NSHC

2014. 03. 05

악성코드 분석 보고서

[Internet Bank Pharming - BlackMoon]

인터넷 뱅킹 파밍용 악성코드가 지속적으로 배포되고 있습니다. 악성코드는 'DNS Cache' 조작 및 'hosts.ics'를 생성하여 사용자로 하여금 변조 웹 페이지로 접근을 유도합니다. 변조 웹 페이지는 실명정보, 계좌정보, 인터넷 뱅킹 계정정보, 보안카드 정보 입력을 유도하여 사용자 정보를 탈취합니다. 감염이 의심되는 시스템에서는 대응방안에 따른 조치와 백신을 통한 치료가 필요합니다.

Red Alert *Information Service about a new vulnerability*

Version 1.0 External

목 차

1. Malware Stub 3
1.1. Malware File Info 3
1.2. Route of infection 3
1.3. Analysis Environment 3
1.4. Drop Flow 3
1.5. IP Info 4
1.6. Infection 5
2. Technical Details 9
2.1. DNS Cache 9
2.2. Hosts.ics 11
3. Red Alert of Opinion 13
4. Removal Recommendations 13
4.1. Delete File 13
4.2. Registry Cleanup 13
4.3. Use of Anti-Virus 14
5. Reference 15

Confidentiality Agreements

본 문서는 Red Alert 팀에서 작성한 분석 보고서로써, Red Alert 팀 허가 없이 배포 및 공유가 가능하나 수정은 금합니다. 분석 보고서는 Red Alert 팀에서 운영하는 Facebook 페이지 (https://www.facebook.com/nshc.redalert)에서 확인할 수 있습니다.

Facebook 에 등록되는 분석 보고서를 포함한 이외의 자료들은 프리미엄 서비스인 isac 페이지 (https://isac.nshc.net)에서 제공 받으실 수 있습니다.

1. Malware Stub

1.1. Malware File Info

Malware Name	log.exe		
File Size	24,789 bytes	MD5	39985C35EA34E66101FD10A54D521F1D
Compiled Date	1987.09.11 01:35:02	Etc	FSG v2.0

Table 1. File Info-1

1.2. Route of infection

- http://**s.*****ldsms.com/sms***/log.exe

1.3. Analysis Environment

Index	Description
OS	Windows XP SP3 KR
Browser	Windows Internet Explorer 8

Table 2. Analysis Environment

1.4. Drop Flow

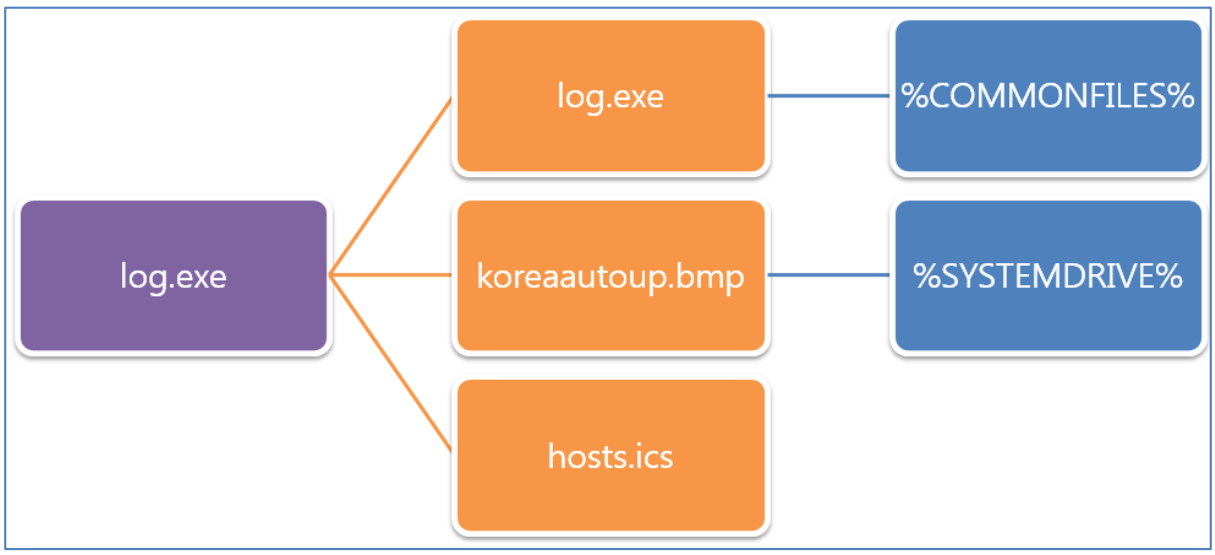

Figure 1. Drop Flow

1.5. IP Info

파밍 웹 서버 IP 정보입니다.

IP address:	[redacted]
hostname:	i223-219-38-180.s41.a013.ap.plala.or.jp
ISP:	NTT Plala Inc.
City:	Tokyo
Region:	Tokyo
Country:	Japan (JP)
latitude:	35.685
longitude:	139.7514

Figure 2. IP Info-1

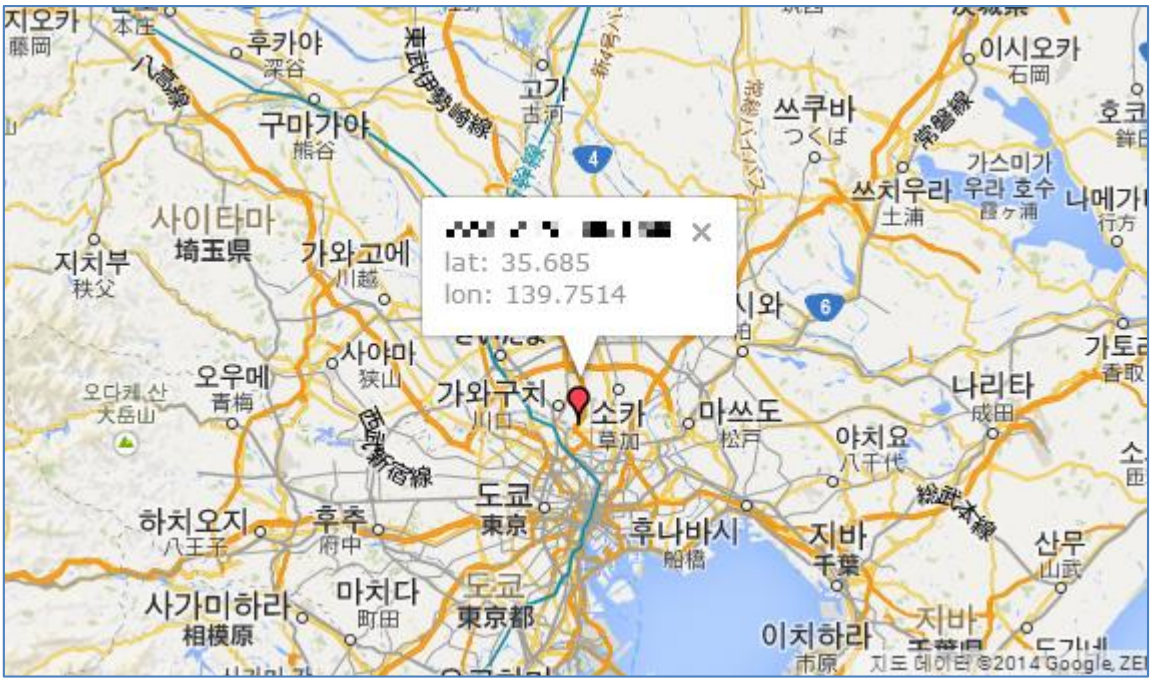

Figure 3. IP Info-2

1.6. Infection

악성코드가 시스템에 감염되면 'hosts' 파일이 변조되고 'hosts.ics' 파일이 생성됩니다.

- **%WINDIR%₩system32₩drivers₩etc₩hosts**
- **%WINDIR%₩system32₩drivers₩etc₩hosts.ics**

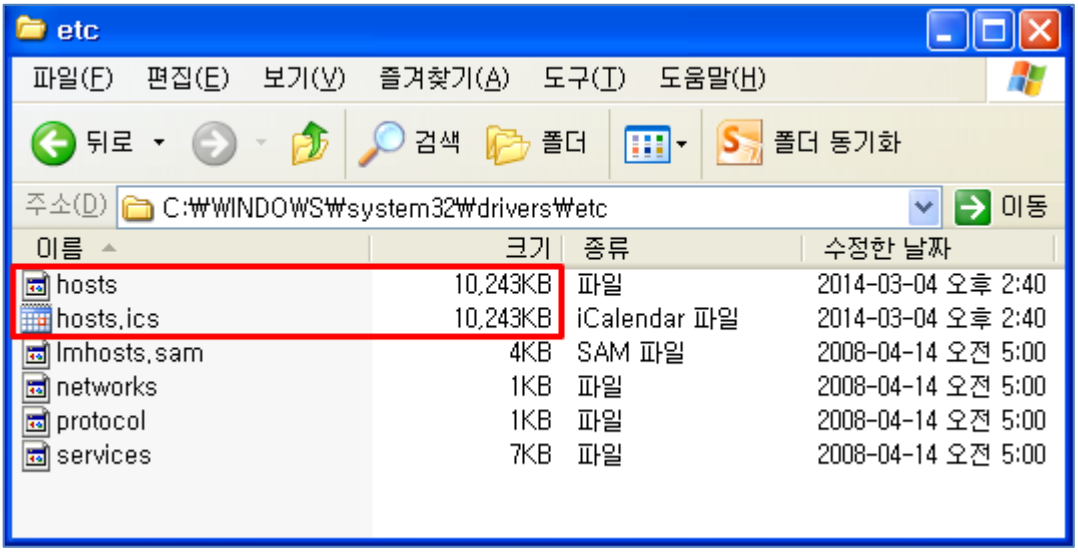

Figure 4. Infected Hosts File

특정 레지스트리 키 값을 변조하여 'Internet Explorer'의 시작 페이지를 변경시킵니다.

- **HKCU₩Software₩Microsoft₩Internet Explorer₩Main**
  - **Value Name : Start Page**
  - **Value Data : http://www.naver.com**

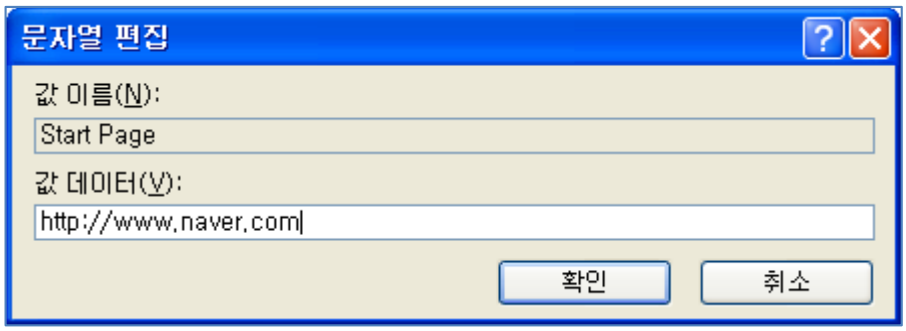

Figure 5. Modify Start Page-1

'Internet Explorer'를 실행시키면 공격자 서버의 변조된 시작 페이지에 접속됩니다.

Figure 6. Modify Start Page-2

변조된 페이지의 팝업을 통해 파밍용 인터넷 뱅킹 페이지에 접속을 유도합니다.

- **kIsA.kBstor.coM**
- **kIsA.Nenghuyp.coM**
- **kIsA.shiNhoN.coM**
- **kIsA.wooribenk.coM**
- **kIsA.idk.co.kR**
- **kIsA.epostbenk.go.kR**
- **kIsA.hoNabenk.coM**
- **kIsA.kcB.co.kR**
- **kIsA.kfoc.co.kR**

시작 페이지 및 각종 포털 사이트, 인터넷 뱅킹 사이트를 파밍하기 위해 'hosts.ics'에 기록된 'URL' 리스트입니다.

kBstar.coM
www.kBstar.coM
OpeN.kBstar.coM
omoNey.kBstar.coM
oBaNk.kBstar.coM
oBaNk1.kBstar.coM
Naver.coM
www.Naver.co.KR
Naver.cO.kR
NoNghyup.coM
www.NoNghyup.coM
BaNkiNg.NoNghyup.coM
iBz.NoNghyup.coM
www.Naver.coM
shiNhaN.coM
Naver.kR
www.Naver.Kr
kIsA.kBstor.coM
kIsA.Nenghuyp.coM
kIsA.shiNhoN.coM
kIsA.wooribenk.coM
kIsA.idk.co.kR
kIsA.epostbenk.go.kR
kIsA.hoNabenk.coM
kIsA.kcB.co.kR
kIsA.kfoc.co.kR
www.NaTe.nEt
www.NaTe.Kr
NaTe.kR
pharmiNg.kIsA.or.kR
www.shiNhaN.coM
BaNkiNg.shiNhaN.coM
BizBaNk.shiNhaN.coM
OpeN.shiNhaN.coM
daUm.NeT
iBk.co.kR

www.NaTe.cO.kr
NaTe.Co.Kr
www.iBk.co.kR
myBaNk.iBk.co.kR
kiup.iBk.co.kR
OpeN.iBk.co.kR
www.daum.NeT
wooriBaNk.coM
www.wooriBaNk.coM
piB.wooriBaNk.coM
u.wooriBaNk.coM
haNmail.NeT
keB.co.kR
www.keB.co.kR
eBaNk.keB.co.kR
oNliNe.keB.co.kR
OpeN.keB.co.kR
www.haNmail.Net
haNaBaNk.coM
www.haNaBaNk.coM
OpeN.haNaBaNk.coM
www.haNacBs.coM
kfCc.co.kR
www.kfcc.co.kR
iBs.kfcc.co.kR
epostBaNk.go.kR
www.epostBaNk.go.kR
nAtE.coM

Table 3. Hosts.ics URL List

2. Technical Details

2.1. DNS Cache

'DNS Cache'는 'DNS Server'에 'DNS Query'를 요청하기 전에 가장 먼저 참조되는 테이블입니다. 시스템 부팅 이후 발생한 'DNS Query'에서 획득한 'IP'정보를 캐시 메모리에 저장하여 이후 발생되는 같은 'DNS Query'요청에서 대해서는 캐시 메모리를 참조하게 됩니다.

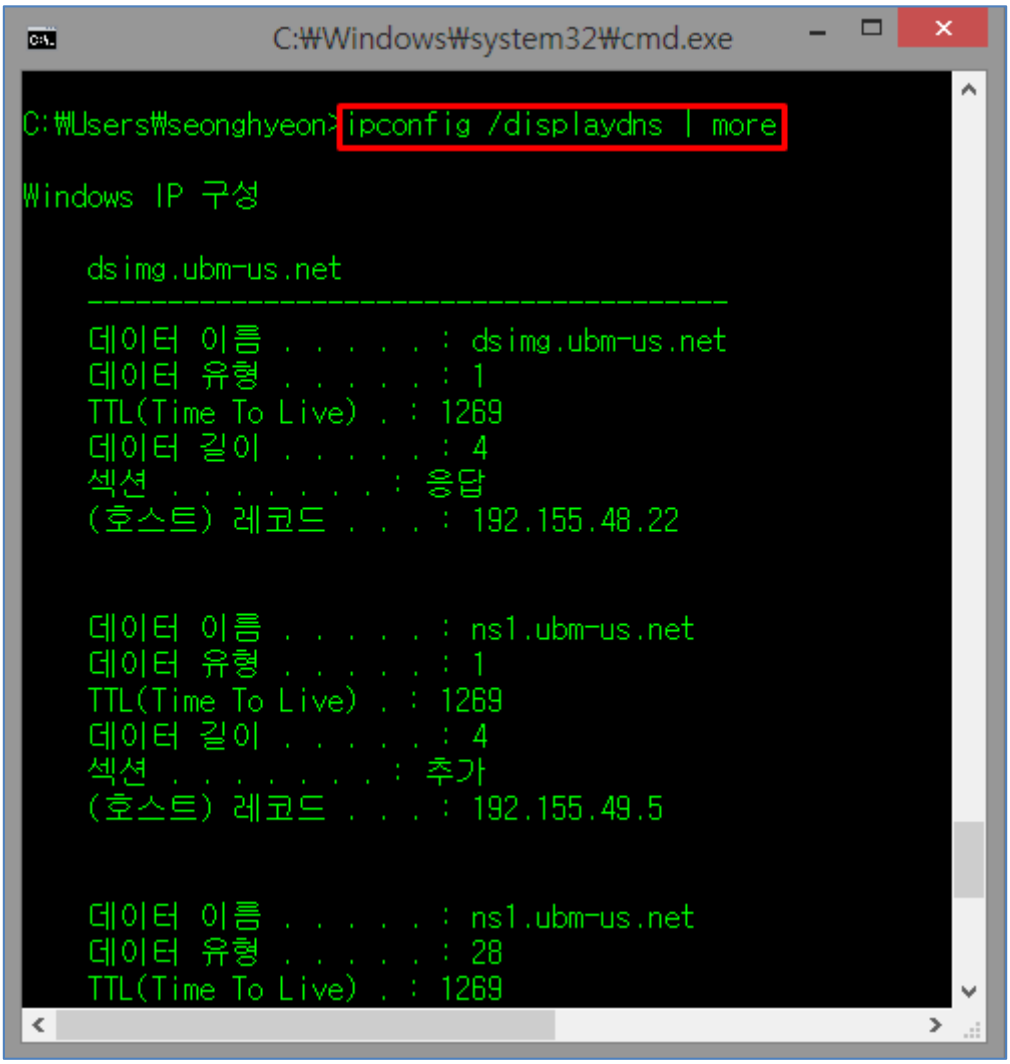

Figure 7. DNS Cache Table

이와 같이 'DNS Query'를 요청하기 전에 'IP'정보를 로컬 시스템에서 검색하며, 순서는 아래와 같습니다.

① **DNS Cache Memory**
② **Hosts.ics**
③ **Hosts**

악성코드는 'hosts.ics' 파일 생성과 'hosts' 파일을 변조하여 파밍 사이트 접속을 유도하기 때문에 'DNS Cache Memory'의 기능을 해제합니다. 'DNS Cache Memory' 기능 해제 관련 레지스트리 키는 아래와 같습니다.

- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : DnsCacheEnabled**
  - **Value Data : 0x00000000**
- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : DnsCacheTimeout**
  - **Value Data : 0x00000000**
- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : ServerInfoTimeOut**
  - **Value Data : 0x00000000**

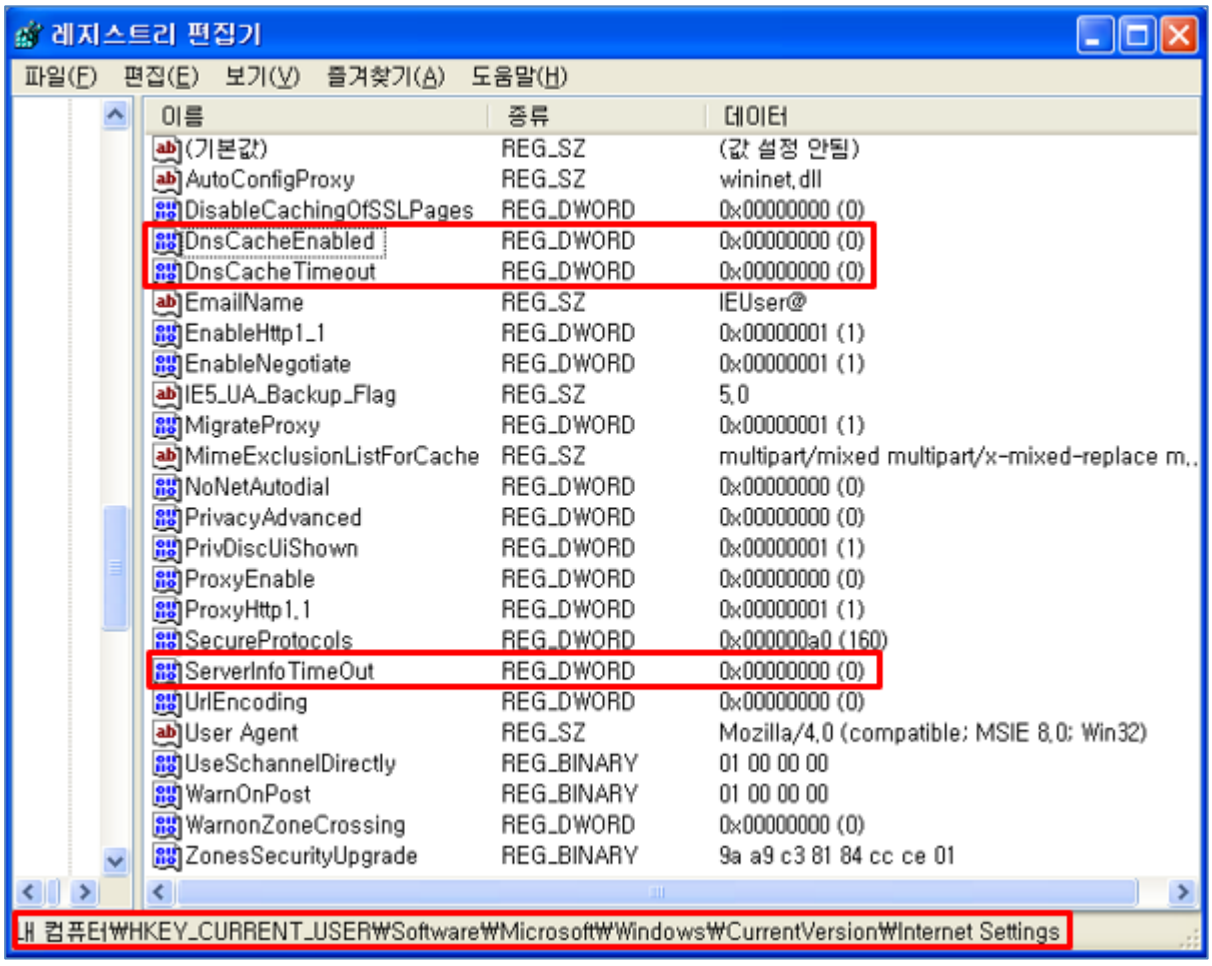

Figure 8. DNS Cache Registry

2.2. Hosts.ics

'Hosts.ics' 파일은 'DNS Query'를 요청하기 전에 도메인 테이블을 참조하는 파일 중에 하나이며, 해당 파일에 'DNS Query'를 요청할 도메인이 있을 경우 'DNS Query'는 발생하지 않습니다. 파밍 대상 도메인 정보는 악성코드 파일에서 확인할 수 있습니다.

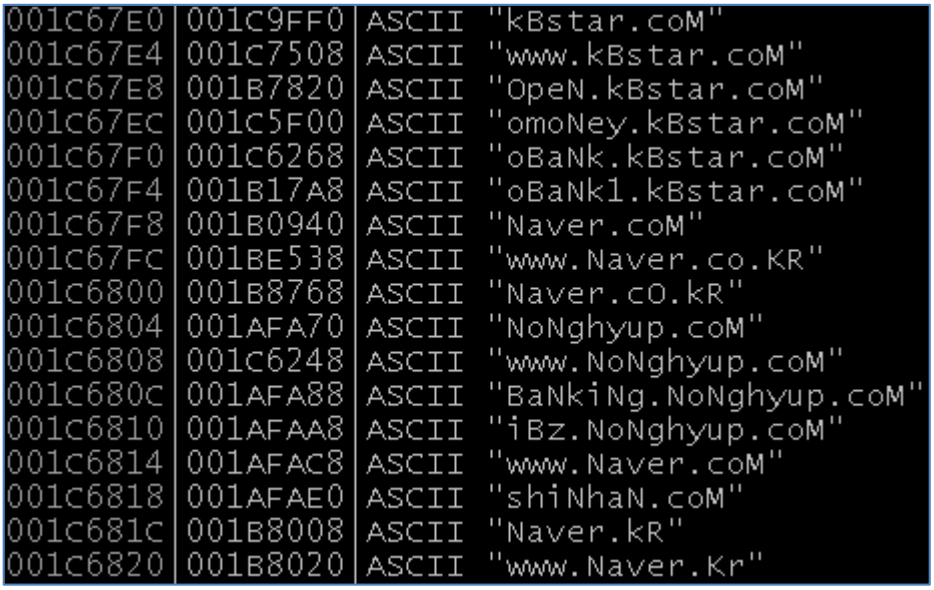

Figure 9. Domain List

도메인에 해당되는 'IP' 정보는 특정 페이지를 통해 동적으로 받아오게 됩니다.

- **http://user.qzone.qq.com/2011******

Figure 10. QQ Blog

해당 페이지의 소스코드를 파싱하여 파밍 페이지의 'IP' 정보를 획득합니다.

```
<script type="text/javascript">\r\n
    var profile_data = {\r\n
        avatar : 'http://qlogo3.store.qq.com/qzone/2011                    ',\r\n
        nickname : '#223.219                #'\r\n
    };\r\n
ed]             (function(){try{if(parent!=self && (parent.document.domain!=docum
</script>\r\n
```

Figure 11. Get Pharming IP Address

동적으로 'IP'를 받아오는 루틴은 타이머 프로시저로 동작하며, 360초 단위로 'IP' 정보를 갱신하게 됩니다.

```
CALL to SetTimer from Temporar.00409135
hWnd = NULL
TimerID = 0x0
Timeout = 360000. ms
Timerproc = Temporar.0040915F
```

Figure 12. Get Pharming IP Procedure

또한, 악성코드는 로컬 시스템의 'DNS Cache' 정보를 1초 마다 삭제하여 'hosts.ics' 파일을 통한 도메인 테이블 참조를 원활하게 합니다.

```
CALL DWORD PTR DS:[0x40D01C]    dnsapi.DnsFlushResolverCache
NOP
NOP
NOP
NOP
```

Figure 13. Flush DNS Cache

3. Red Alert of Opinion

인터넷 뱅킹 파밍에 관련된 악성코드가 지속적으로 배포되고 있습니다. 'IP'정보를 특정 페이지에서 동적으로 파싱하여 동작하는 것은 기존에 보고되었던 'Internet Bank Pharming with CVE-2013-3897'와 매우 유사한 형태를 가지고 있습니다. 파밍 페이지의 경우 일반 사용자들은 구분하기 어렵기 때문에 은행에서 제공하는 보안 정책(OTP, PC지정, SMS승인 등)을 이용하여 추가 인증을 하시기 바랍니다. 또한, 은행에서는 보안카드의 전체 일련번호와 전체 번호를 요구하지 않으니 유의하시기 바랍니다.

4. Removal Recommendations

4.1. Delete File

윈도우 탐색기의 폴더옵션에서 '보호된 운영 체제 파일 숨기기(권장)' 체크박스의 체크를 해제하시고 '숨김 파일 및 폴더 표시'의 라디오 버튼을 클릭하여 적용한 뒤 아래 경로의 파일을 삭제하시기 바립니다.

- **%WINDIR%₩system32₩drivers₩etc₩hosts.ics**
- **%TEMP%₩[RndFolder]₩TemporaryFile**
- **%COMMONFILES%₩log.exe**
- **C:₩koreaautoup.bmp**

4.2. Registry Cleanup

윈도우 레지스트리 편집기를 이용하여 악성코드 관련 레지스트리를 삭제합니다.

- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run**
  - **Value Name : koreaautoup**
  - **Value Data : C:₩Program Files₩Common Files₩log.exe**
- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : DnsCacheEnabled**
  - **Value Data : 0x00000000**
- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : DnsCacheTimeout**
  - **Value Data : 0x00000000**
- **HKCU₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings**
  - **Value Name : ServerInfoTimeOut**
  - **Value Data : 0x00000000**
- **HKCU₩SOFTWARE₩Microsoft₩Internet Explorer₩Main(Option)**
  - **Value Name : Start Page**
  - **Value Data : http://www.naver.com**

4.3. Use of Anti-Virus

'Reference. [1] Virus Total'을 참고하여 해당 악성코드를 치료할 수 있는 'Anti-Virus' 제품을 이용하여 시스템 정밀 검사를 진행하시기 바립니다.

5. Reference

[1] Virus Total
https://www.virustotal.com/en/file/bd863ab5da6b95ccf04e2d84173ae2c052dde11234f830b4659131f63f0286d8/analysis/

[2] Red Alert Report
https://www.facebook.com/photo.php?fbid=527477547329302&set=a.361893127221079.82385.345221158888276&type=1&theater