First Half of 2017, SSL Traffic Analysis in KOREA Brief Report

September 15, 2017

Research and Development Center,
SOOSAN INT Co.,Ltd

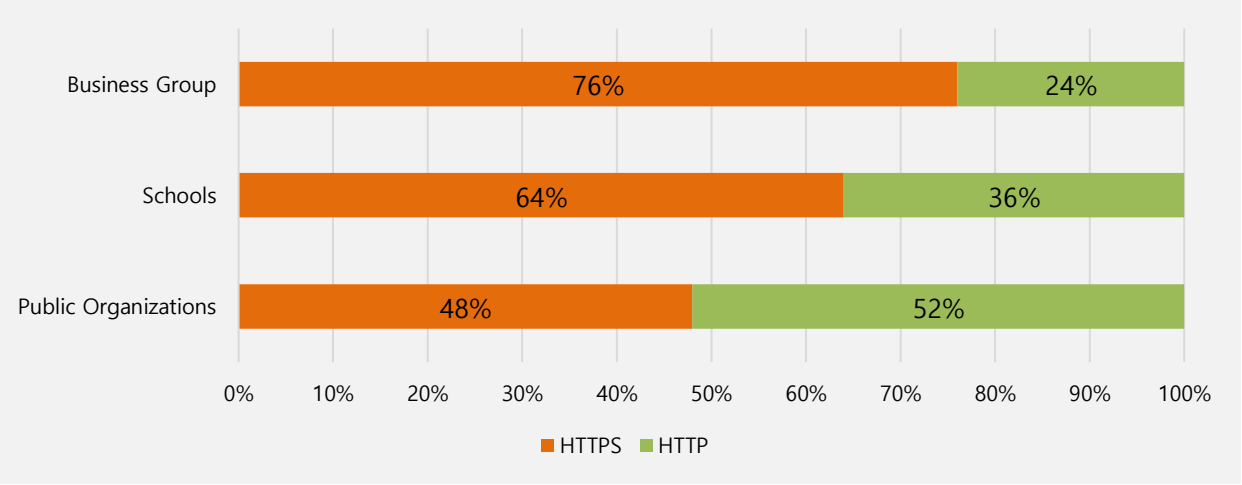
SOOSAN INT

Delivering Innovative Security Solutions and Services

First Half of 2017,

SSL Traffic Analysis Brief Report

1. Total Usage of Web Traffic By the Organization



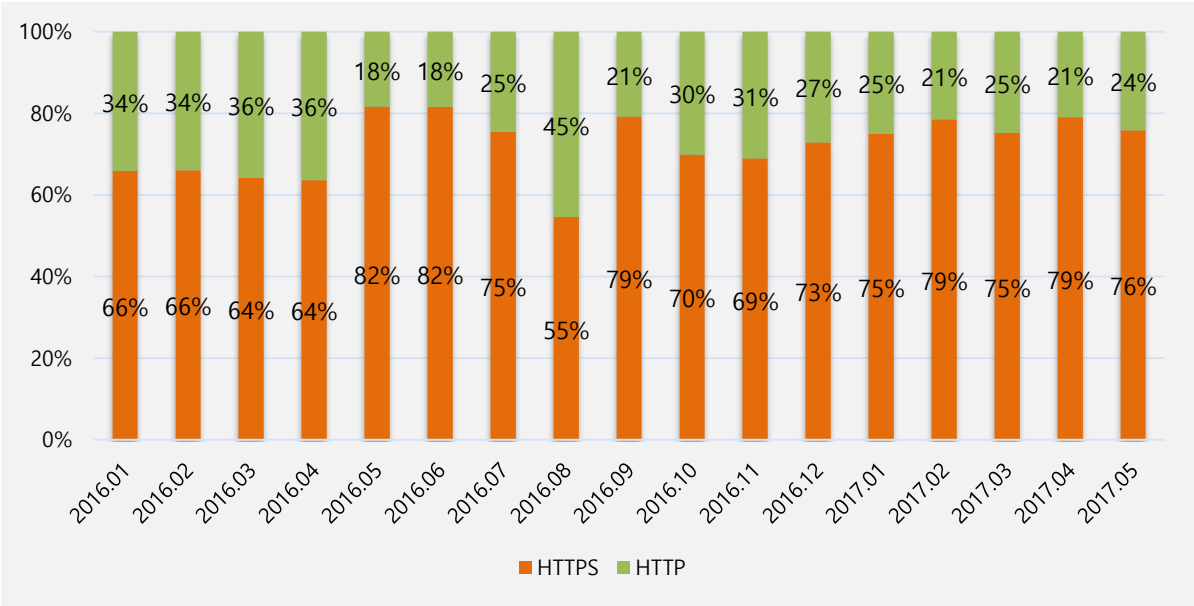
2017.1Q Web Traffic Analysis by the Organization

Since the **Business Group** visits various websites very much such as google.com, more than 70% of entire web traffic that the this group uses is encrypted traffic. The **Schools** including elementary schools and middle schools uses encrypted traffic by the volume of more than 60 % of entire web traffic, while the **Public Organizations** uses only about 50 % of web traffic for encrypted traffic.

First Half of 2017,

SSL Traffic Analysis Brief Report

2. Web Traffic Monthly Usage of the Business Group



2016/2017 Web Traffic Analysis of the Business Group

While the Business Group uses encrypted websites in the range of 60 % in 2016, the encrypted traffic used by the Business Group in 2017 has been increasing by the range of 70 % in average. Comparing both years, about 10 % of increase for encrypted traffic has happened.

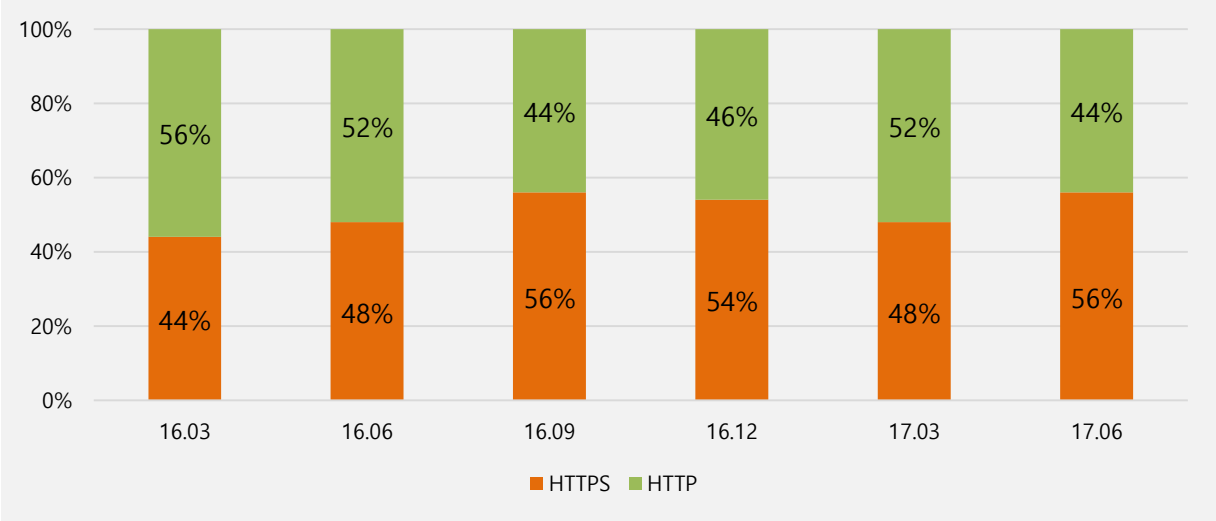
ePrism SSL Visibility Device is available for various solutions:
If you use one of the followings, please think about adopting SSL decryption solutions.

- Firewalls
- Secure Web Gateways (SWG)
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM) platforms
- Data Loss Prevention (DLP) products
- Threat Prevention platforms
- Network Forensics and Web Monitoring tools

First Half of 2017,

SSL Traffic Analysis Brief Report

3. Web Traffic Quarterly Usage of the Public Organizations

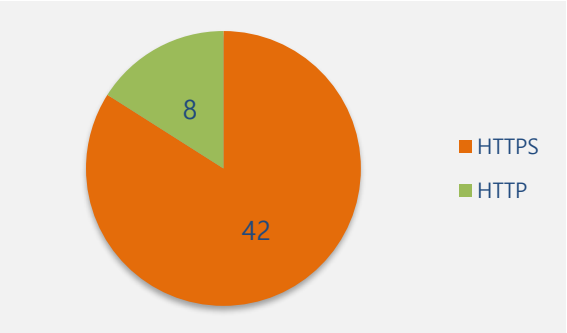


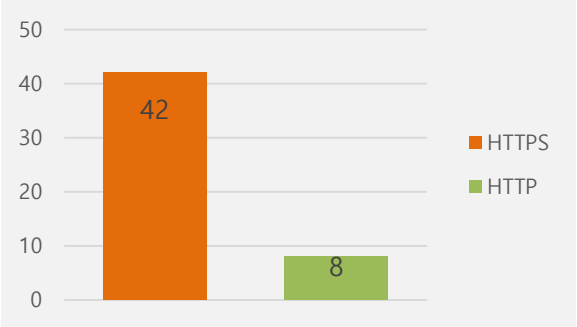
2016/2017 Web Traffic Analysis of the Public Organizations

The Public Organizations uses average 50 % of entire web traffic for encrypted traffic. However, when comparing the first half of 2017 with the first half of 2016, the volume of encrypted traffic increased by 10 % during the 1Q and 15 % during the 2Q . The percentage of the increase is expected to be bigger during 3Q and 4Q in 2017.

First Half of 2017,
SSL Traffic Analysis Brief Report

4. Encryption Coverage Rate for the Top 50 Global Websites for Traffic

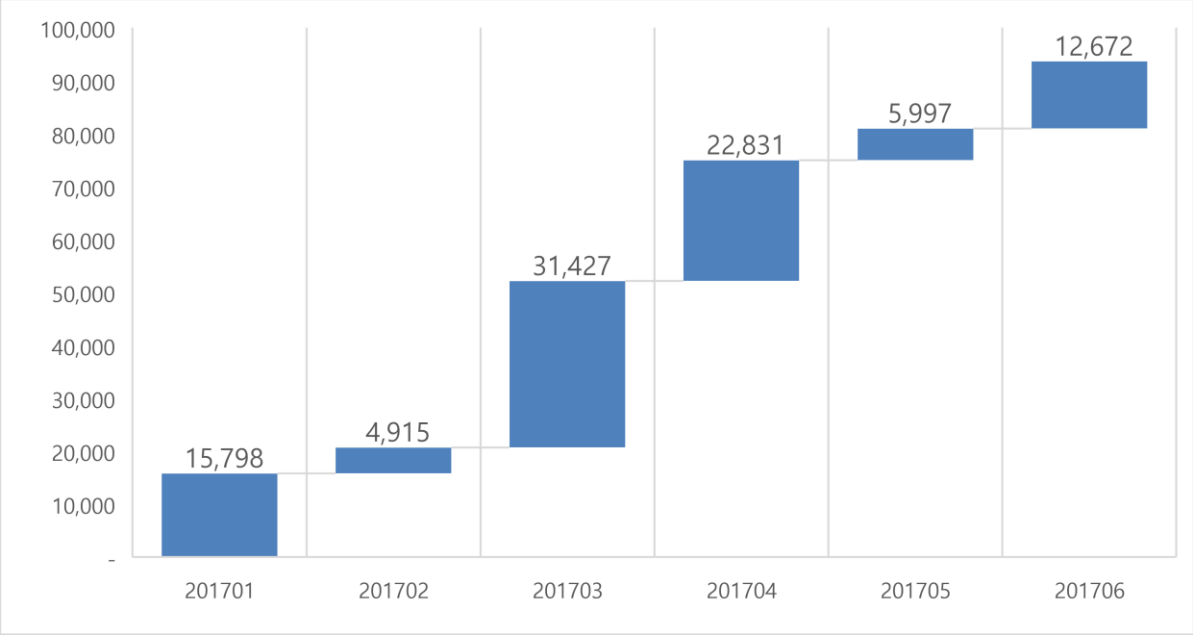




Rank	Website	SSL Application	Rank	Website	SSL Application
1	Google.com	o	26	Google.fr	o
2	Youtube.com	o	27	Google.com.br	o
3	Facebook.com	o	28	List.tmall.com	o
4	Baidu.com	x	29	Linkedin.com	o
5	Wikipedia.org	o	30	Google.com.hk	o
6	Yahoo.com	o	31	Netflix.com	o
7	Google.co.in	o	32	Yandex.ru	o
8	Reddit.com	o	33	Google.it	o
9	Qq.com	x	34	Yahoo.co.jp	o
10	Taobao.com	x	35	Google.es	o
11	Amazon.com	o	36	T.co	o
12	Google.co.jp	o	37	Pornhub.com	o
13	Twitter.com	o	38	Google.com.mx	o
14	Tmall.com	o	39	Ebay.com	o
15	Vk.com	o	40	Imgur.com	o
16	Live.com	o	41	Google.ca	o
17	Instagram.com	o	42	Alipay.com	x
18	Sohu.com	x	43	Twitch.tv	o
19	Sina.com.cn	x	44	Xvideos.com	o
20	Jd.com	x	45	Bing.com	o
21	Weibo.com	x	46	Youth.cn	o
22	360.cn	o	47	Msn.com	o
23	Google.de	o	48	Aliexpress.com	o
24	Google.co.uk	o	49	Ok.ru	o
25	Google.ru	o	50	Tumblr.com	o

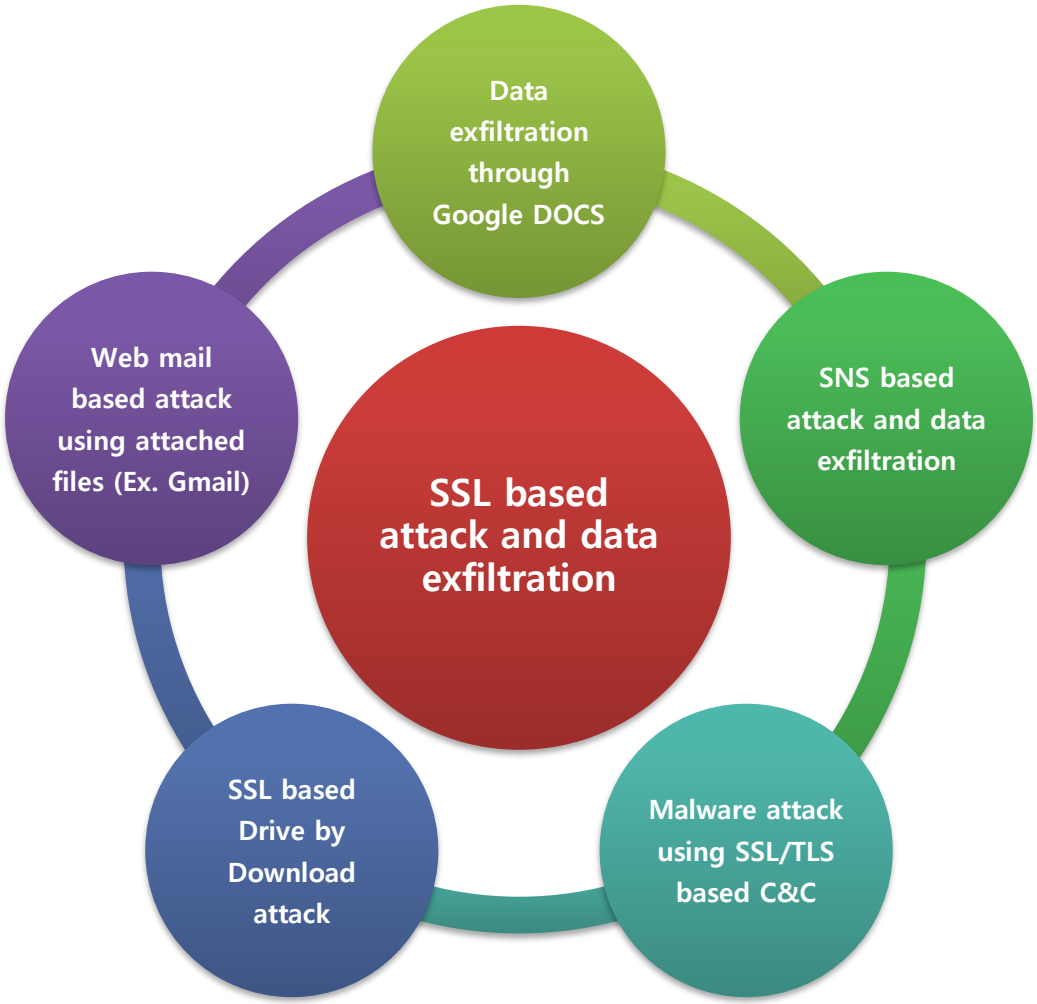
First Half of 2017,
SSL Traffic Analysis Brief Report

5. HTTPS Based Malware Collection Status



According to the statistics that show HTTPS based malware URL and that are provided by malwares.com or mangoscan.com, average fifteen thousand of new HTTPS based malwares are collected per month and ninety three thousand of new HTTPS based malwares were collected during the first half of 2017. From this, it is expected that the number of HTTPS based malwares will continuously bigger along with the increase of SSL traffic.

6. Types of SSL Based Attack and Data Exfiltration



ePrism SSL Visibility Device is available for various solutions:
If you use one of the followings, please think about adopting SSL decryption solutions.

- Firewalls
- Secure Web Gateways (SWG)
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM) platforms
- Data Loss Prevention (DLP) products
- Threat Prevention platforms
- Network Forensics and Web Monitoring tools

First Half of 2017,

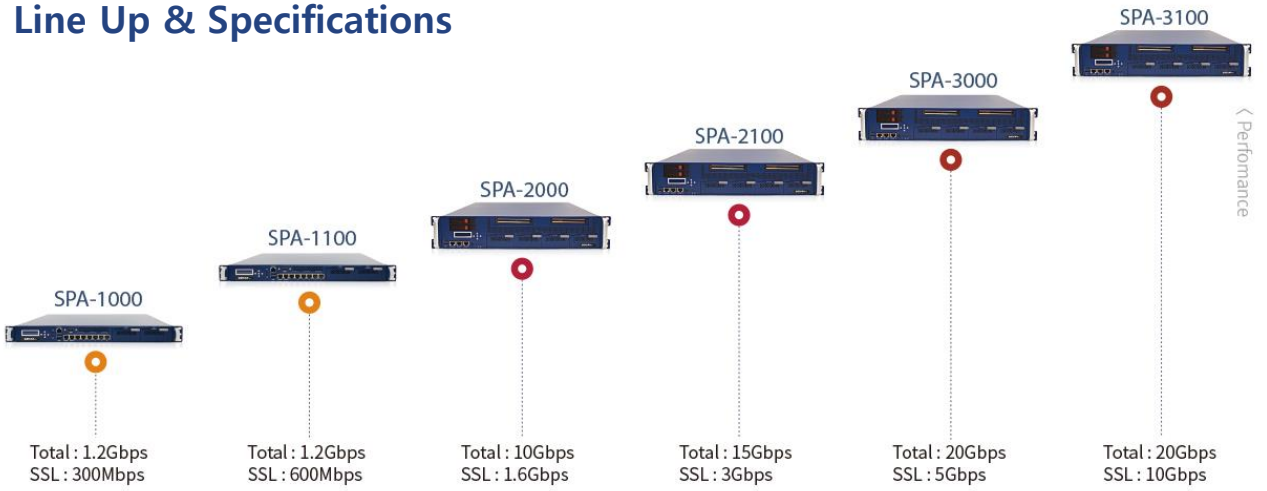
SSL Traffic Analysis Brief Report

- The statistics referred in this document sampled the customer companies by industry that were using eWalker Series (Secure Web Gateway Solution).
- The statistics regarding malicious code in this document is based on the information of malwares.com and mangoscan.com that provide malware DB to SOOSAN INT.
- The top 50 global websites for traffic in this document referred to the Alexa.com, an affiliated company of Amazon that announced top 500 global websites generating most traffic, September 11, 2017.

SOOSAN INT Co., Ltd.
3F, Suseo Hyundai Venture0ville, 10, Bamgogae-ro-gil,
Gangam, Seoul, Korea06349
Tel 02.541.0073 | **Fax** 02.541.0204 | **E-mail** gb@soosan.co.kr
Website: http://www.soosanint.com

SSL Visibility Solution,
ePrism SSL VA Lineup

Line Up & Specifications



	SPA-1000	SPA-1100	SPA-2000	SPA-2100	SPA-3000	SPA-3100
Performance						
Total Throughput	1.2Gbps	1.2Gbps	10Gbps	15Gbps	20Gbps	20Gbps
SSL Intercept Throughput	300Mbps	600Mbps	2Gbps	4Gbps	6Gbps	10Gbps
Number of SSL Session for New Handshake (CPS)	1,500/sec	2,500/sec	4,500/sec	6,000/sec	8,000/sec	21,000/sec
Number of SSL Flows (Concurrent process)	50,000	100,000	220,000	350,000	500,000	800,000
SSL Visibility						
Session Management Mapping	Supported	Supported	Supported	Supported	Supported	Supported
Traffic Analysis/Monitoring	Supported	Supported	Supported	Supported	Supported	Supported
Multi-dimensional Analysis & Report (Category/User/Time)	Supported	Supported	Supported	Supported	Supported	Supported
Certificate Publishing Tool	Supported	Supported	Supported	Supported	Supported	Supported
Filtering (*SSL/Non-SSL)						
Block malware based on DB/Bypass managment	Supported	Supported	Supported	Supported	Supported	Supported
Etc.						
Network Interface	Fixed 8 x 1Gbps Copper (Including 2 bypass pairs)		1X 4Port 1G/10G Fiber Bypass (SR) & 1X 4Port 1G/10G Fiber NIC (Configuration can be customized)			
Operation Mode	In-Line Mode (Hardware bypass available)					
SSL Management Transparency	Provide TCP transparency via Certification Resign (maintain 5-Tuple)					
Encryption Protocol	TLS 1.0, TLS 1.1, TLS 1.2, SSL v3					
Public Key Algorithm	RSA, DHE, ECDHE					
Symmetric Key Algorithm	AES, AES-GCM, 3DES, SEED, ARIA, CAMELLIA, DES, RC4					
Hash Algorithm	MD5, SHA-1, SHA-2					
RSA Key	512 to 8192 bits					