빛스캔(Bitscan)

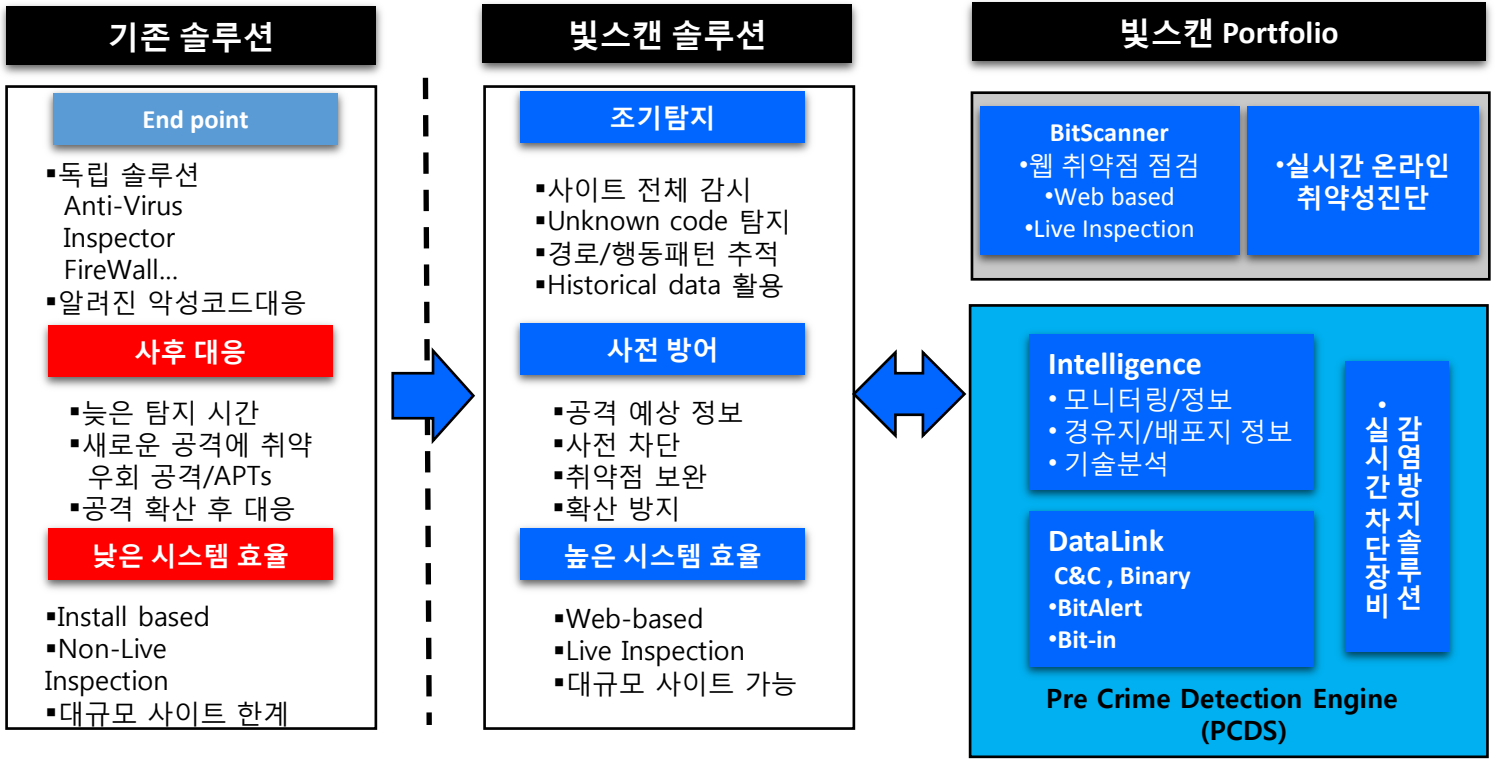
Web APT Proactive Malware Defense

2016.6.9.

빛스캔 주식회사
Bitscan Co.,Ltd. / www.bitscan.co.kr
(04789) 서울시 성동구 아차산로 17 L타워 지식산업센터 806호
T: 02 3486 7544 / F: 02 3486 7543 / info@bitscan.co.kr

빛스캔 Web Security Solution Overview

➢ 빛스캔 Web security solution은 '조기 탐지'와 '대응시간 Zero Time'이라는 기본 전략에 충실하게 구성



Bit-In Service : 감염기록 확인 서비스

➢ **개요** : 개인이 이용하는 인터넷 망에서 악성코드에 감염된 내역이 있는지 여부를 확인하는 서비스.
자신도 모르게 감염 되었던 내역 및 특정한 정보가 유출된 기록이 있는지 여부를 지속적으로 확인 가능.

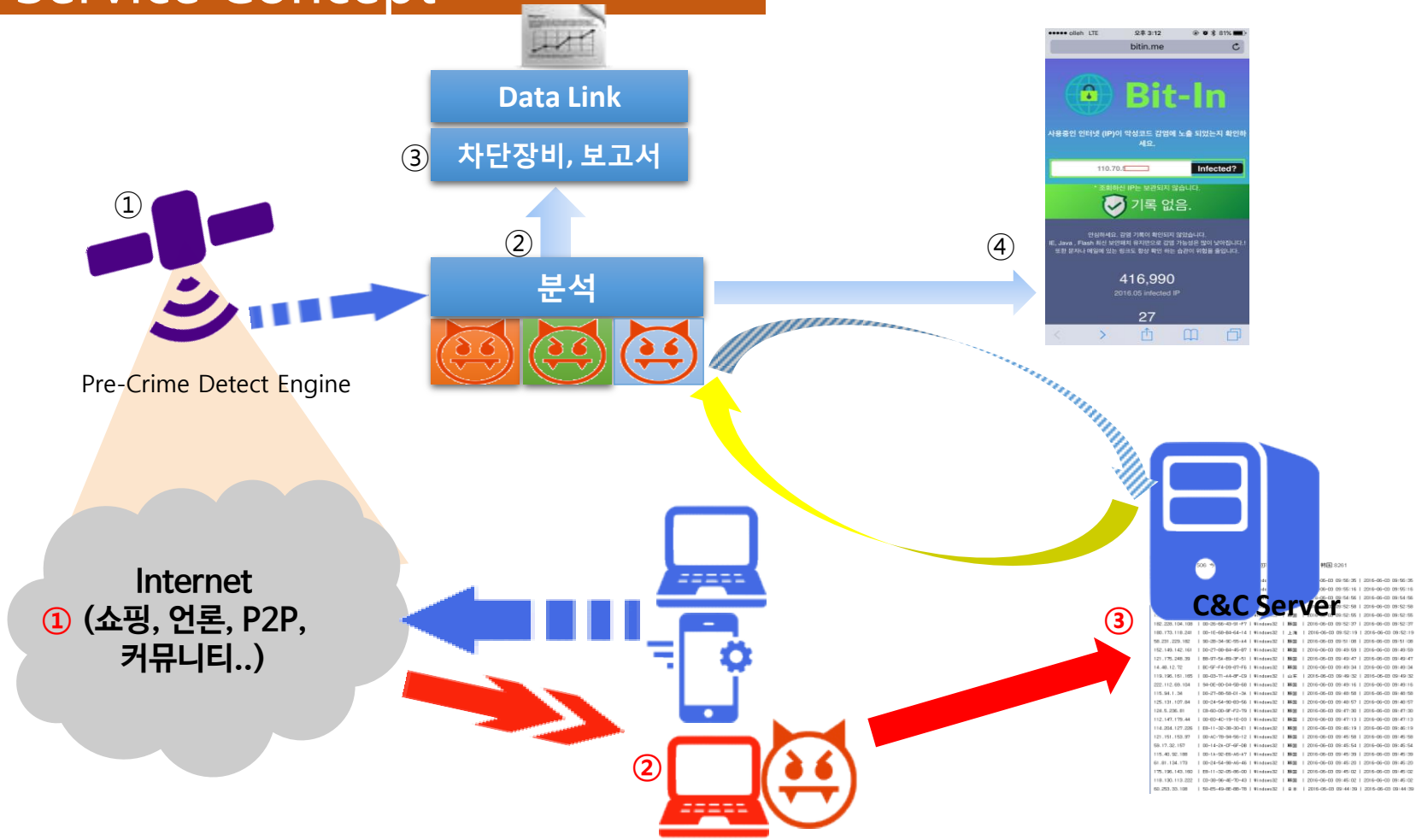
➢ **차별성**

1. 다년간 **Pre-Crime 엔진**을 통해 **수집, 분석, 추적**된 악성링크 정보와 바이너리 정보를 분석해서 나온 공격자의 수집 서버에서 확인.
2. 클릭 한번 만으로 감염 여부를 지속적으로 확인.
3. 실제 감염되었거나 유출 되었던, 감염 IP 정보를 지속적으로 업데이트 가능.
4. pc/mobile 을 이용한 WiFi 환경에서 공유기의 감염여부 확인 가능.

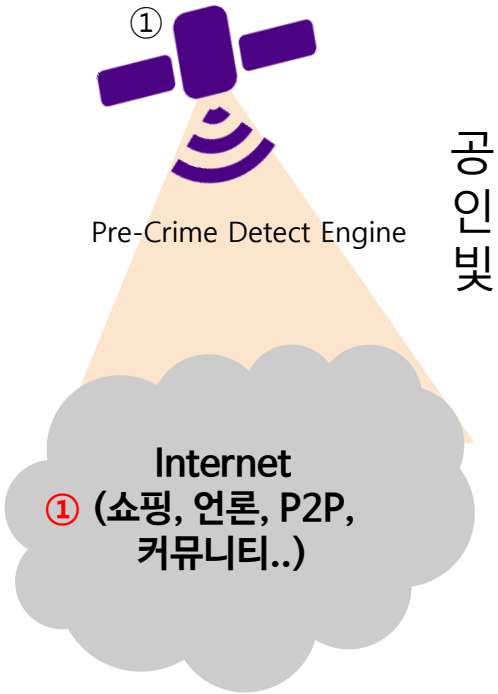
➢ **기대효과**

1. 공인적인 목적의 캠페인 가능 – 최신 업데이트 및 백신 검사 유도.
2. 개인정보 및 금융정보가 유출된 기록이 있는지 여부에 대해 확인 가능.
3. 내부 PC의 감염기록 여부를 확인 함으로써, 추가 위협에 대해서 대응가능.

Bit-In Service Concept

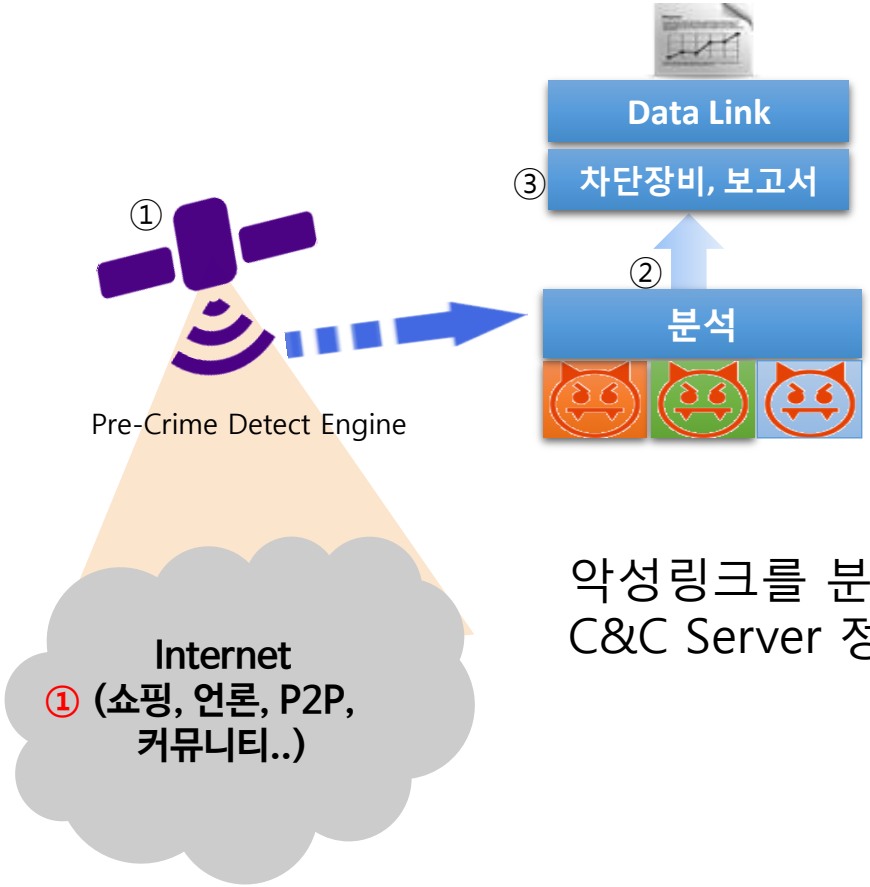


1. 악성링크 탐지



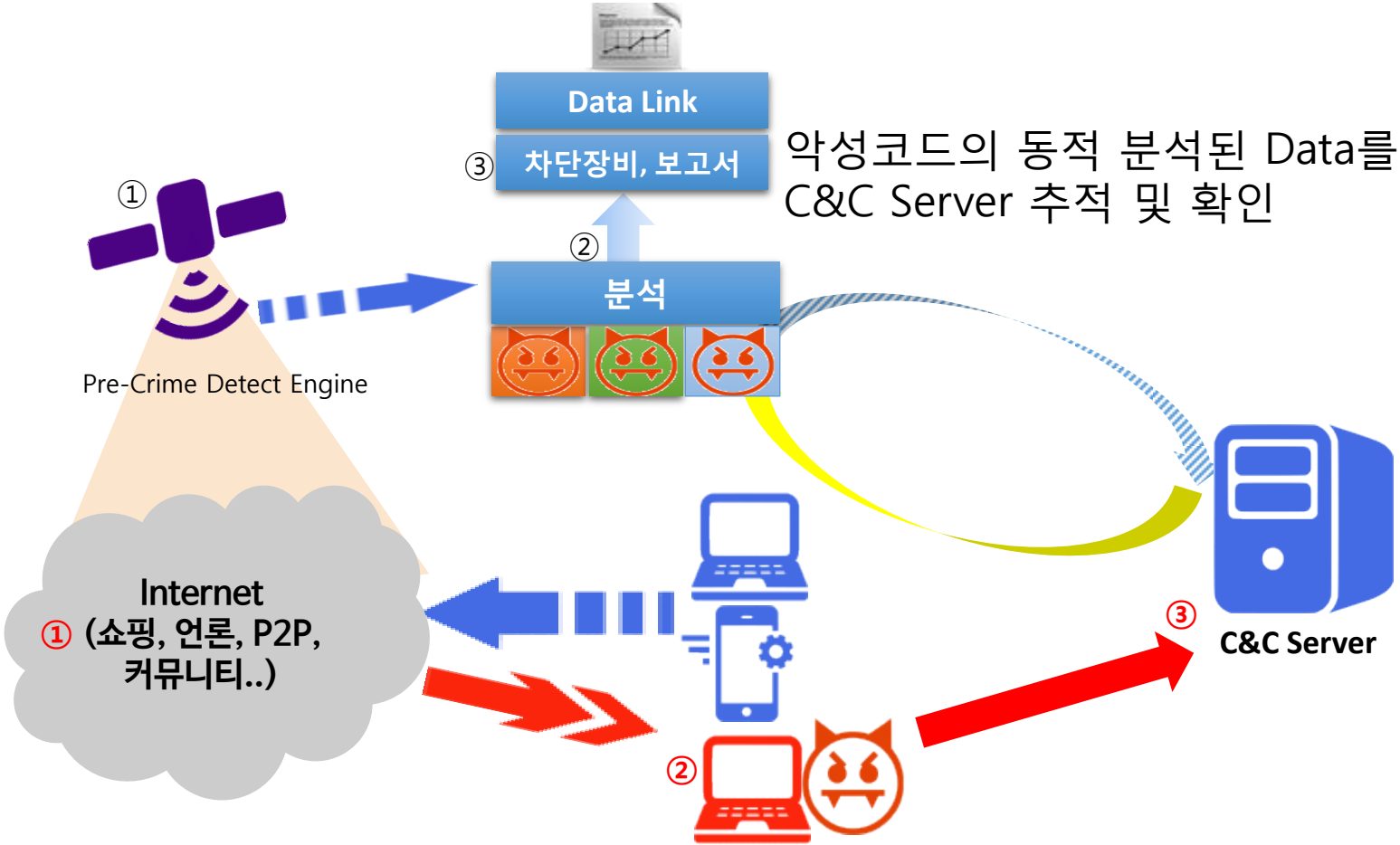
공격자는 방문자가 많은 웹 사이트에 **악성링크 삽입**
인터넷 서비스 모니터링(국내 210만개 / 국외 200만개)
빛스캔㈜ Pre-Crime Detect Engine이 **악성링크만 탐지**

2. 악성링크 분석 및 차단



악성링크를 분석 및 차단(20분내 완료)
C&C Server 정보 분석 및 추적

3. C&C Server 추적 및 확인



4. 감염된 PC 정보 확인

수집, 분석, 추적을 통하여 C&C Server에서
감염된 PC정보 확인(IP/Mac/OS/국가/날짜)

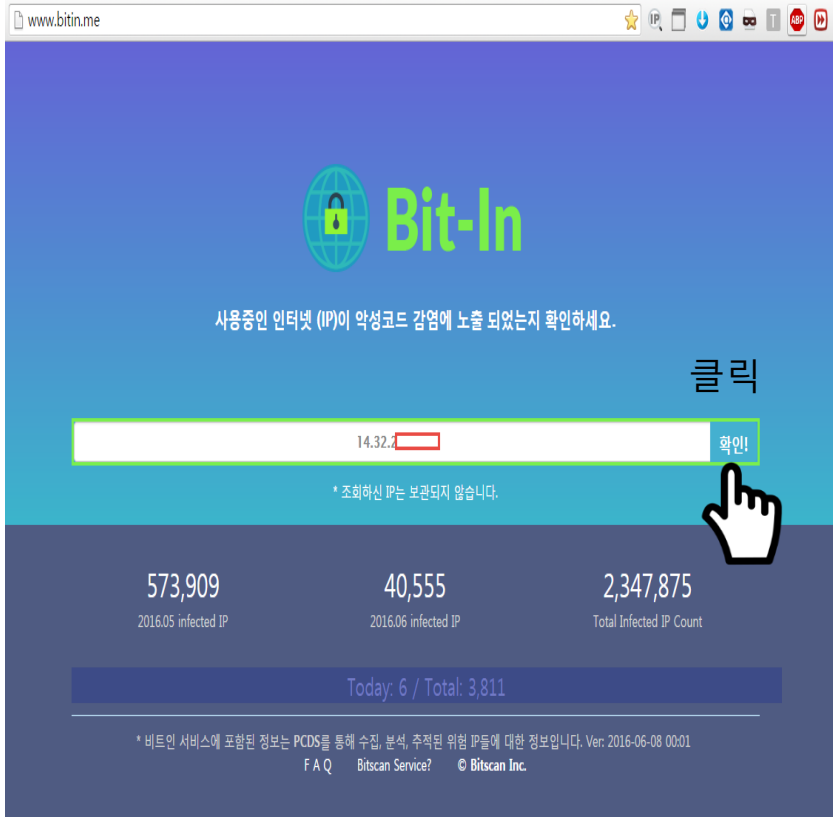
C&C Server

今日:13 昨日:47 今日回访:709 今日回率:0.85% 总数:83200 韩国:80090

180.[redacted]2.2	5C-AC-[redacted]CE-1F	Windows32	韩国	2016-05-31 11:04:18	2016-05-31 11:04:18
114.[redacted]239.4	00-0C-[redacted]83-68	Windows32	韩国	2016-05-31 09:30:08	2016-05-31 09:30:08
183.[redacted]10.18	48-5D-[redacted]AB-C6	Windows32	韩国	2016-05-31 08:44:44	2016-05-31 08:44:44
23.1[redacted]29.219	00-50-[redacted]0C-87	Windows32	北美	2016-05-31 08:28:17	2016-05-31 08:28:17
122.[redacted]4.141	24-B6-[redacted]0D-15	Windows32	韩国	2016-05-31 08:23:50	2016-05-31 08:23:50
143.[redacted]130.239	00-C0-[redacted]0D-0E	Windows32	美国	2016-05-31 08:06:28	2016-05-31 08:06:28
58.1[redacted]58.215	00-26-[redacted]58-50	Windows32	韩国	2016-05-31 08:02:27	2016-05-31 08:02:27
143.[redacted]130.15	00-C0-[redacted]0C-80	Windows32	美国	2016-05-31 07:14:59	2016-05-31 07:14:59
64.1[redacted]7.106	08-00-[redacted]79-3E	Windows32	美国	2016-05-31 06:46:10	2016-05-31 06:46:10
64.1[redacted]7.106	08-00-[redacted]35-72	Windows32	美国	2016-05-31 06:12:33	2016-05-31 06:12:33

5. 감염된 PC의 IP정보 암호화 저장

- pc/mobile에서 접속하면 자동으로 사용자의 IP 입력



- 한번 클릭만으로 감염 기록 확인

6. Bit-In Service : 기대효과

- **개인 및 기업 내부의 감염된 PC를 확인.**
  - 고객사의 경우 감염된 PC의 Mac address로 확인 및 조치 가능

- **회사에서 사용중인 공인 IP의 위험도 확인**
  - IP Reputation Management

- **개인 및 기업의 감염기록확인을 통한 발생 일시 확인**
  위험관리 - 모르면 사고가 발생되지만, 알게 되면 관리할 수 있는 위험이 된다.

- **공용 Wifi 사용시 위험성 체크 가능**
  감염기록 여부의 확인을 통해 앞으로 발생될 수 있는 문제를 줄이는데 도움

* 본 서비스는 유.무선 모든 환경에서 클릭 한번만으로 손쉽게 확인이 가능합니다.

- 안정적인 서비스를 제공하기 위해 **과다 접속** 시 IP가 차단될 수 있습니다.
- IP 제한 없는 조회를 원하시는 기업/기관에서는 info@bitscan.co.kr 로 연락 부탁 드립니다.
- 향후 Mobile App을 통해 차단과 감염 확인 서비스를 동시에 제공할 예정입니다.

Thanks

Beyond Inspiration!

info@bitscan.co.kr

빛스캔 주식회사

Bitscan Co.,Ltd. / www.bitscan.co.kr

(04789) 서울시 성동구 아차산로 17 L타워 지식산업센터 806호

T: 02 3486 7544 / F: 02 3486 7543 / info@bitscan.co.kr