www.alyac.co.kr

피해갈 수 없는 탐지력

알약

월간 보안동향 보고서

ESTsoft

목차

Part Ⅰ 5 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 – "Castov 악성코드" 6

(1) 개요 6

(2) 행위 분석 6

(3) 결론 10

3. 허니팟/트래픽 분석 11

(1) 상위 Top 10 포트 11

(2) 상위 Top 5 포트 월별 추이 11

(3) 악성 트래픽 유입 추이 12

4. 스팸 메일 분석 13

(1) 일별 스팸 및 바이러스 통계 현황 13

(2) 월별 통계 현황 13

(3) 스팸 메일 내의 악성코드 현황 14

Part Ⅱ 보안 이슈 돋보기 15

1. 5 월의 보안 이슈 15

2. 5 월의 취약점 이슈 17

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 5월의 악성코드 통계

1. 악성코드 통계

(1) 감염 악성코드 Top 15

[2013년 05월 01일 ~ 2013년 05월 31일]

순위		악성코드 진단명	카테고리	합계 (감염자수)
1	New	Trojan.Dropper.OnlineGames.wsxp	Trojan	2,421
2	↑1	Trojan.Rootkit.killav	Spyware	2,345
3	↑1	Trojan.KillAV.sysdll	Trojan	2,245
4	New	Gen:Variant.Adware.Graftor.Elzob.19694	Etc	2,054
5	New	Gen:Trojan.Heur.SFC.mu3@a0WEtZabb	Trojan	1,973
6	New	DeepScan:Generic.PWS.WoW.784C1BFC	Etc	1,963
7	New	DeepScan:Generic.PWS.WoW.384BFE16	Etc	1,705
8	↑3	Spyware.OnlineGames.wsxp	Spyware	1,590
9	New	Gen:Variant.Kazy.125570	Etc	1,588
10	New	Gen:Trojan.Heur.PT.mmZ@aSYZPXo	Trojan	1,570
11	New	Gen:Trojan.Heur2.RP.fCXbaCV3gqfO	Trojan	1,519
12	New	Trojan.Heur.GM.1004030428	Trojan	1,514
13	New	Gen:Trojan.Heur.PT.mqZ@a4OTGYk	Trojan	1,423
14	New	Trojan.Heur.GM.1000030428	Trojan	1,391
15	↓14	Trojan.Dropper.OnlineGames.ver	Trojan	1,356

※ 자체 수집, 신고된 사용자의 감염통계를 합산하여 산출한 순위임

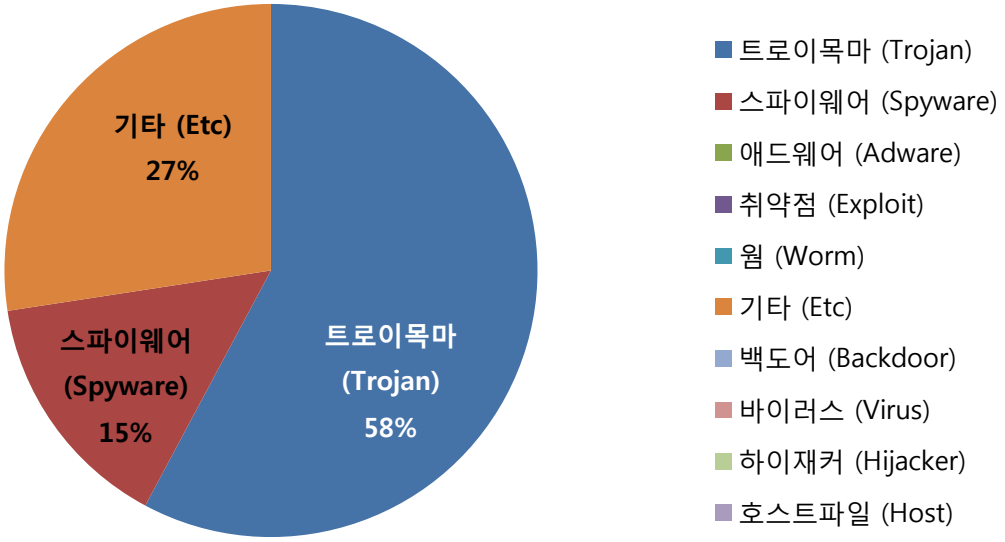
감염 악성코드 Top 15는 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

5월의 감염 악성코드 TOP 15에서는 지난달 순위권 밖이었던 Trojan.Dropper.OnlineGames.wsxp가 새롭게 1위를 차지하였습니다. 1위를 차지한 이 악성코드는 온라인게임 계정 탈취를 목적으로 하는 악성코드를 PC내에 드롭시키기 위한 트로이목마입니다. 아울러 4월 통계에서 1위를 차지했던 Trojan.Dropper.OnlineGames.ver가 14단계가 떨어진 15위를 차지했습니다.

2위와 3위는, 지난달 3위와 4위에서 한계단씩 상승한 Trojan.Rootkit.killav와 Trojan.KillAV.sysdll가 차지하였는데, 이들은 모두 Trojan형태로써 윈도우OS의 보안 취약점을 이용하여 윈도우 시스템 파일을 변조하여 이를 통해 백신 무력화를 시도하는 악성코드입니다. 1,2,3위를 차지한 악성코드 모두 온라인게임 계정 탈취를 위한 연계동작(침투, 시스템파일변조, 백신무력화, 정보탈취)과 관련 있으며, 이러한 악성코드들은 변조된 웹사이트를 통해 최초 유포되는 경우가 많으므로 항상 알약의 실시간감시기능을 활성화 시키고 신뢰할 수 있는 웹사이트만 방문하는 것이 안전합니다.

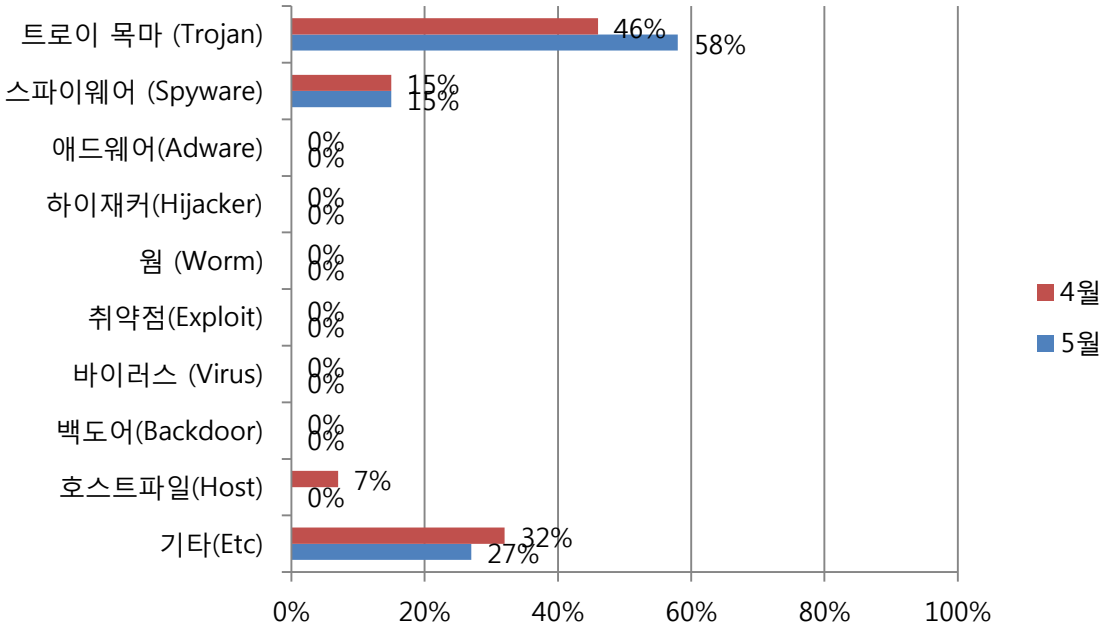
ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(2) 카테고리별 악성코드 유형



악성코드 유형별 비율에서 트로이목마(Trojan) 유형이 가장 많은 58%를 차지했으며, 기타(Etc) 유형이 27%로 2위를 차지했습니다. 스파이웨어(Spyware)유형의 경우 15%로 3위의 점유율을 보였습니다.

(3) 카테고리별 악성코드 비율 전월 비교

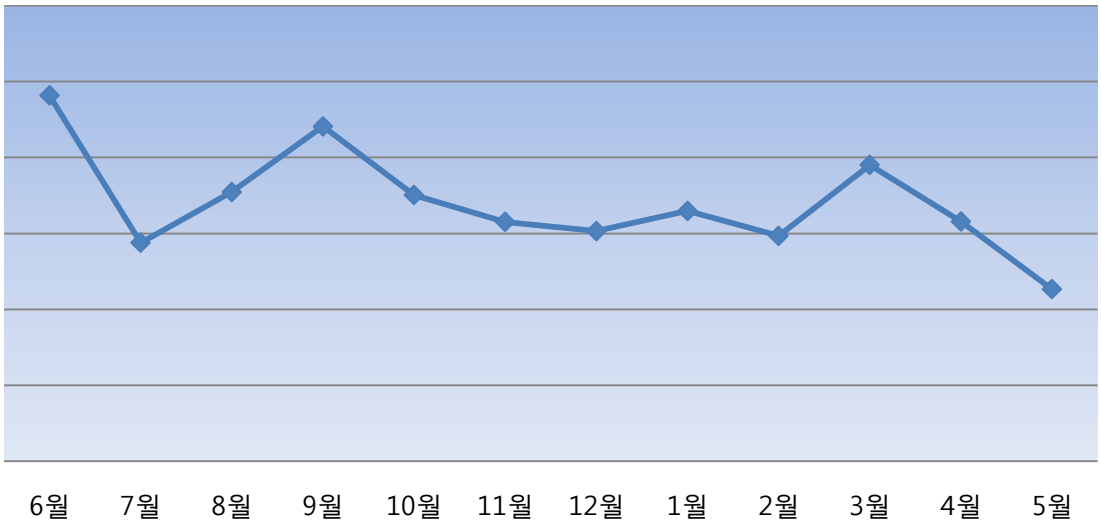


5월에는 지난 4월과 비교하여 트로이목마(Trojan)유형이 크게 증가하는 모습을 보였습니다. 스파이웨어(Spyware)유형은 지난달과 동일하며, 호스트파일(Host)유형과 기타(Etc)유형은 감소하였습니다. 전체적인 감염수치는 4월보다 5월이 전체적으로 대폭 감소하였습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(4) 월별 피해 신고 추이

[2012년 06월 ~ 2013년 05월]

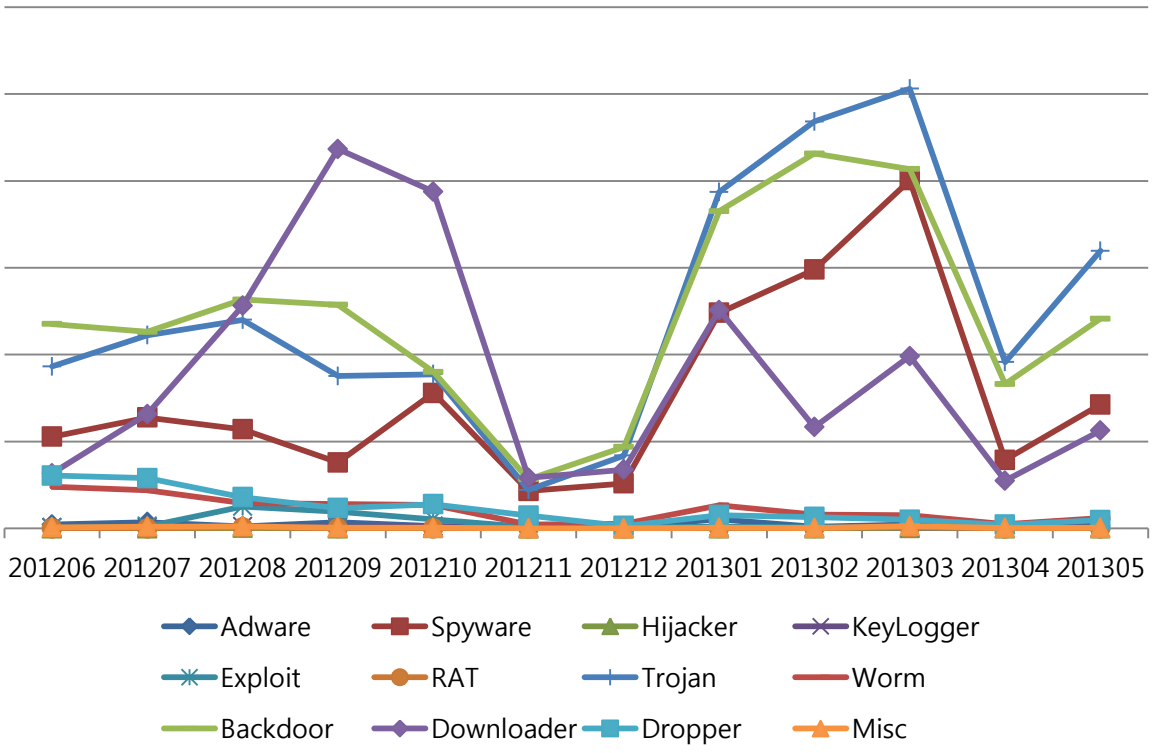


※ 알약 사용자의 신고를 합산에서 산출한 결과임

월별 피해 신고추이는 알약 사용자의 신고를 합산해서 산출한 결과로써, 월별 신고 건수를 나타내는 그래프입니다. 알약 2.0의 신고기능에 의해 접수된 피해 문의 신고는 4월은 3월에 비해 20% 정도 감소하였습니다.

(5) 월별 악성코드 DB 등록 추이

[2012년 06월 ~ 2013년 05월]

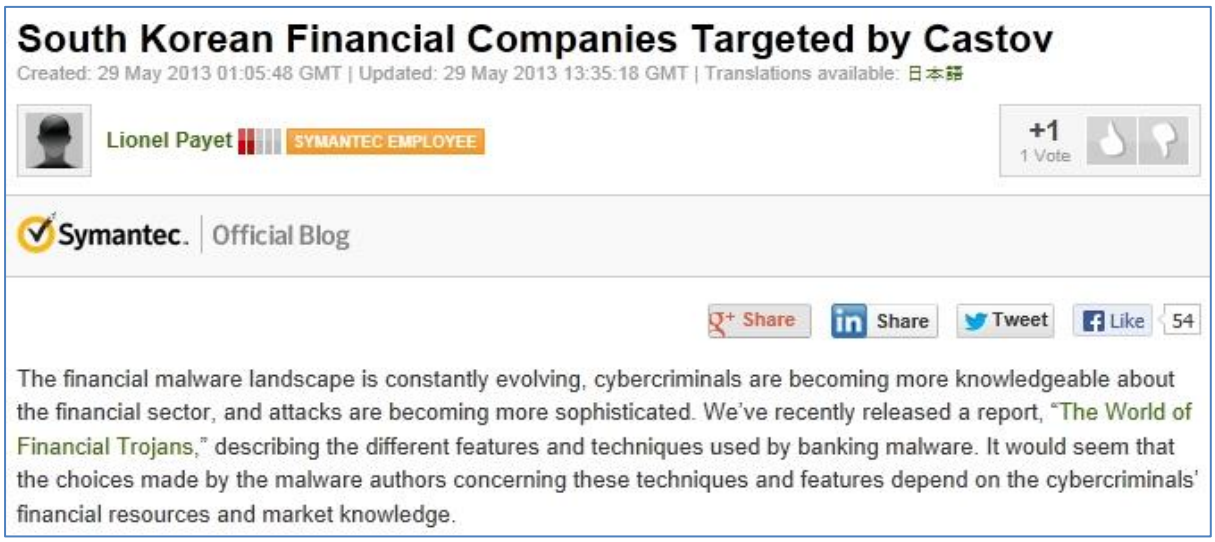


ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 5월의 악성코드 통계

2. 악성코드 이슈 분석 – "Castov 악성코드"

(1) 개요


South Korean Financial Companies Targeted by Castov

Created: 29 May 2013 01:05:48 GMT | Updated: 29 May 2013 13:35:18 GMT | Translations available: 日本語

Lionel Payet SYMANTEC EMPLOYEE

+1 1 Vote

Symantec. Official Blog

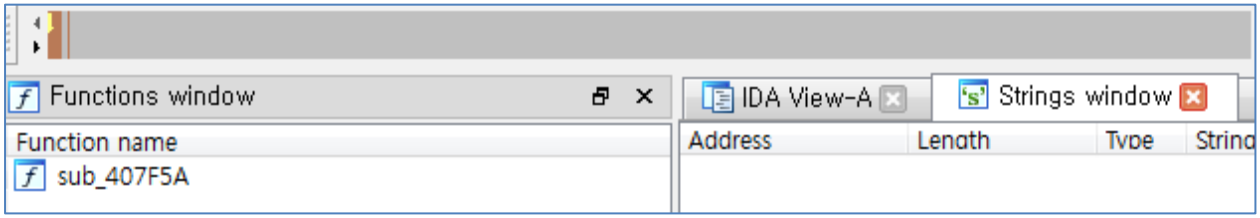
Share Share Tweet Like 54

The financial malware landscape is constantly evolving, cybercriminals are becoming more knowledgeable about the financial sector, and attacks are becoming more sophisticated. We've recently released a report, "The World of Financial Trojans," describing the different features and techniques used by banking malware. It would seem that the choices made by the malware authors concerning these techniques and features depend on the cybercriminals' financial resources and market knowledge.

CASTOV는 SYMANTEC에서 말하길 국내 금융 회사들을 타겟으로 한 Banking malware라고 공개했다. 프로세스명이 svohcst.exe인 것을 추적해 보면 이와 같은 공격방식은 5월부터 본격 유포된 것으로 보인다. 블로그 내용에 따르면 흥미롭게도 Online banking software and security DLLs에 후킹을 시도한다고 하여 분석해 보았다.

(2) 행위 분석

먼저 이 코드는 난독화가 잘 되어있다. 두세 번의 메모리 할당과 복호화를 통해 원래 코드를 찾을 수 있다.



이 샘플은 주말간 취약한 웹사이트를 통해 유포가 되었던 것으로, 배포 방식 또한 툴을 사용하여 계속적으로 해쉬값을 변경하도록 했다. 이것은 난독화 + 해쉬 변경의 조합으로 최대한 시그니처 탐지를 회피, 생존성을 높이려 했다는 것을 추측해 볼 수 있다.

복호화 이후 자신을 "svohcst.exe" 숨김 속성으로 재실행 한다. 그리고 다음과 같이 프로세스 중에 Anti AV 제품의 프로세스 이름을 찾아 **'SetTcpEntry'** 함수를 호출한다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

```
  v9 = v0;
  v0 = &v9;
  v8 = &v20;
  v7 = 1940008;
  v6 = v0;
  v0 = &v6;
  sub_1D8CF0(&v19, 0);
  for ( i = 0; !*(_BYTE *)(v19 + 28 * i); ++i )
  {
    sub_1D3890(
      &v18,
      "MUpdate2.exe|mautoup.exe|restoreu.exe|mupdate2.exe|v3light.exe|v3lsvc.exe|aflogvw.e
    sub_1D5D9C(v18, &v17);
    v4 = v17;
    Search_Process(*(_DWORD *)(v19 + 28 * i + 24), &v15);
    sub_1D5D9C(v15, &v16);
    if ( sub_1D3CB8(v16, v4) > 0 )
      Call_SetTcpEntry(v19 + 28 * i);
  }
  v0 = v9;
  v11 = 1940066;
  sub_1D381C(&v15, 4);
  return sub_1D450C(&v19, off_1D8C9C);
}
```

Anti AV code

MUpdate2.exe|mautoup.exe|restoreu.exe|mupdate2.exe|v3light.exe|v3lsvc.exe|aflogvw.exe|afquavw.exe|v3lexec.exe|wsctsk.exe|setup_v3rcv.exe|v3lrun.exe|v3ltray.exe|v3medic.exe|v3restore.exe|afquavw.exe|restore.exe|afquavw.exe|btscan.exe|ahnrpt.exe|restoreu.exe|AFLogVw.exe|AhnAzExE.exe|V3LExec.exe|V3Light.exe|V3LNetDn.exe|V3LRun.exe|WscTsk.exe|AKDVE.exe|V3Medic.exe|V3LAxAgn.exe|ahnrpt.exe|V3LTray.exe|AFQuaVw.exe|V3LSvc.exe|setup_v3rcv.exe|MAutoup.exe|MUpdate2.exe|mautoup.exe|restoreu.exe|mupdate2.exe|sgdnldr.exe|sgrun64.exe|sgui.exe|sgrun.exe|sgsvc.exe|v3restore.exe|afquavw.exe|restore.exe|restoreu.exe|ahnrpt.exe|Sgui.exe|SgRun64.exe|SgDnldr.exe|SgSvc.exe|SgRun.exe|ALUpdate.exe|ALUpExt.exe|ALUpProduct.exe|ALYac.aye|AYAgent.aye|AYCon.exe|AYHost.aye|AYLaunch.exe|AYPatch.aye|AYRTSrv.aye|AYRunSC.exe|AYShell.aye|AYTask.aye|AYUpdate.aye|AYUpdSrv.aye|ESTCM.exe|bootalyac.exe|NaverAgent.exe|Uninst_Agent.exe|NaverCommonUpdater_1_0_0_4.exe|NELO_CrashReporter.exe|RemoveUpdater.exe|NaverSafeGuard.exe|NELO_CrashReporter.exe);

AV process list

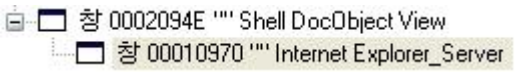
찾아본 바로는 xp이하에서 update를 방해하기 위한 코드로 보인다. (vista 이상은 권한이 있어야 실행된다고 하나 따로 확인하지 않음)

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

```
v8 = j_InternetOpenA("loadMM", 0, 0, 0, 0, v16, &unk_1DA552, &v29, v17, &sub_1DA58B, &v29, v18, v19, v20);
sub_1DA1D8(v23, &v22);
sub_1D3C6C(v22);
v4 = j_InternetOpenUrlA(v8);
v7 = v4;
if ( v4 )
{
  v25 = j_VirtualAlloc(0, 681984, 4096, 64);
  v9 = v25;
  do
  {
    v15 = &v26;
    v14 = (int)v28;
    v4 = j_InternetReadFile(v7);
    v5 = v26;
    if ( v26 > 0 )
```

Download Encrypted Data

이후 특정 사이트로 접속하여 암호화된 DATA를 읽어오고 해당 데이터를 다시 메모리상에서 복호화한다. 읽어오는 DATA는 IE Injection Routine과 Injection시 실행되는 코드로 구성되어있다. IE Injection은 "GetClassNameA" API를 활용, "Internet Explorer_Server" 인 ClassName을 찾아 PID를 얻어 Injection한다.



Injection이 완료되면 다음과 같이 "**INIdirectbankUI60.dll**", "**BankPayEFT.ocx**", "**ssa_LG_UPLUS.dll**"를 타겟으로 한 스레드가 반복해서 돌게 된다. 모두 전자 결제 관련 모듈들로 IE와 ActiveX로 구동되는 환경이다.

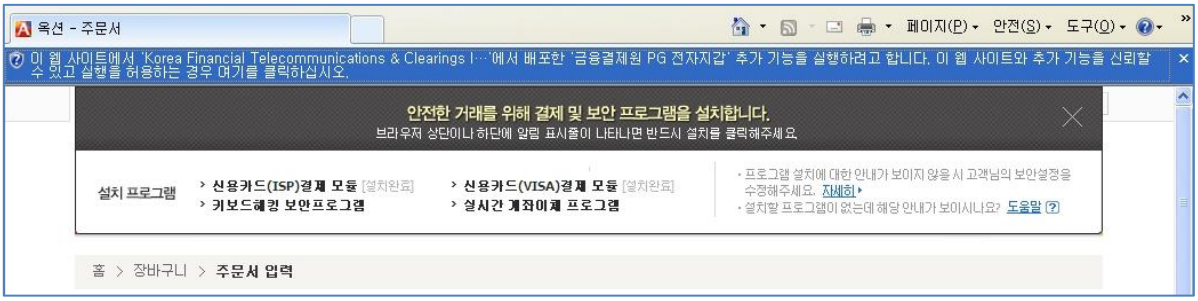
```
10431DE6 8D 45 FC      lea     eax, [ebp+var_4]
10431DE9 50            push    eax
10431DEA 6A 00         push    0
10431DEC 6A 00         push    0
10431DEE 68 C4 1D+     push    offset loc_10431DC4 ; INIdirectbankUI60.dll
10431DF3 6A 00         push    0
10431DF5 6A 00         push    0
10431DF7 E8 14 40+     call    j_CreateThread
10431DFC 8D 45 FC      lea     eax, [ebp+var_4]
10431DFF 50            push    eax
10431E00 6A 00         push    0
10431E02 6A 00         push    0
10431E04 68 CC 1D+     push    offset loc_10431DCC ; BankPayEFT.ocx
10431E09 6A 00         push    0
10431E0B 6A 00         push    0
10431E0D E8 FE 3F+     call    j_CreateThread
10431E12 8D 45 FC      lea     eax, [ebp+var_4]
10431E15 50            push    eax
10431E16 6A 00         push    0
10431E18 6A 00         push    0
10431E1A 68 D4 1D+     push    offset loc_10431DD4 ; ssa_LG_UPLUS.dll
10431E1F 6A 00         push    0
10431E21 6A 00         push    0
10431E23 E8 E8 3F+     call    j_CreateThread
```

Hooking Code

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

INIdirectbankUI60.dll – 이니시스 전자결제 모듈
BankPayEFT.ocx – 금융결제원 전자결제 모듈
ssa_LG_UPLUS.dll – 펜타시큐리티시스템 전자결제 모듈

이중 많이 사용하는 BankPayEFT.ocx 모듈은 국내 대표적인 온라인 쇼핑몰 옥션(auction) 사이트에서도 주문시 요구하는 결제 모듈로 실제 테스트 진행 후 모듈의 특정 주소 코드가 변경되는 것을 확인하였다.



Screenshot – "Auction" site

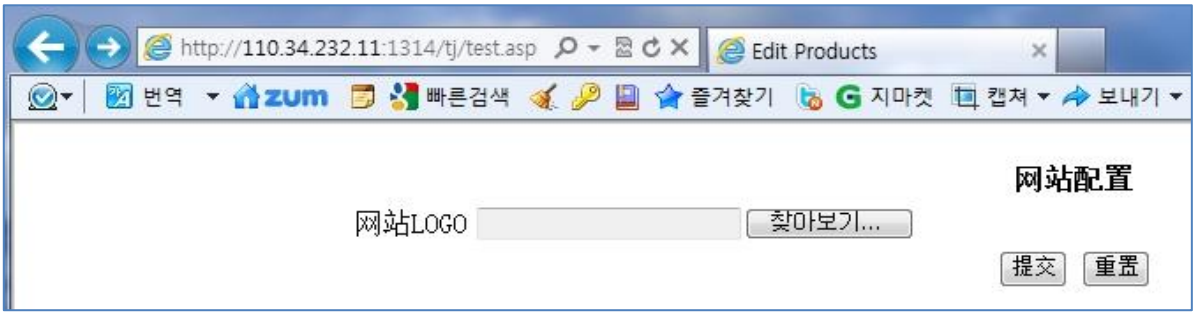
BankPayEFT.ocx 모듈이 IE에 로드되면 스레드는 이를 탐지하고 이어서 "y7csel.dll"의 모듈 핸들을 얻어 "cs_get_pwd"라는 함수 주소를 찾아 +33 offset의 주소를 변경(후킹)한다.

```
0C45A553    8B40 0C         MOV EAX,DWORD PTR DS:[EAX+C]
0C45A556    894A 04         MOV DWORD PTR DS:[EDX+4],ECX
0C45A559    83C4 08         ADD ESP,8
0C45A55C    C3              RETN
0C45A55D    90              NOP
0C45A55E    90              NOP
0C45A55F    90              NOP
0C45A560    83EC 08         SUB ESP,8
0C45A563    E8 17E40400     CALL y7csel.0C4A897F
0C45A568    50              PUSH EAX
0C45A569    8D4C24 04       LEA ECX,DWORD PTR SS:[ESP+4]
0C45A56D    E8 82E20400     CALL <JMP.&MFC42.#6467>
0C45A572    8B4424 0C       MOV EAX,DWORD PTR SS:[ESP+C]
0C45A576    85C0            TEST EAX,EAX
0C45A553  - E9 20650504     JMP 104B0A78
0C45A558    04 83           ADD AL,83
0C45A55A    C408            LES ECX,FWORD PTR DS:[EAX]      Modifica
0C45A55C    C3              RETN
0C45A55D    90              NOP
0C45A55E    90              NOP
0C45A55F    90              NOP
0C45A560    83EC 08         SUB ESP,8
0C45A563    E8 17E40400     CALL y7csel.0C4A897F
0C45A568    50              PUSH EAX
0C45A569    8D4C24 04       LEA ECX,DWORD PTR SS:[ESP+4]
0C45A56D    E8 82E20400     CALL <JMP.&MFC42.#6467>
0C45A572    8B4424 0C       MOV EAX,DWORD PTR SS:[ESP+C]
0C45A576    85C0            TEST EAX,EAX
```

Module Hooking

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

후킹(hooking)된 주소를 따라가게 되면 전자인증서, 패스워드, 스크린샷 등 수집된 정보를 압축파일로 생성하여 특정 웹 서버로 POST 전송 하는 코드를 확인 할 수 있다.



Remote Server Site

각각의 전자 결제 모듈 별로 후킹 함수를 정리하면 다음과 같다.
INIdirectbankUI60.dll –> inicore_v2.3.16.dll -> ICL_COM_Check_Password
BankPayEFT.ocx –> y7csel.dll -> cs_get_pwd
ssa_LG_UPLUS.dll –> BG_SSACnK_Load

정확한 주소를 찾아서 후킹하는 것을 보면 크래커에 의한 상당한 분석작업이 이루어 졌음을 추측할 수 있다. 따라서 앞으로 더 다양한 환경과 모듈들을 추가하여 다시 악성코드를 배포할 것이라 예측해 본다.

(3) 결론

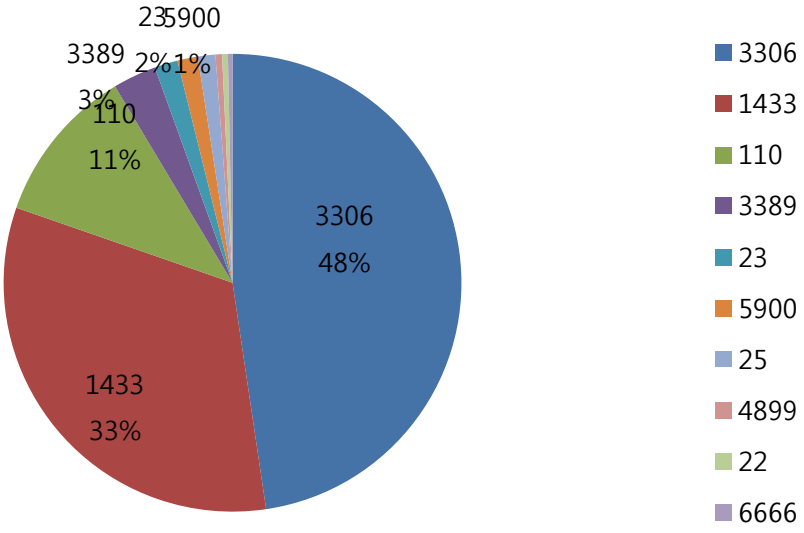
전자결제 모듈이 후킹되어 개인정보 수집에 이용된다는 것은 그 많큼 안전하지 않다는 것을 의미하므로 모듈 개발에 좀 더 보안조치가 이루어져야 할 것이며, 백신 또한 메모리 검사 및 행위 탐지 등 여러 방법을 통해 시그니처 탐지의 한계를 보완해야 할 것 같다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 5월의 악성코드 통계

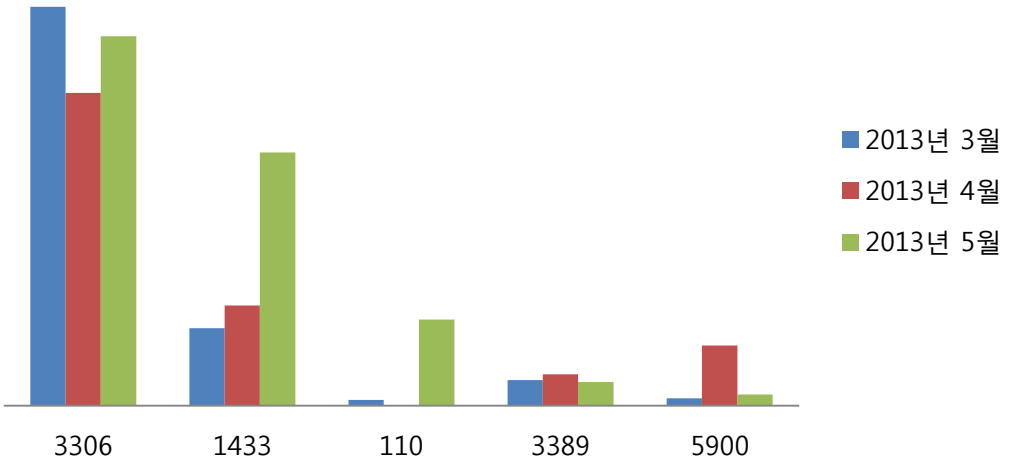
3. 허니팟/트래픽 분석

(1) 상위 Top 10 포트



(2) 상위 Top 5 포트 월별 추이

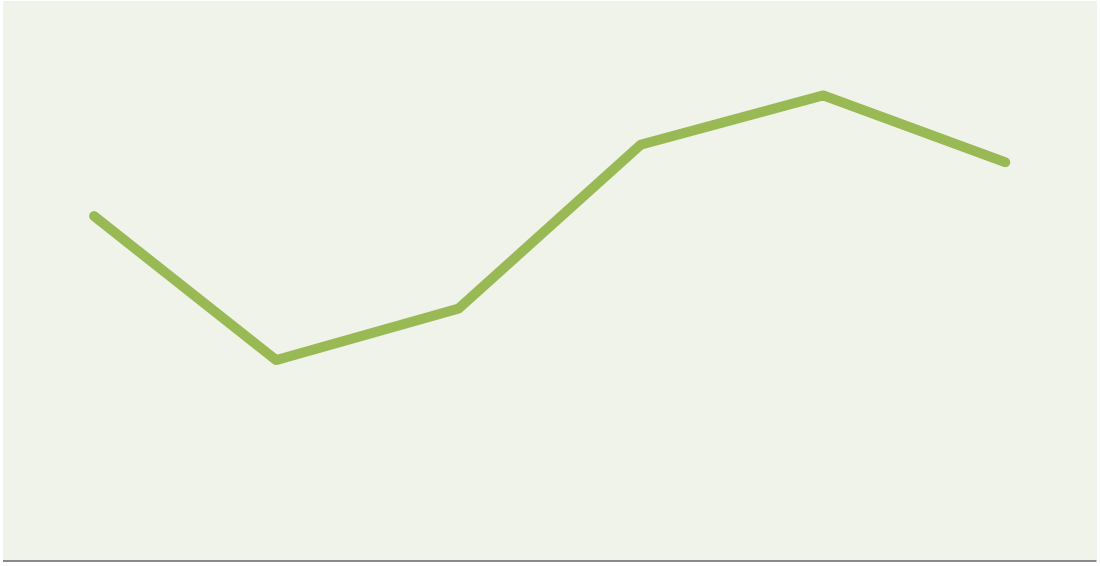
[2013년 03월 ~ 2013년 05월]



ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(3) 악성 트래픽 유입 추이

[2012년 12월 ~ 2013년 05월]



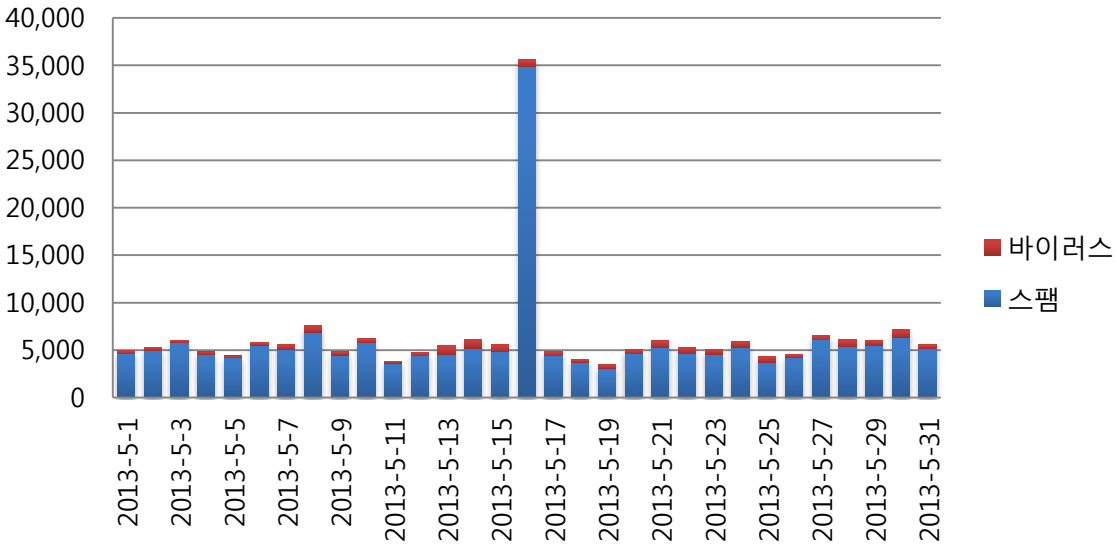
2012년 12월 2013년 1월 2013년 2월 2013년 3월 2013년 4월 2013년 5월

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅰ 5월의 악성코드 통계

4. 스팸 메일 분석

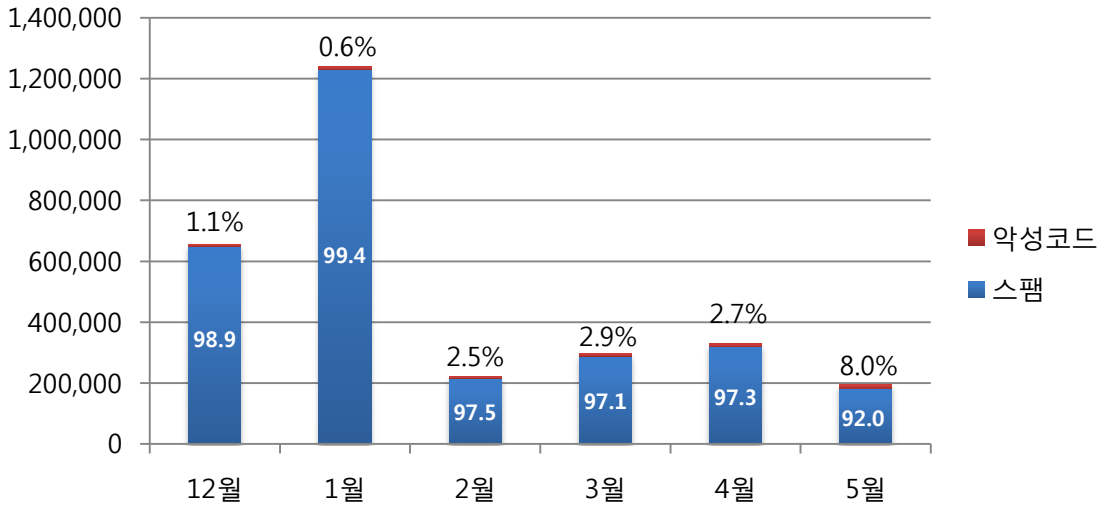
(1) 일별 스팸 및 바이러스 통계 현황



일별 스팸 및 바이러스 통계 현황 그래프는 하루에 유입되는 바이러스 및 스팸 메일의 개수를 나타내는 그래프입니다. 5월의 경우 4월에 비해 스팸메일수의 수치는 40% 넘게 감소했으나 오히려 해당 스팸메일에 포함되어 있는 바이러스의 수치는 2배가량 증가하였습니다.

(2) 월별 통계 현황

[2012년 12월 ~ 2013년 05월]



월별 통계 현황은 전체 악성메일 중 단순 스팸메일과 악성코드 첨부메일의 각 비율을 나타내는 그래프입니다. 5월에는 스팸 메일이 92.0%, 악성코드 첨부메일이 8.0%의 비율로 수신된 것으로 확인되었습니다. 스팸메일은 4월에 비해 40% 넘게 줄었으나 메일에 포함된 악성코드는 4월에 비해 무려 2배 가까이 증가했습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

(3) 스팸 메일 내의 악성코드 현황

[2013년 05월 01일 ~ 2013년 05월 31일]

순위	악성코드 진단명	메일수[개]	비율[%]
1	W32/Mytob-C	1,451	16.45%
2	W32/MyDoom-H	1,117	12.67%
3	Mal/ZipMal-B	478	5.42%
4	Mal/DrodZp-A	447	5.07%
5	Mal/BredoZp-B	433	4.91%
6	Mal/Phish-A	212	2.40%
7	W32/MyDoom-N	193	2.19%
8	Troj/20120158-P	140	1.59%
9	W32/Virut-T	126	1.43%
10	Troj/Invo-Zip	114	1.29%

스팸 메일 내의 악성코드 현황은 5월 한달 동안 수신된 메일에서 발견된 악성코드 중 Top 10을 뽑은 그래프입니다. 4월과 마찬가지로 W32/MyDoom-H와 W32/Mytob-C가 서로 자리만 바꾸어 각각 1,2위를 차지했으며 지난달 3위를 차지했던 W32/MyDoom-N이 7위로 떨어지고 대신 지난달 10위였던 Mal/ZipMal-B가 3위로 크게 순위가 상승하였습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Part Ⅱ 보안 이슈 돋보기

1. 5월의 보안 이슈

해킹 등 부당한 전자금융 사고에 대해 은행에 책임을 묻는 전자금융거래법 개정안이 지난 주 국회를 통과했습니다. 그밖에 한,일 공동 연구진, '해킹 불가능한 양자통신' 기술 개발, 지정 단말기에서만 인터넷 뱅킹, SW 취약점 신고 포상제, 시행 6개월 만에 3배, 액티브X 필요 없는 윈도8 뱅킹 등이 5월의 이슈가 되었습니다.

• 전자금융거래법 개정안 통과

해킹 등 부당한 전자금융 사고에 대해 은행에 책임을 묻는 전자금융거래법 개정안이 지난 주 국회를 통과하였다. 전자금융거래법 개정안은 은행 등 금융사업자의 책임을 명문화 하였습니다. 개정안의 주요 내용은 해킹사고가 발생하면 일단 금융사가 책임을 지게 됩니다. 물론 이용자 고의나 중과실이 있으면 은행이 면책을 받을 가능성도 있지만, 입증 책임은 은행이 지게 됩니다. 이번에 통과된 전자금융거래법 개정안은 6개월 후에 시행 될 예정입니다.

• 윈도우XP 지원 곧 종료... 기업의 보안은?

마이크로소프트 윈도XP의 지원기간이 채 일년도 남지 않았지만, 국내기업 PC의 절반 이상이 여전히 윈도 XP를 사용하고 있는 것으로 나타났습니다. 이는 세계평균에 비해 비교하기 힘들 정도로 높은 비중입니다. 윈도우XP 서비스 지원이 종료되면 사용자는 보안업데이트, 핫픽스, 기술 지원 등을 받을 수 없게 되며, 최신 드라이버 지원 및 추가로 발견된 취약성에 대한 패치를 받을 수 없기 때문에 보안에 취약한 상태로 불안하게 이용할 수 밖에 없게 되는 것입니다.

• 한,일 공동 연구진, '해킹 불가능한 양자통신' 기술 개발

한,일 공동 연구진이 양자상태의 빛을 증폭시켜 손실 없이 공간 이동시키는 데 성공하였습니다. 양자상태의 빛은 여러 양자상태의 중첩을 이용하여 고 용량의 정보를 담을 수 있으며, 빠른 속도 및 손실 없는 정보전달로 획기적인 보안능력을 갖춘 양자통신, 초고속 양자컴퓨터 등을 구현할 수 있을 것으로 기대됩니다.

• 지정 단말기에서만 인터넷 뱅킹

금융위원회와 금융감독원은 14일부터 그 동안 일부 신청자를 대항으로 시험 시행해 온 '전자금융사기 예방서비스'를 오는 9월 26일부터 모든 이용자를 대상으로 확대 시행한다고 밝혔습니다. 이에 따라서, 앞으로 인터넷뱅킹으로 300만원 이상의 돈을 이체하거나 공인인증서를 재발급 받으려면 이리 지정한 단말기를 이용해야 합니다. 또한 지정되지 않은 단말기로 인터넷뱅킹 시에는, 휴대전화 문자인증이나 유선전화를 통한 인증 등 추가 본인확인 절차를 걸쳐야 합니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

• SW 취약점 신고 포상제, 시행 6개월 만에 3배↑

소프트웨어 취약점을 신고하면 포상금을 지급하는 '신규 취약점 신고 포상제'가 본격적으로 활성화 되고 있습니다. 취약점 수집의 확대를 위하여, 지난 10월부터 우수 신규 취약점에 대해 포상금을 지급하기 시작하였고 이에 신고건수가 크게 증가하였습니다. 신고된 취약점은 국내 소프트웨어가 대부분이였으며, 주로 홈페이지 구축 소프트웨어, PC용 소프트웨어, 모바일 앱 순인 것으로 알려졌습니다.

• 액티브X 필요 없는 윈도8 뱅킹 나왔다

20일, IBK기업은행이 국내 은행권 최초로 윈도8 앱기반 타일모드에서 지원하는 윈도 뱅킹 서비스를 출시하였습니다. 이 윈도뱅킹은 터치기반의 사용자 경험을 반영하였으며, 마우스와 키보드로 이용할 수 있으며, 기존 윈도 기반 인터넷 뱅킹 서비스와의 가장 큰 차이는 애플리케이션 기반이라는 점 입니다. 특히 액티브 X설치가 필요 없으며, 공인인증서는 MS가 제공하는 '공인인증서 관리 앱'에 저장하는 방식입니다.

• 금감원 사칭 익스플로러 팝업창 피싱 주의보

최근 인터넷 사용자들을 대상으로 금융정보를 탈취하기 위하여 피싱사이트로 유도시키는 팝업창이 발견되었습니다. 이번 경우, 사용자가 인터넷을 이용하기 위하여 포털사이트에 접속하면, '금융감독원 보안관련 인증절차 진행'을 사칭한 팝업창이 나타난 후 사라지지 않았습니다. 이렇게 팝업창을 이용한 피싱은 새로운 형식의 피싱 방식으로, 사용자들의 주의가 필요합니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

2. 5월의 취약점 이슈

• Microsoft 5월 정기 보안 업데이트

Internet Explorer 누적 보안 업데이트, HTTP.sys 취약점으로 인한 서비스 거부 문제, .NET Framework의 취약점으로 인한 스푸핑 문제, Lync의 취약점으로 인한 원격 코드 실행 문제 해결 등을 포함한 Microsoft 5월 정기 보안 업데이트가 발표되었습니다.

<해당 제품>

- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows RT**
- **Windows Server 2003**
- **Windows Server 2008**
- **Windows Server 2008 R2**
- **Windows Server 2012**

Internet Explorer 누적 보안 업데이트(2829530)

이 보안 업데이트는 Internet Explorer의 비공개적으로 보고된 취약점 11건을 해결합니다. 가장 위험한 취약점으로 인해 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행이 허용될 수 있습니다. 가장 위험한 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Internet Explorer 누적 보안 업데이트(2847204)

이 보안 업데이트는 Internet Explorer의 공개된 취약점 1건을 해결합니다. 이 취약점은 사용자가 Internet Explorer를 사용하여 특수하게 조작된 웹 페이지를 볼 경우 원격 코드 실행을 허용할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

HTTP.sys 취약점으로 인한 서비스 거부 문제점(2829254)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Windows의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 영향을 받는 Windows 서버나 클라이언트에 특수하게 조작된 HTTP 패킷을 보낼 경우 서비스 거부가 발생할 수 있습니다.

.NET Framework의 취약점으로 인한 스푸핑 문제점(2836440)

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

이 보안 업데이트는 .NET Framework의비공개적으로 보고된 취약점 1건과 공개적으로 보고된 취약점 1건을 해결합니다. 가장 위험한 취약점으로 인해 .NET 응용 프로그램에서 특수하게 조작된 XML 파일을 수신할 경우 스푸핑을 허용할 수 있습니다. 취약점 악용에 성공한 공격자는 파일의 서명을 무효화하지 않으면서 XML 파일의 내용을 수정하고 인증된 사용자인 것처럼 종점 기능에 대한 액세스 권한을 얻을 수 있습니다.

Lync의 취약점으로 인한 원격 코드 실행 문제점(2834695)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Lync의 취약점을 해결합니다. 이 취약점으로 인해 공격자가 특수하게 조작된 콘텐츠(파일 또는 프로그램 등)를 Lync 또는 Communicator에서 프레젠테이션으로 공유한 다음 사용자가 초대를 수락하여 프레젠테이션 가능한 콘텐츠를 보거나 공유하도록 유도할 경우 원격 코드 실행이 허용될 수 있습니다. 어떠한 경우에도 공격자는 강제로 사용자가 공격자 제어 파일 또는 프로그램을 보거나 공유하도록 만들 수는 없습니다. 대신 공격자는 사용자가 Lync 또는 Communicator에서 초대를 수락하여 프레젠테이션 가능한 콘텐츠를 보거나 공유하게 하는 등의 조치를 취하도록 유도해야 합니다.

Microsoft Publisher의 취약점으로 인한 원격 코드 실행 문제점(2830397)

이 보안 업데이트는 Microsoft Office에서 발견되어 비공개적으로 보고된 취약점 11건을 해결합니다. 이러한 취약점으로 인해 사용자가 영향을 받는 버전의 Microsoft Publisher로 특수하게 조작된 Publisher 파일을 열 경우 원격 코드 실행이 허용될 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Word의 취약점으로 인한 원격 코드 실행 문제점(2830399)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 영향을 받는 Microsoft Office 소프트웨어에서 특수하게 조작된 파일을 열거나 특수하게 조작된 전자 메일 메시지를 미리 볼 경우 코드 실행을 허용할 수 있습니다. 취약점 악용에 성공한 공격자는 현재 사용자와 동일한 권한을 얻을 수 있습니다. 시스템에 대한 사용자 권한이 적게 구성된 계정의 사용자는 관리자 권한으로 작업하는 사용자에 비해 영향을 적게 받습니다.

Microsoft Visio의 취약점으로 인한 정보 유출 문제점(2834692)

이 보안 업데이트는 비공개적으로 보고된 Microsoft Office의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 Visio 파일을 열 경우 정보 유출이 발생할 수 있습니다. 이 취약점으로 인해 공격자가 직접 코드를 실행하거나 해당 사용자 권한을 상승시킬 수는 없지만 영향을 받는 시스템의 손상을 악화시키는 데 사용할 수 있는 정보를 생성할 수 있습니다.

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Windows Essentials의 취약점으로 인한 정보 유출 문제점(2813707)

이 보안 업데이트는 비공개적으로 보고된 Windows Essentials의 취약점을 해결합니다. 이 취약점으로 인해 사용자가 특수하게 조작된 URL을 사용하여 Windows Writer를 열 경우 정보 유출이 발생할 수 있습니다. 취약점 악용에 성공한 공격자는 Windows Writer 프록시 설정을 무시하고 대상 시스템에서 사용자가 액세스할 수 있는 파일을 덮어쓸 수 있습니다. 웹 기반의 공격 시나리오에서 웹 사이트는 이 취약점을 악용하는 데 사용되는 특수하게 조작된 링크를 포함하고 있을 수 있습니다. 공격자는 사용자가 웹 사이트를 방문하고 특수하게 조작된 링크를 열도록 유도해야 합니다.

커널 모드 드라이버의 취약점으로 인한 권한 상승 문제점(2840221)

이 보안 업데이트는 Microsoft Windows에서 발견되어 비공개적으로 보고된 취약점 3건을 해결합니다. 공격자가 시스템에 로그온하고 특수하게 조작된 응용 프로그램을 실행할 경우 이 취약점으로 인해 권한 상승이 허용될 수 있습니다. 이 취약점을 악용하려면 공격자가 유효한 로그온 자격 증명을 가지고 로컬로 로그온할 수 있어야 합니다.

<해결방법>

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

한글 : http://technet.microsoft.com/ko-kr/security/bulletin/ms13-may
영문 : http://technet.microsoft.com/en-us/security/bulletin/ms13-may

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

• 아래한글 임의코드 실행 취약점 보안 업데이트 권고

한글과컴퓨터社에서 개발한 워드프로세서인 '아래한글'에서 임의 코드실행이 가능한 취약점이 발견됨

낮은 버전의 아래한글 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 보안업데이트 권고
공격자는 웹 게시물, 스팸 메일, 메신저의 링크 등을 통해 특수하게 조작된 한글문서(HWP)를 열어보도록 유도하여 임의코드를 실행시킬 수 있음

<해당 제품>

- 한글 2007 7.5.12.672 이전 버전
- 한글 2010 SE+ 8.5.8.1340 이전 버전

<해결 방법>

- 한글과컴퓨터 홈페이지에서 보안업데이트 파일을 직접 다운로드 받아 설치하여 아래 버전으로 업데이트
  - 한글 2007 7.5.12.672 이상 버전
  - 한글 2010 SE+ 8.5.8.1340 이상 버전
  - 다운로드 경로 : http://www.hancom.co.kr/downLoad.downPU.do?mcd=001

- 한글과컴퓨터 자동 업데이트를 통해 한글 최신버전으로 업데이트
  - 시작 → 모든 프로그램 → 한글과컴퓨터 → 한글과컴퓨터 자동 업데이트

<참고사이트>

http://www.hancom.co.kr/downLoad.downPU.do?mcd=001

• Adobe Reader/Acrobat 신규 취약점 주의 권고

Adobe社는 Adobe Reader와 Acrobat에 영향을 주는 취약점을 해결한 보안 업데이트를 발표.
낮은 버전의 Adobe Reader/Acrobat 사용자는 악성코드 감염에 취약할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Adobe社는 Adobe Reader/Acrobat의 취약점 27개에 대한 보안 업데이트를 발표

- 임의코드 실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, CVE-2013-3341)

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

- 임의코드 실행으로 이어질 수 있는 정수형 언더플로우 취약점(CVE-2013-2727, CVE-2013-2549)
- 샌드박스 보호기능 우회로 이어질 수 있는 'use-after-free' 취약점(CVE-2013-2550)
- 정보 유출로 이어질 수 있는 자바 스크립트 API 취약점 (CVE-2013-2737)
- 임의코드 실행으로 이어질 수 있는 스택오버플로우 취약점(CVE-2013-2724)
- 임의코드 실행으로 이어질 수 있는 버퍼오버플로우 취약점(CVE-2013-2730, CVE-2013-2733)
- 임의코드 실행으로 이어질 수 있는 정수형 오버플로우 취약점(CVE-2013-2727, CVE-2013-2729)
- 운영체제에 의해 블랙리스트 처리된 도메인을 Reader에서 처리하는데 발생한 취약점 (CVE-2013-3342)

<해당 제품>

• Adobe Reader XI 윈도우즈 및 Mac 11.0.02 및 이전 버전
• Adobe Reader X 윈도우즈 및 Mac 10.1.6 및 이전 버전
• Adobe Reader 9 윈도우즈, Mac 및 리눅스 9.5.4 및 이전 버전
• Adobe Acrobat XI윈도우즈 및 Mac 11.0.02 및 이전 버전
• Adobe Acrobat X 윈도우즈 및 Mac 10.1.6 및 이전 버전
• Adobe Acrobat 9 윈도우즈 및 Mac 9.5.4 및 이전버전

<해결 방법>

• Adobe Reader 사용자
- Adobe Download Center(http://get.adobe.com/kr/reader/otherversions/)를 방문하여 최신 버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

• Adobe Acrobat 사용자
- 아래의 Adobe Download Center를 방문하여 최신 버전을 설치하거나 [메뉴]→[도움말]→[업데이트확인]을 이용하여 업그레이드

• 윈도우즈 환경의 Adobe Acrobat
http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Windows

• 맥킨토시 환경의 Adobe Acrobat Pro
http://www.adobe.com/support/downloads/product.jsp?product=1&platform=Macintosh

<참고사이트>

http://www.adobe.com/support/security/bulletins/apsb13-15.html

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

• Adobe Flash Player 취약점 보안 업데이트 권고

Adobe社는 Adobe Flash Player에 영향을 주는 코드실행 취약점을 해결한 보안 업데이트를 발표.

낮은 버전의 Adobe Flash Player 사용으로 악성코드 감염 등의 사고가 발생할 수 있으므로 해결방안에 따라 최신버전으로 업데이트 권고

Adobe社는 Adobe Flash Player의 13개 취약점을 해결한 보안 업데이트를 발표

- 코드실행으로 이어질 수 있는 메모리 손상 취약점 (CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, CVE-2013-3335)

<해당 제품>

- Flash Player 윈도우즈 및 Mac11.7.700.169 및 이전 버전
- Flash Player 리눅스 11.2.202.280 및 이전 버전
- Flash Player 안드로이드 4.x 11.1.115.54 및 이전 버전
- Flash Player 안드로이드 3.x, 2.x 11.1.111.50 및 이전 버전
- AIR 윈도우즈 및 Mac3.7.0.1530 및 이전 버전
- AIR 안드로이드 3.7.0.1660 및 이전버전
- AIR SDK 및 Compiler3.7.0.1530 및 이전버전

<해결 방법>

- 윈도우, Mac, 리눅스 환경의 Adobe Flash Player 사용자
  - Adobe Flash Player Download Center

(http://get.adobe.com/kr/air/http://get.adobe.com/kr/air/) 에 방문하여 Adobe Flash Player 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

- 윈도우8 버전에서 동작하는 인터넷익스플로러10 버전 사용자
  - 윈도우 자동업데이트 적용

- 안드로이드 환경의 Adobe Flash Player 사용자
  - Adobe Flash Player가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속
    → 메뉴 선택 → 내 애플리케이션 선택 → Adobe Flash Player 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

- 구글 크롬브라우저 사용자
  - 크롬브라우저 자동업데이트 적용

- 윈도우, Mac 환경의 Adobe AIR 사용자

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

- Adobe AIR Download Center(http://get.adobe.com/kr/air/)에 방문하여 Adobe AIR 최신 버전을 설치하거나, 자동 업데이트를 이용하여 업그레이드

• Adobe AIR SDK 사용자

- (http://www.adobe.com/devnet/air/air-sdk-download.html)에 방문하여 Adobe AIR SDK 최신 버전을 설치

• 안드로이드 환경의 Adobe AIR 사용자

- Adobe AIR가 설치된 안드로이드 폰에서 '구글 플레이 스토어' 접속

→ 메뉴 선택 → 내 애플리케이션 선택 → Adobe AIR 안드로이드 최신 버전으로 업데이트 하거나 자동업데이트를 허용하여 업그레이드

<참고사이트>

http://www.adobe.com/support/security/bulletins/apsb13-14.html

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.

Contact us...

㈜이스트소프트 알약대응팀

Tel : 02-3470-2999

E-mail : help@alyac.co.kr

알약 홈페이지 : www.alyac.co.kr

ESTsoft Copyright © by ESTsoft Corp. All rights reserved.