Brazil Hacking Group 분석 및 대책
(Windows Attack II)

2002년 8월 29일

(29th birthday)

작성자: 전 상훈 (nickname: 바다란)
(winsnort@securityindepth.net)

Brazil Hacking Group Analysis
Windows Attack –II

==========

1. Details

지난번 문서에서는 중국내의 동향과 Exploit에 대한 시야를 밝혔고 (http://www.hackerslab.org/korg/news_letter/pdf/Threat_of_china.pdf) 이번에는 최근 2달 사이에 가장 왕성한 활동을 하는 Brazil Hacker group에 대해서 알아보도록 하겠다. 이 부분은 최근 언론에 몇 번 언급 되기도 하였지만 (영국의 보안그룹 mi2g의 자료인용) 본인의 경우에는 New Attack Pattern에 관하여 조사하고 분석하던 중 최근 들어 유심히 Brazil hacker group에 대해서 관심을 가지고 보았다. 그들이 공격하는 서버들간의 취약성에 대한 해킹패턴과 기법들에서 일전의 문서에서 기술한 취약점을 공격하는 공개되지 않은 Exploit 이 일정 수준 진화 되었으며 고전적인 방법 (Netbios ,관리자들의 실수) 도 병행하여 Web Page Deface 가 이루어 지고 최근 국내서버에 대한 Deface의 경우도 많은 기여(?)를 하고 있고 국외의 인터넷 서버에 대한 해킹도 아주 높은 비율을 차지하고 있기 때문이다.

일반적인 수치의 나열에 그치는 Security group report 가 아닌 좀 더 세밀한 내용과 기술적인 분석 그리고 동향에 대해서 언급하고자 이 문서를 만들게 되었다.
(이번에는 한문이 아닌 스페니쉬 였다. -,-;)

이 문서를 만들고 있는 8월 29일 현재 Defaced.alldas.org 사이트에 대한 접속 불가로 정확한 수치에 대한 통계는 틀릴 수 있으나 브라질 내에 존재하는 Deface mirror 사이트와 다른 Deface mirror 사이트 두 곳을 이용하여 통계치를 추정하도록 하겠다.

http://www.delta5.com.br/mirror/ 2002년 6월 말부터 활동
http://www.zone-h.org/en/defacements/filter

2.Explain

우선 http://www.delta5.com.br/mirror/topdefacer/에서 6월말 이후 Deface 활동이 활발했던 그룹을 Filtering 해보면 다음과 같다.

Top Defacer Ranking (2002/8/29. statistic)

Fatal Error	363	15.0%
ISOTK	332	13.7%
Red Eye	310	12.8%
Xfaulz	158	6.54%
hax0rs lab	157	6.50%
ION	142	5.87%
Perfect Attack	136	5.63%
tty0	114	4.72%
Endiabrad0s	101	4.18%
Pinchadores Web	92	3.80%
0day	65	2.69%
Perfect.Br	63	2.60%
cybers satans	37	1.53%
Web Pirates	34	1.40%
uname-a	34	1.40%
Affix	24	0.99%

가장 많은 Defacement를 기록한 그룹으로 Fatal Error 와 ISOTK , Red Eye 그룹이 되겠다. 최근 지속적으로 주시한 그룹은 ISOTK 와 Red Eye 그룹이 였었고 이 두 그룹이 MS 계열에 대한 해킹과 공격에 활발한 활동을 보였다.
Fatal Error 의 경우 FreeBSD와 MS 계열이 절반 정도 비율로 Deface 를 하였으며 ISOTK는 MS와 Linux 서버의 비율이 7:3 정도로 Deface 하였다.Red Eye는 MS 의 비율이 99% 정도 차지 하고 있다. 브라질내의 해커들이 활발하게 활동하고 Deface 된 사이트를 적극적으로 Upload 하는 브라질 내의 사이트 이므로 신뢰성이 높으리라 생각된다.

==========

그룹단위로 해킹이 이루어 지므로 전문적인 지식을 보유한 OS에 따라 비율이 편향된 것으로 보여지며 참고로 haXors lab에 대한 자료는 *nix 계열 (Unix ,Linux , BSD Series…) 이 전체를 차지 하고 있다.

다음은 또 다른 Defacement Mirror 사이트에서 위의 그룹들에 대해서 전체적인 통계를 알아 보도록 하겠다.
http://www.zone-h.org/en/defacements/filter

그룹별 Deface site count

Fatal Error : 371 deface site 2002.7.5 ~ 2002.8.27
Red Eye: 650 deface site 2002.4.5 ~ 2002.8.28
ISOTK : 1055 deface site . 2002.3.5 ~ 2002.8.28
hax0rs lab : 2000 deface site 2002.1.3 ~2002.8.24
M4F14 : 568 deface site 2002.1.14~ 2002.8.27

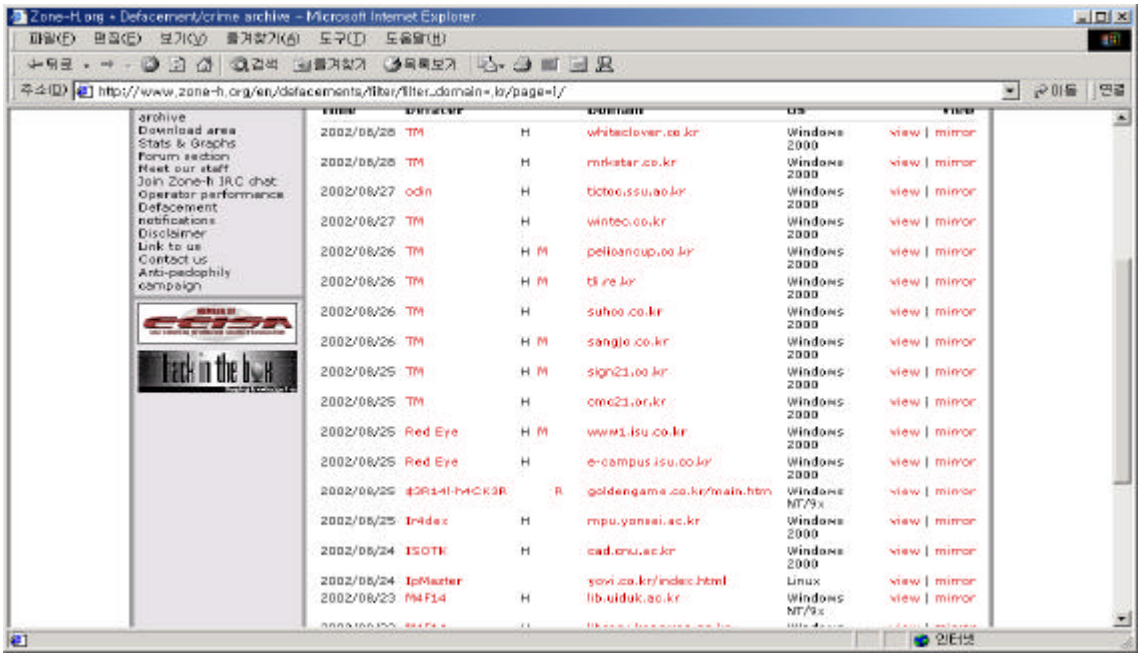
Kr domain defacement

Kr deface : 1091 deface site : 1999.9 ~ 2002.8

Red Eye : 18 deface site 2002.4.5 ~ 2002.8.28 :기업체 다수
Fatal Error: 5 deface site 2002.7 ~ 2002.8 :관공서 포함
ISOTK : 23 deface site 2002.3 ~ 2002. 8 : 대학,기업체
hax0rs lab : 11 deface site 2002.1.3 ~2002.8.24 :대학 ,기업체
M4F14 : 5 deface site 2002.1.14~ 2002.8.27:대학 ,관공서

kr 도메인 만 포함한 것이므로 .com , .net 등의 도메인은 포함되지 않았다. 또한 defaced mirror site 의 데이터를 종합하기가 어려운 관계로 대략적인 추정치라고 할 수 있다. 여러분들도 직접 해보시면 다수의 알만한 기업 및 대학들이 지속적으로 해킹을 당하는 것을 볼 수 있다. 또 이런 Defaced mirror site에 등록이 되면 지속적으로 스크립트 키드로부터 공격을 받을 수 있는 대상이 되므로 더욱 더 관심

을 기울이고 보안에 신경을 써야 한다.
일반적으로 mirror 사이트에 올라오는 비율은 타이트하게 통계치를 추정 했을 경우이며 실제 해킹 비율의 10% 정도로 추정을 할 수 있다. 개인적인 경험상 이 정도 일 것으로 추정하는 것일 뿐 정확한 데이터는 아님을 밝혀둔다.



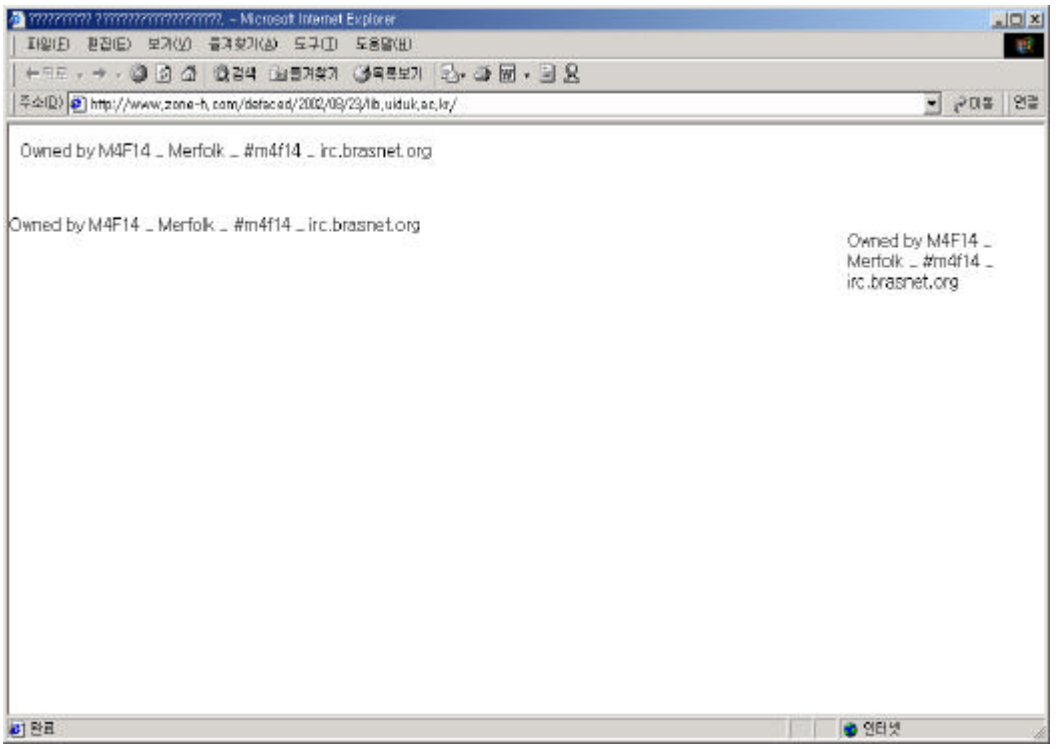
8월 28일 kr deface list

7,8월 들어서 해킹패턴의 특이한 형태라면 Windows 계열이 급격하게 증가한 것을 들 수 있다. 이 부분에 대한 것은 습득한 Exploit 및 제작한 취약성 점검도구를 이용하여 체크 해본바 일전의 문서에서 지적한 취약점을 업그레이드 한 형태로 파악이 되며 비단 브라질 해커들 뿐 아니라 전 세계의 해커 클럽들이 어느 정도는 Exploit을 확보하거나 갱신한 것으로 보인다. .idc, .ida , .printer 확장자에 대한 overflow 공격과 FrontPage Extension에 대한 공격 등이 주된 공격으로 보여지며 몇몇 deface 된 사이트들의 점검에서 언급된 취약점들을 공통적으로 찾을 수 있었다.
특히 ServicePack 1,2를 적용 했음에도 불구하고 공격이 가능한 exploit 이 지속적으로 개발되어 Underground에서 배포되는 것을 중국의 홍커의 예에서도 볼 수 있었지만 이곳도 마찬가지라 판단되며 또한 IRC (Internet Relay Chat)를 통한 Chatting 문화에 익숙해져

있어서 IRC를 통한 폐쇄적인 자료의 공유와 토론으로 일정수준에 동시에 도달하지 않았나 하는 판단을 하게 된다.

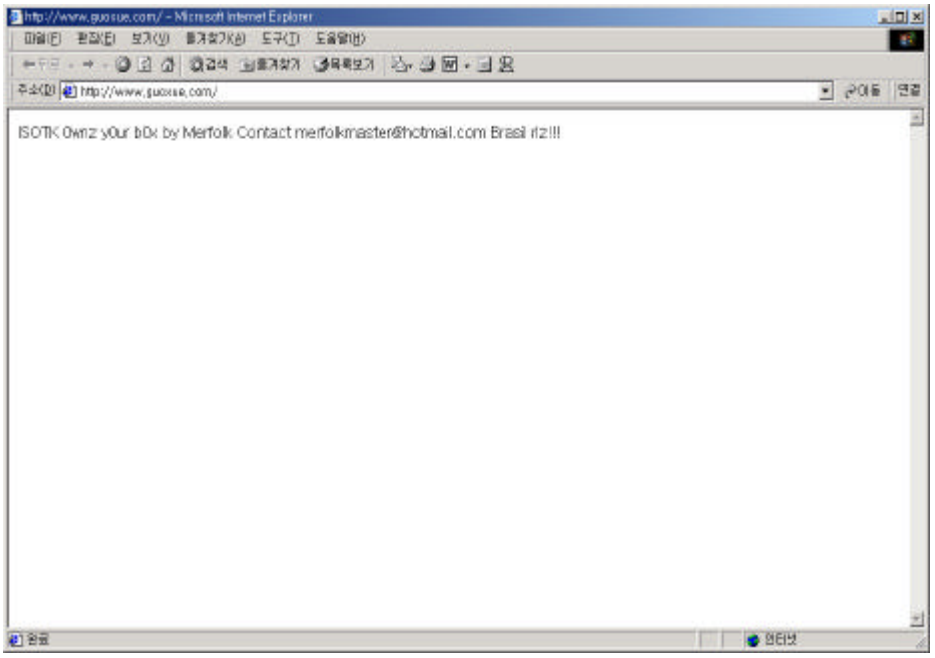
심지어 침해를 당한 시스템을 간단히 살펴보게 되면 패스워드정책의 잘못된 설정도 다수 있었으며 Hotfix 와 ServicePack 등을 충실하게 설치 했음에도 불구하고 해킹을 당한 곳들도 있었다. 해킹 당한 시스템의 1/3 이상은 방화벽을 갖추고 있음에도 불구하고 해킹을 당한 곳들이다. 적절한 필터링 정책과 방화벽의 세팅 에도 불구하고 HTTP Port에 대한 공격에는 무방비 일 수 밖에 없는 상태였다. BSD 및 *nix 계열의 경우에는 Apache 와 RPC 관련된 공격이 주류를 이루는 것으로 판단하며 MS windows 계열에는 IIS 상에 설치된 Default Extension 및 서비스에 대하여 공격이 이루어 지는 것으로 판단된다. NT 시스템의 경우는 98년부터 많은 해킹과 공격이 이루어졌던 MSADC 에 대한 공격 비율이 높은 것으로 판단이 된다. 검사결과 대부분의 시스템에서 발견 할 수 있었다.

각 해킹 페이지에 대한 샘플 갭쳐이다.

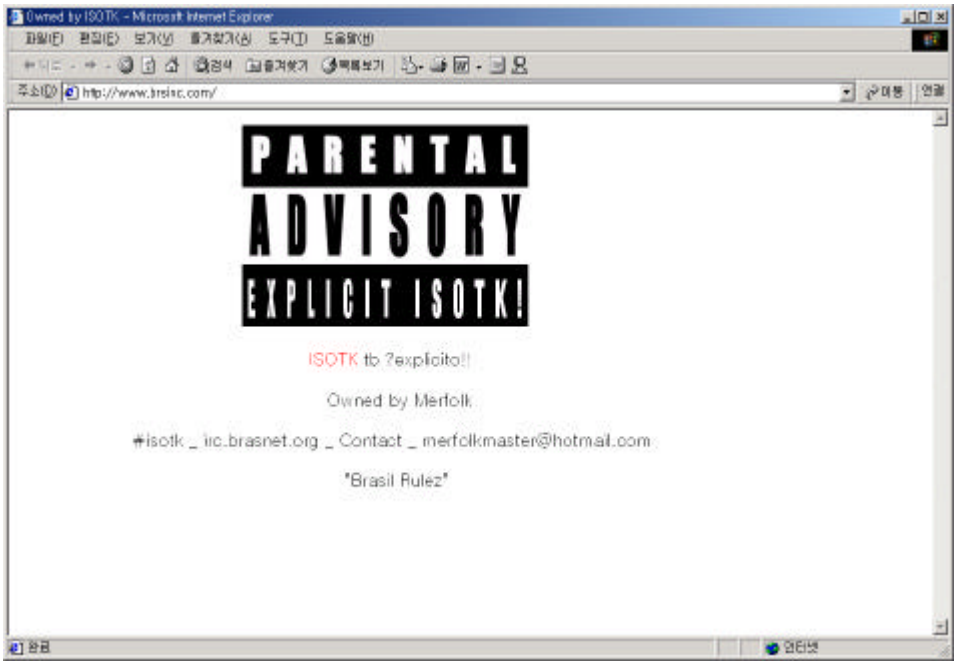


M4F14 Defaced

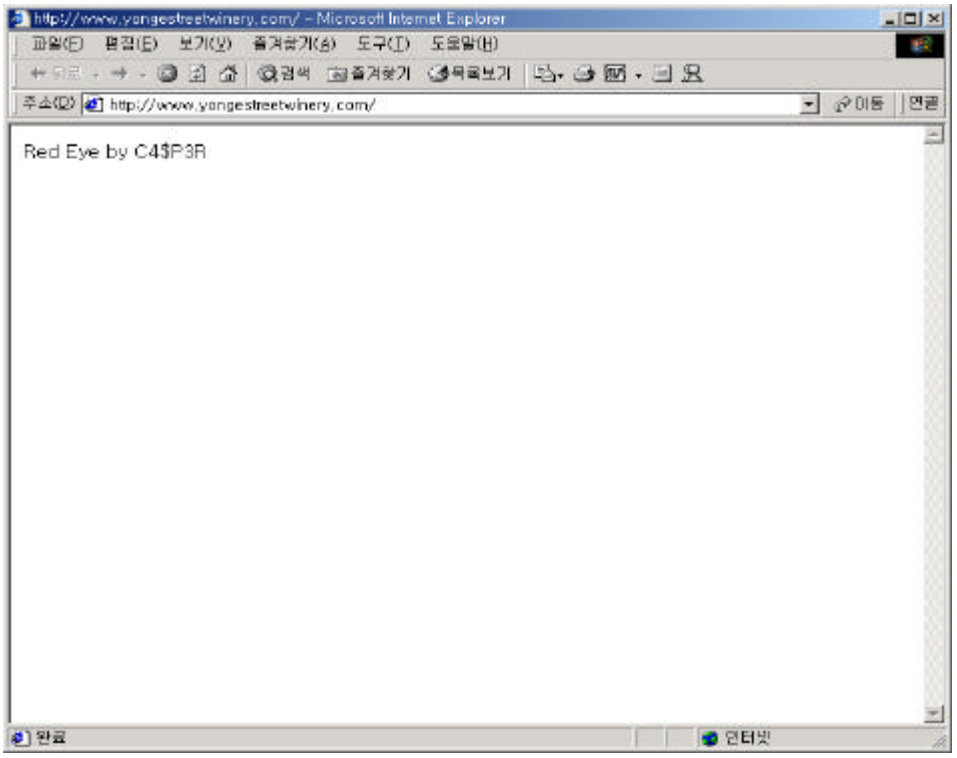
Supr3m3.L0rds



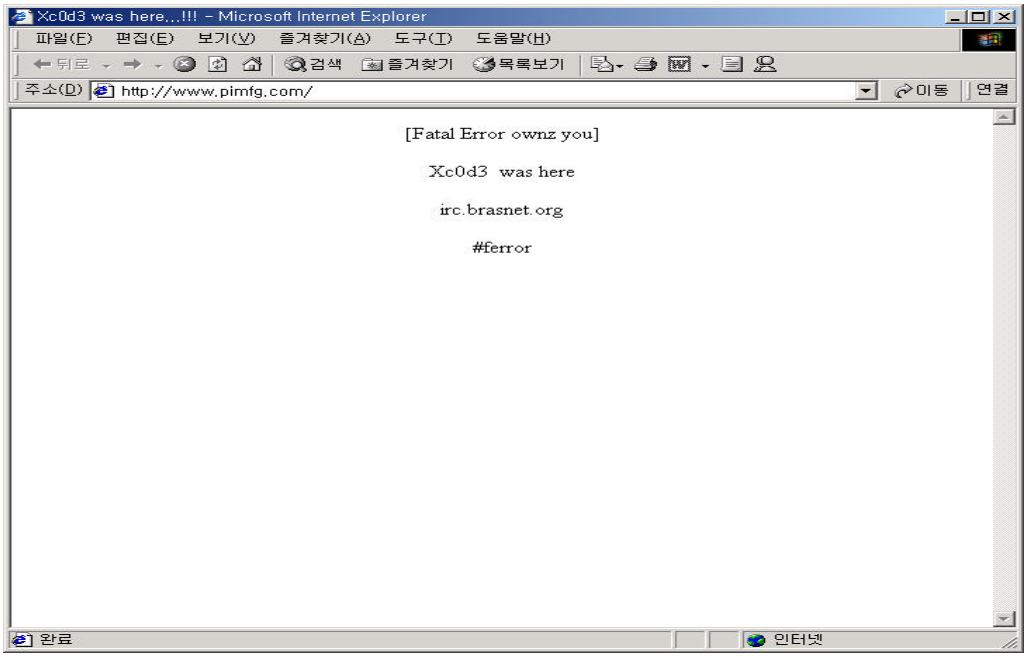
ISOTK defaced site



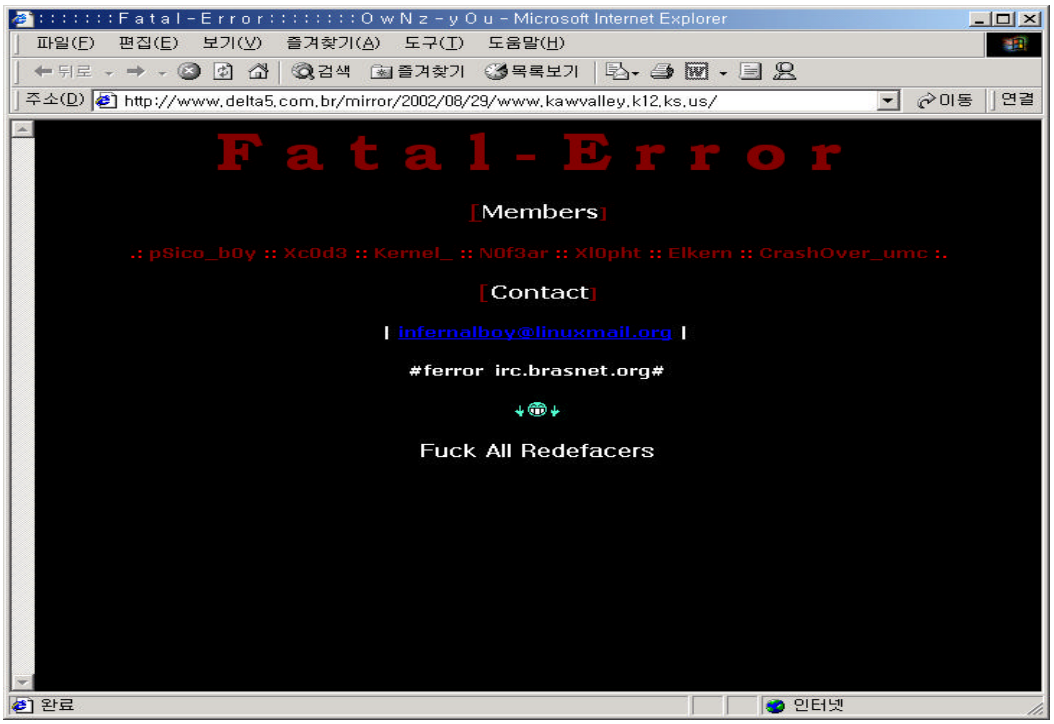
ISOTK Defaced



Red Eye Defaced



Fatal Error Defaced



Fatal Error Defaced

Attack 을 한 후 Page를 변조하고 defaced mirror site에 정보를 올리는 순간부터 다른 크래커 및 해커그룹에 의해 Redeface 가 자주 일어남을 Fatal Error 가 8월29일 해킹 한 사이트에서도 지적하고 있다.

Brazil Hacking Group Analysis

Windows Attack –II

==========

Page Deface에서 Text 문자로 입력된 부분은 만약 NT 계열 이었다면 MSADC Attack에 의한
echo “defaced by ~ ~”~ > c:\Inetpub\wwwroot\index.html 등과 같은 문자열 입력에 의한 공격이 이루어 졌을 가능성이 높고 이미지까지 같이 올려진 사이트의 경우는 직접 System 권한을 획득 한 후 백도어 (nc ,icmd …)등을 이용하여 파일을 업로드 하게 된다. (이 부분에 대해서는 다음에 나올 New Attack Pattern 분석 문서에서 나올꺼다.)
대략 짧게 언급한 방법에 의해 웹페이지 변조가 이루어 지게 되며 Linux 의 경우 rhost에 의한 Trust 관계가 맺어져 있을 경우 같은 Subnet 상의 모든 시스템에 대해서 공격이 가해짐을 볼 수 있다. NT, 2000 의 경우에서는 Web Hosting server 가 해킹을 당했을 경우에는 웹호스팅을 제공 받고 있는 전체 웹페이지에 대한 변조가 일어 난다. 그러므로 Linux 등 Windows 계열이든 대량 Deface 가 종종 일어나기도 하는데 다음은 그와 같은 예이다.

Windows ASP.NET 을 설치한 Italy 의 웹호스팅 회사의 서버가 해킹당한 후 페이지가 Deface 된 List 이다.

Time	Defacer	Domain	OS
2002/08/27	R[]l4nD	infoplus.gare.it	Windows 2000
2002/08/27	R[]l4nD	garedappalto.it	Windows 2000
2002/08/27	R[]l4nD	ifras.it	Windows 2000
2002/08/27	R[]l4nD	…aplus.infoplus.gare.it	Windows 2000
2002/08/27	R[]l4nD	entiappaltanti.it	Windows

			2000
2002/08/27	Shellc0d3	eurotech.it	Windows 2000
2002/08/27	R[]l4nD	art.trento.gare.it	Windows 2000
2002/08/27	R[]l4nD	Mauri.infoplus.gare.it	Windows 2000
2002/08/27	R[]l4nD	omnia.gare.it	Windows 2000
2002/08/27	R[]l4nD	partner.infoplus.gare.it	Windows 2000
2002/08/27	R[]l4nD	sa.infoplus.gare.it	Windows 2000
2002/08/27	R[]l4nD	tuttoappalti.it	Windows 2000
2002/08/27	R[]l4nD	appaltiininternet.it	Windows 2000

위의 사이트는 계정관리의 잘못으로 인해 전체 호스팅 웹페이지에 대한 Deface 가 단기간에 이루어진 곳 이다. Windows 2000 의 관리자 권한 계정에 대한 정책 부재 및 무관심으로 인하여 Italy 웹페이지 몇 십개가 해킹을 당했다.

NT 나 2000 의 경우 rhost 등의 Trust 관계 대신 Domain Controller 가 사용되나 Domain Controller 해킹 후 하위 시스템을 해킹하는 것이 아닌 웹 호스팅 업체의 서버를 공격 후 여러 곳을 일괄적으로 Deface 하는 것들이 많이 사용된다.

*nix , BSD 계열은 rhost 등의 Trust 관계를 이용하여 인접 시스템을 공격하기도 하고 Subnet 상에 Sniffer 설치 후 일괄적으로 패스워드 및 계정정보 습득 후 Deface 하기도 한다.

아래의 표는Fatal Error Group 이 한대를 해킹 한 후 rhost 등의 관계를 이용하여 서브넷 상의 시스템을 유린한 결과 이다.

2002/08/26	Fatal Error	161.58.4.212	FreeBSD
2002/08/26	Fatal Error	161.58.4.217	FreeBSD
2002/08/26	Fatal Error	161.58.4.219	FreeBSD
2002/08/26	Fatal Error	161.58.4.226	FreeBSD
2002/08/26	Fatal Error	161.58.4.233	FreeBSD
2002/08/26	Fatal Error	161.58.4.237	FreeBSD
2002/08/26	Fatal Error	161.58.4.239	FreeBSD
2002/08/26	Fatal Error	161.58.4.243	FreeBSD
2002/08/26	Fatal Error	161.58.4.245	FreeBSD
2002/08/26	Fatal Error	161.58.4.246	FreeBSD
2002/08/26	Fatal Error	161.58.4.249	FreeBSD

2001년에 해킹 그룹이 인터뷰한 내용을 다시 한번 보며 공격하는 패턴과 선호하는 패턴이 어떠했고 또 현재는 대략적으로 어떤 형식으로 변화 하였는지 짚어 보도록 하자.

전문을 읽고 싶으면 해당 URL에 가면 읽을 수 있다. 다양한 항목에 대해서 의견을 받고 기재해 놓은 내용이므로 이해에 도움이 될 수도 있다.
http://www.dominasecurity.com/eng/allnews.asp?newsid=65

hax0rs lab

http://www.dominasecurity.com/hackerz/hax0rs_lab.htm

How do you choose your targets: do you plan first to attack some precise site or just scan one C class and find targets there?

We make A, B or C class scans from a shell so we hack the vulnerable hosts, although sometimes we plan to hack a specific
target but ofter this target is an hard work so we spend a lot of time on it.

If you have the possibility, do you usually install a backdoor into a computer you've just conquered so to leave open to you the possibility to come always back?

Yeah, usually we install a backdoor on the target but just if the connection is fast (something like Cable, T1, T3...).
We do it to leave open for us the possibility of using this computer as a bounce for future attacks or just to scan hosts.

What is the most common method of attacks in order to deface (buffer overflows, configuration errors, brute forcing, common vulnerabilities, etc.)? Why?

We think that common vulnerabilities and buffer overflows are the most common bugs, but if the admin is stupid, also configuration errors.

..Buffer Overflow 와 그리고 일반적인 스캐너에 나타나는 버그 그리고 관리자의 Mistake를 이용하여 해킹에 이용한다고 했다. 또 대상의 선정에 있어서도 A, B , C class 대역을 무작위 스캔하여 취약점이 발견 되는 사이트를 공격한다고 되어 있다. (전형적인 스크립트 키드 이나 자체 툴 및 Exploit 이 존재한다고 판단 하므로 수준 있는 크래커라 할 수 있다.) 백도어의 설치는 망 속도에 따라 설치 한다고 되어 있는데 국내사이트는 아주 좋은 목표다.

Brazil Hackers Sabotage

http://www.dominasecurity.com/hackerz/bhs.htm

How do you choose your targets: do you plan first to attack some precise site or just scan one C class and find targets there?

Currently, we're defacing many famous sites, as Sony, Unicef, Jesus, Llinux, etc.. these are precises sites.

But we wanna be the group that have more defaces in the world, so we scan the classes B and C, to find anything to hack.

If you have the possibility, do you usually install a backdoor into a computer you've just conquered so to leave open to you the possibility to come always back?

Only if the shells are good. As pPentium 3 whith more than 3 mb link. (very fast connection).
So we install backdoor, and take off the deface and the admin won't notice anything.

What is the most common method of attacks in order to deface (buffer overflows, configuration errors, brute forcing, common vulnerabilities, etc.)? Why?

Common vulnerabilities are the most popular. Buffer overflows also. Brute force, sometimes because takes too much time to do it.

hax0rs lab에서 언급된 내용과 동일하다.

Silverlords of Brazil

How do you choose your targets: do you plan first to attack some precise site or just scan one C class and find targets there?

Both =] usually I write down the site that I want to hack and then I wait for the right exploit to come =] but sometimes I scan c classes most of the times that I do that is to get shells...

If you have the possibility, do you usually install a backdoor into a computer you've just conquered so to leave open to you the possibility to come always back?

Yes, always

What is the most common method of attacks in order to deface (buffer overflows, configuration errors, brute forcing, common vulnerabilities, etc.)? Why?

Errors like UNICODe, php-nuke, frontpage... are the most communs because those are the easiest way to hack =].

SilverLords의 경우는 원하는 대상을 지정하고 익스플로잇이 나오기를 기다리기도 하고 클래스대역을 스캔 해서 공격하기도 한다고 하였다. 2001년도에 자주 사용하였던 공격방법을 기술하고 있는데 이것을

2002년 8월 버전으로 바꾸게 되면 다음과 같다.
Apache에 대한 취약점과 PHP 그리고 ida, idq , printer extension overflow , frontpage attack 등을 이용하여 공격을 한다고 변경할 수 있다.

BlackHat Israel

How do you choose your targets: do you plan first to attack some precise site or just scan one C class and find targets there?

Basically, we like to own famous sites, such as linux address sites etc, the top is to find very famous site, and own him if he is hackable, then it will be good.

==========

If you have the possibility, do you usually install a backdoor into a computer you've just conquered so to leave open to you the possibility to come always back?

Well, if we want to get the site information every day, such as mails, telphones, passwords, Credit Cards, or some other important information, we install BackDoor, its good that you will have some RooTkiT on your box.

What is the most common method of attacks in order to deface (buffer overflows, configuration errors, brute forcing, common vulnerabilities, etc.)? Why?

We think that common vulnerabilities, cuz all the poeple know that, its very popular on hackers, about the buffer overflows, we sometimes use it for down some site its kind a of lame, we dont use it so much, brute force - take a lot of time, and maybe it can give you what you want, we often use common vulnerabilities but we use buffer overflows too, it's defend of the site demons and holes.

전체 그룹의 의견을 대변하는 것은 아니지만 일반적인 Deface group 의 생리와 특성에 대해서 이해하는 데 도움이 될 것이다. 가끔은 특별한 Exploit을 제작하여 공격하기도 하지만 대부분의 일반적인 Deface Group 의 경우는 기존의 Exploit과 관리자의 mistake를 적극적으로 활용하여 가능한 서버에 대해서 공격을 가한다고 되어 있다. 또 몇몇은 목표를 지정하고 Exploit이 나올 때 까지 기다리기도 한다고 되어 있다. 관리자가 더 빨리 Exploit에 대해서 조치를 취하여야 문제를 해결 할 수 있을 텐데 국내의 경우는 무작정 Patch 나 Hotfix 가 나오기 만을 기다리는 형태이다.

즉 목표가 되었을 경우에는 언제든 해킹 당할 수 있다는 이야기가 된다. 또한 대부분의 국내 서버 관리자들의 경우에도 서버관리 업무만을 담당하는 것이 아니며 보안에 관한 지식도 충분하지 않으므로 무방비로 당할 수 밖에 없다.

앞으로도 계속해서 쭉 당할 수 밖에 없다.

회사의 의사결정권을 지닌 사람들의 보안의식도 높아지지 않는 한 또 해킹을 당한 서버의 근원적인 문제점들을 치유하지 않은 채 백업 받아 놓은 웹 페이지만 다시 덮어 씌운다고 해결될 문제도 아닌 것을 알 것이다. 몇몇 해킹 그룹들의 인터뷰를 보면 알겠지만 대부분이 백도어를 설치 한다고 되어 있고 이것이 현실인 것이다. 앞으로는 더욱 더 심해질 것이다.

앞으로의 미래는 어찌 되건 간에 온라인으로 상당부분이 천천히 혹은 급격하게 옮겨가게 될 것이다. 이런 온라인의 침입에 대응하는 인력의 육성과 전문적인 지식의 축적 없이는 모래사장에 빌딩을 짓는 것과 마찬가지 일 것이다.
지식의 축적을 위해서 학원 또는 학교에서 가르치는 것이 정답이 아니라 지식을 충족하려는 사람들이 생존하고 생활할 수 있으며 성과나 가치를 인정해 주어야 한다고 생각한다. 가끔은 이런 일들을 하는 것이 여유 있고 의식주의 문제가 없는 사람들이 해야 하는 것이 아닌가 고민해 보기도 한다. 변명일지 모르지만 본인 또한 빈자 이고 환경에서 허덕이며 많은 것을 보고 고민하기엔 여유가 없음을 고백한다.

3.Solution

지난번 문서와 똑같다. 왜냐하면 수준이 그 수준일 정도로 해킹과 크래킹도 어느 곳이든 평준화가 되어 있기 때문에 보안설정도 범주를 벗어나지 않는다.

솔루션은 Hotfix 를 이용한 패치와 URLScan 을 이용한 필터링 , 그리고 내부 보안설정이 있을 수 있다. 공격코드에 포함된 내용이 SP 2 까지 적용된 내용이 있어서 Hotfix 를 설치 했을 경우에도 문제가 발생할 수 있으므로 주의를 기울여야 하며 가장 근원적인 대책은 확장자에 대한 삭제 및 Unicode 공격으로부터 안전한 웹 사이트 보안이 되겠다.

HotFix: 2000에서 ServicePack 1 과 Service Pack 2 는 기본적으로 설치 할 것을 권고 . MBSA Tool 을 이용하여 설치 안된 Hotfix 의 설치를 권고한다. 특정 문제점에 대한 것들만 기술하면 아래와 같다.

Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise Q321599
http://www.microsoft.com/windows2000/downloads/security/q321599/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3Freleaseid%3D39224%26redirect%3Dno

Debug 기능을 이용한 로컬 exploit Fix ?q320206 2002.5.22
Authentication Flaw in Windows Debugger can Lead to Elevated Privileges
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-024.asp

Cumulative Patch for Internet Information Services (Q319733) 2002.4.11
Htr overflow 및 ASP 의 Chunked encoding , Cross Site scripting 의 이용 가능한 취약점을 패치 한다. ASP 의 Server Side Include 의 버퍼오버플로우 문제도 해결이 가능하다. 중국내 그룹에 오버플로우 코드 확인 되었슴.
http://xfocus.org

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/secur

ity/bulletin/MS02-018.asp

ida, idq 등 index server 에 대한 보안 사항
Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

보안사항은 각 서버마다 다르므로 HFNETCHK 와 URLScan 을 다운 받아서 설치할 것을 권고.

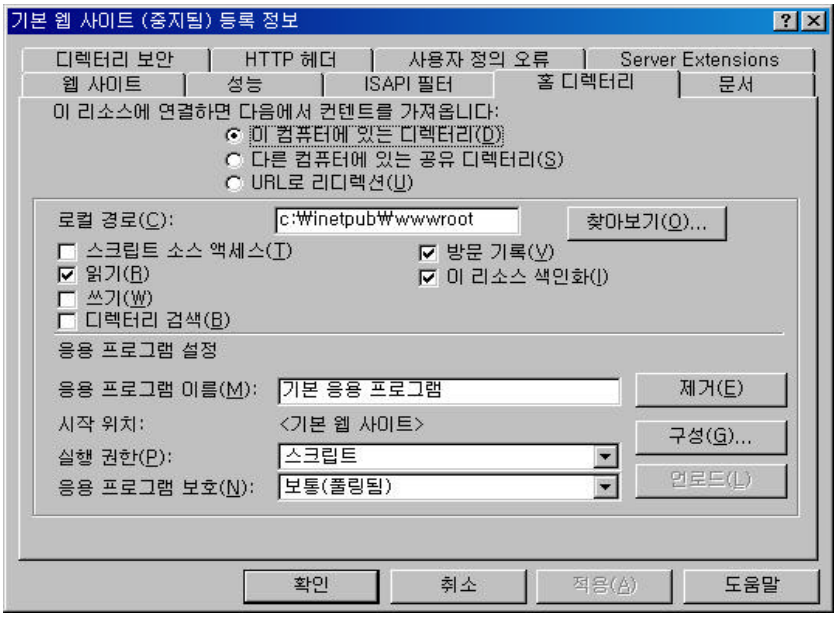
HFNetchk.: 설치 안된 Hotfix 목록을 정리해준다.
http://www.microsoft.com/downloads/release.asp?ReleaseID=31154&area=search&ordinal=39

URLScan : IIS Security 를 Default 로 강화. 확장자에 대한 필터링 가능
http://www.microsoft.com/downloads/release.asp?ReleaseID=32571&area=search&ordinal=67

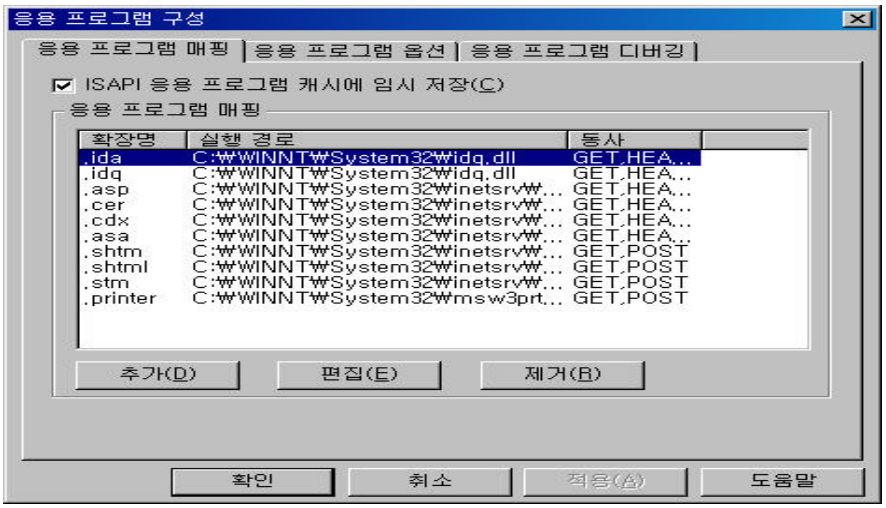
URLScan 사용설명자료는 이곳:
http://www.bizsecure.co.kr/download/tool/Urlscan.pdf

그러나 ServicePack2 까지의 공격코드로 미루어 볼 때 Security Update를 했을 경우에도 문제가 있을 수 있으므로 다음과 같은 조치사항을 실시한다.

웹사이트 등록정보.



구성 메뉴 선택



ISAPI Link 부분에서 확장자가 링크 되어 있는 것을 삭제해야 된다. 기본적으로 .ida , .idq , .Shtm ,.Shtml ,.Printer 확장자를 선택 후 삭제한다. .Shtm ,.Shtml 은 SSI (Server side include) 오버플로우 시키는 공격에 이용되므로 삭제 권고.

✍✍Exchange Server 와 연동하여 Index Server 기능을 사용하는 곳은 .ida , .idq 확장자를 삭제 하여서는 안되며 상황에 따라 설정할 것을 권고한다.

==========

✍✍FrontPage Server Extension의 제거
현재 이용되고 있는 것으로 추정되는 것은 fp30reg.dll 의 Overflow 이다. 이 것은 웹 디렉토리에서 *vti_bin* 디렉토리의 삭제와 Program Files 밑에서 검색을 하면 fp30reg.dll 이 있는 위치가 나오는데 이 파일에 대한 삭제가 되어야 한다. 이외에도 다수의 취약점이 있으나 현재 문서에서는 여기까지 기술한다. 다음 웹 서버 보안문서를 기대하자. ^^;

NT ,2000 시스템에서의 관리자와 웹 서버 관리자 , 보안정책 수립자 , 보안 담당자, 보안 컨설턴트 는 이 곳에 설명되어 있는 내용을 이해하여 침해로부터 안전한 환경을 구현하여야 할 것이다.

다음 문서 예정:

✍✍최근 해킹 분석 (역 해킹에 의한 분석) ?이 문서를 기획하던 중에 갑작스럽게 지금의 문서가 나오게 되었다. ^^; 역 해킹은 법에 걸리나 모르겠다 아시는 분 답 주시길. 나에게 공격이 들어온 서버였는데. ^^;

✍✍Windows Security Setting

✍✍Web Server Security

✍✍쓰고 싶어 지면 문서로 만들 듯.

ETC:

✍✍Self Check Tool 및 최근 보안 취약점들을 A,B,C Class 대역에 관계없이 일괄적으로 점검할 수 있는 점검툴을 만들고 공개할 예정이다.

✍✍Perl로 만들어진 초 간편 점검 스크립트 및 Exploit 도 생각나면 공개.

뭐든지 정해진 것은 없다. 하고 싶을 때 할 뿐.

29번째의 생일인 8월29일을 자축하며..

--
소심하고 안정적인 상태의 성공을 바라기 보다는
거대하고 야심찬 꿈의 실현에서의 실패를
나는 바라노라. - 절망의 바다에서
--