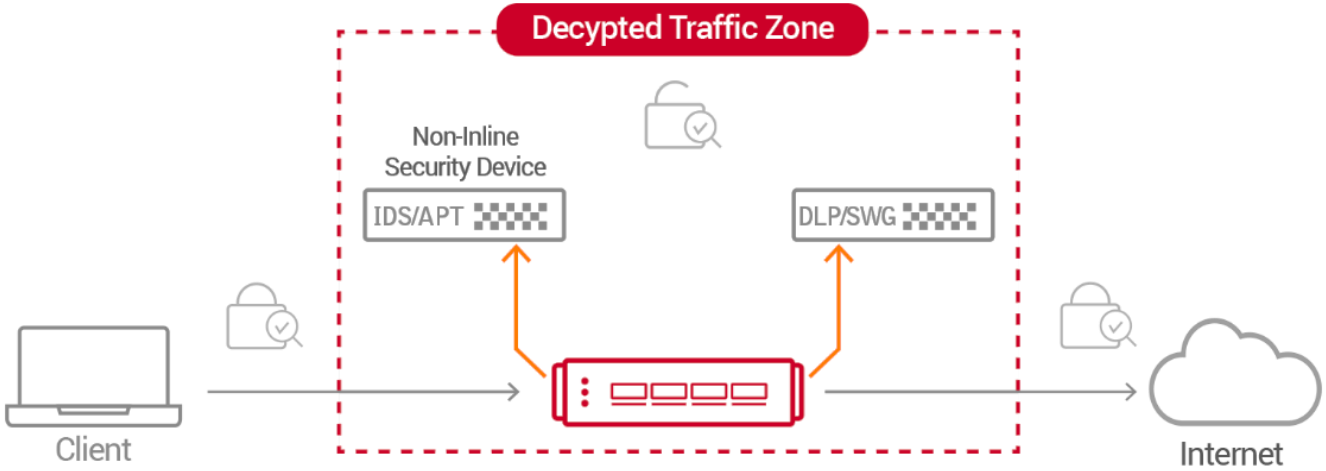
SSL inspection and cryptography can degrade network performance

by as much as **75 percent**

©2018 FireEye | Private & Confidential

SSL복호화 적용 방안

One Source Multi Use

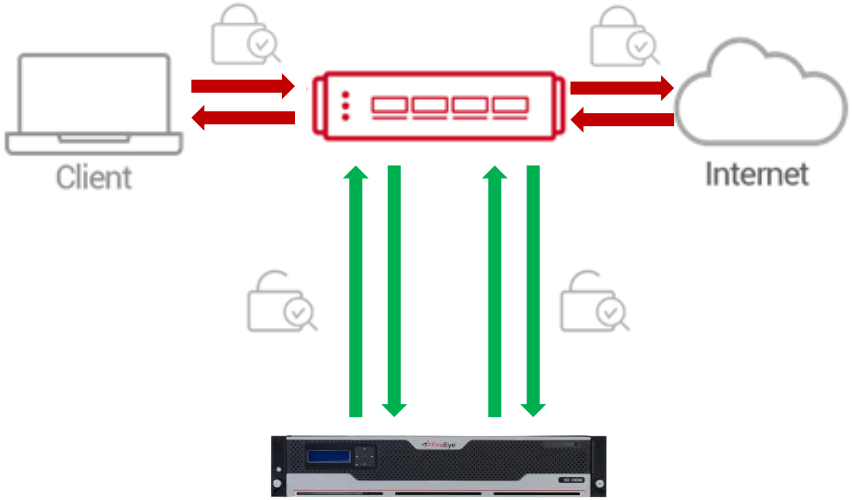


Decrypted Traffic Zone 구성을 통한 기존 보안 체계 유지.

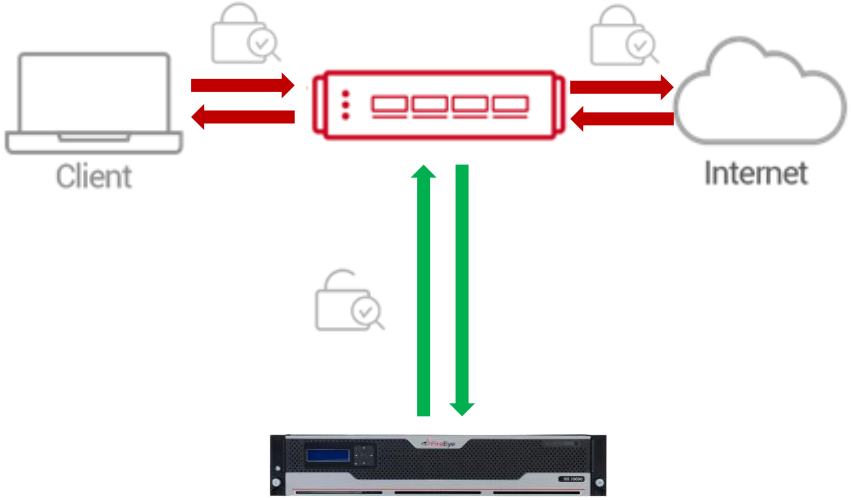
1회 복호화 후 다양한 보안 장비를 그대로 유지하는 체계 구성

©2018 FireEye | Private & Confidential

SSL복호화 솔루션과 FireEye



Active Intercept Deployment



Passive Intercept Deployment

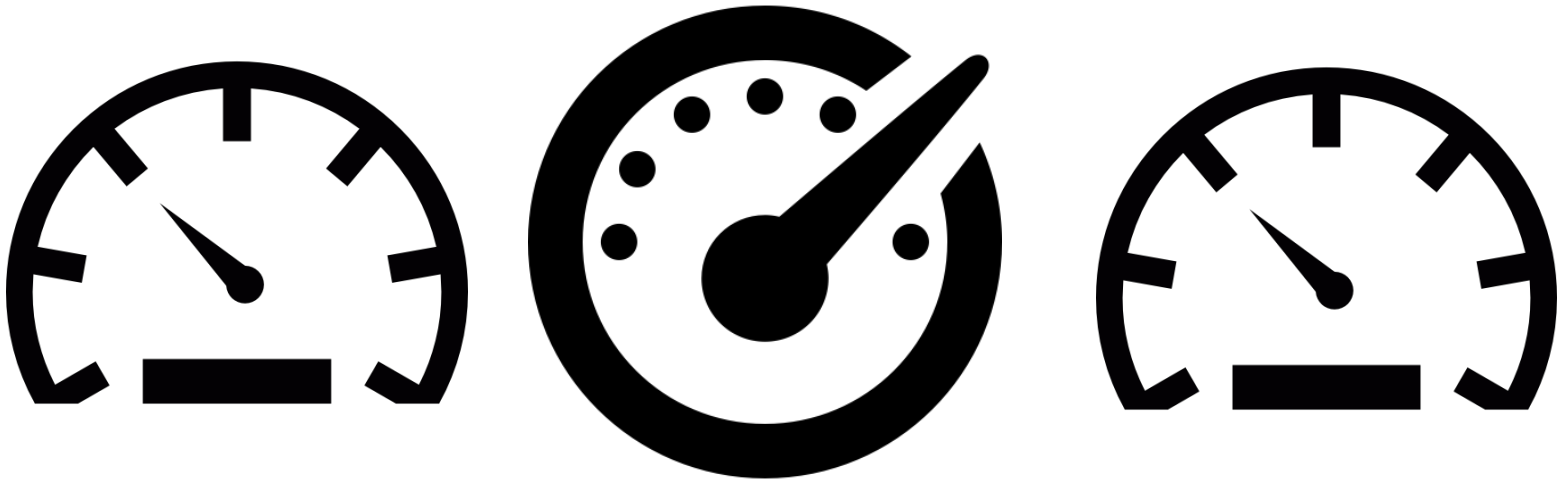
©2018 FireEye | Private & Confidential

FireEye

SSL 복호화 솔루션 체크리스트

Pain Point #1

네트워크 성능 저하가 있는가?



©2018 FireEye | Private & Confidential

Pain Point #2

기존 시스템과의 연동은 완벽히 동작하는가?



©2018 FireEye | Private & Confidenti

Pain Point #3

가시성 확보



©2018 FireEye | Private & Confidential

Pain Point #4

구축 편의성 – 구성변경 최소화 및 인증서배포



DEPLOY FAST

DEPLOY EASY

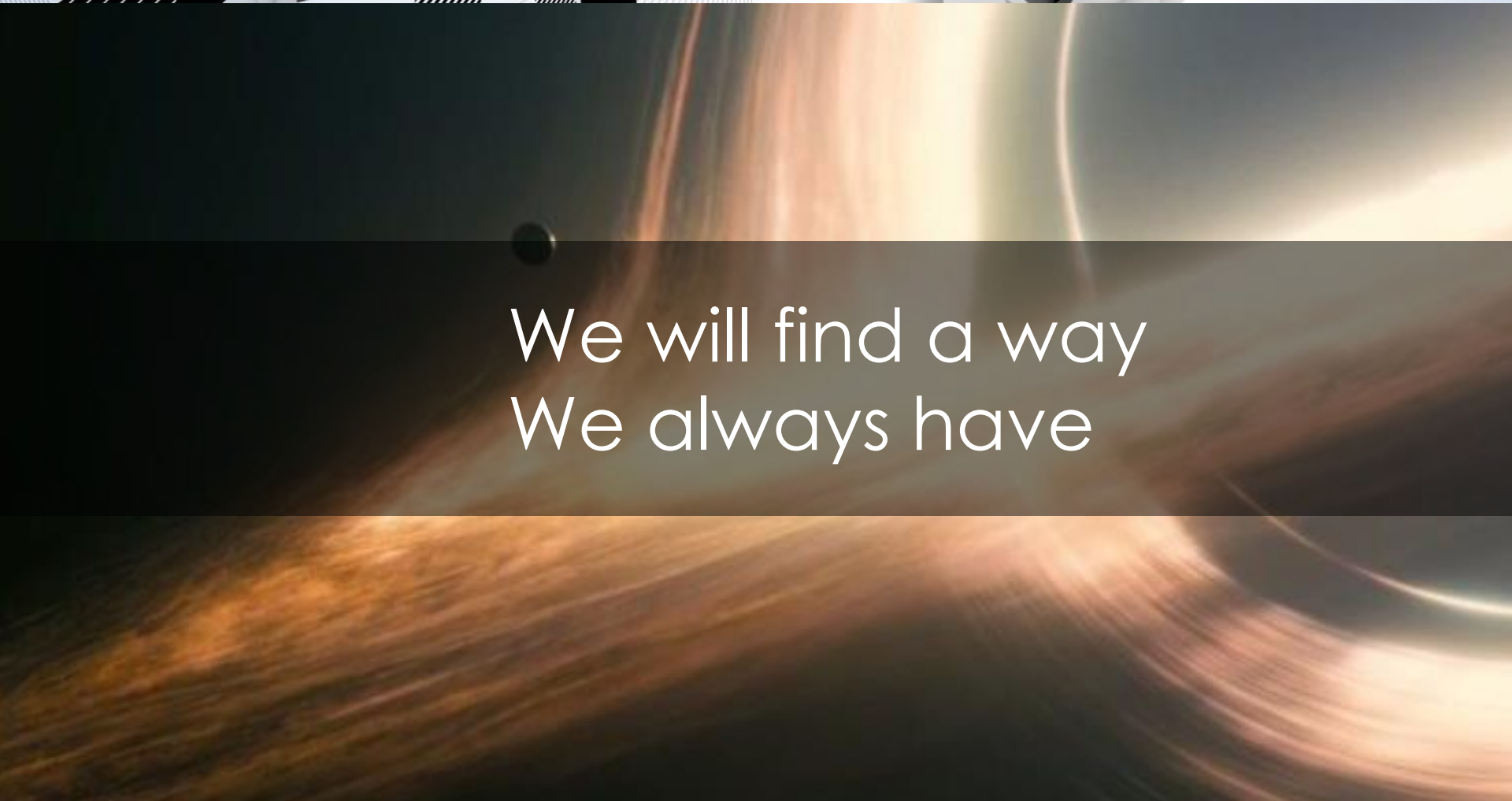
©2018 FireEye | Private & Confidential

Pain Point #5

High Availability



©2018 FireEye | Private & Confidential


We will find a way
We always have

FireEye

Thank You