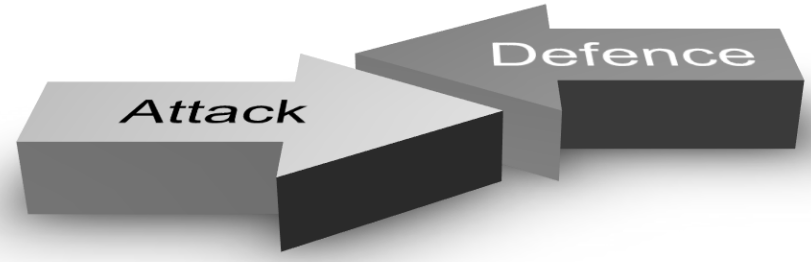
Eyeon Security

Information security company

실시간 웹쉘 및 악성URL 탐지 / 방어 솔루션

쉘모니터 (ShellMonitor)

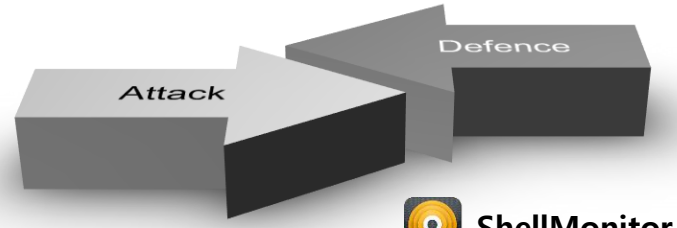


2015.05

IT Business Partner ㈜아이온시큐리티

Eyeon Security
Information security company

목 차



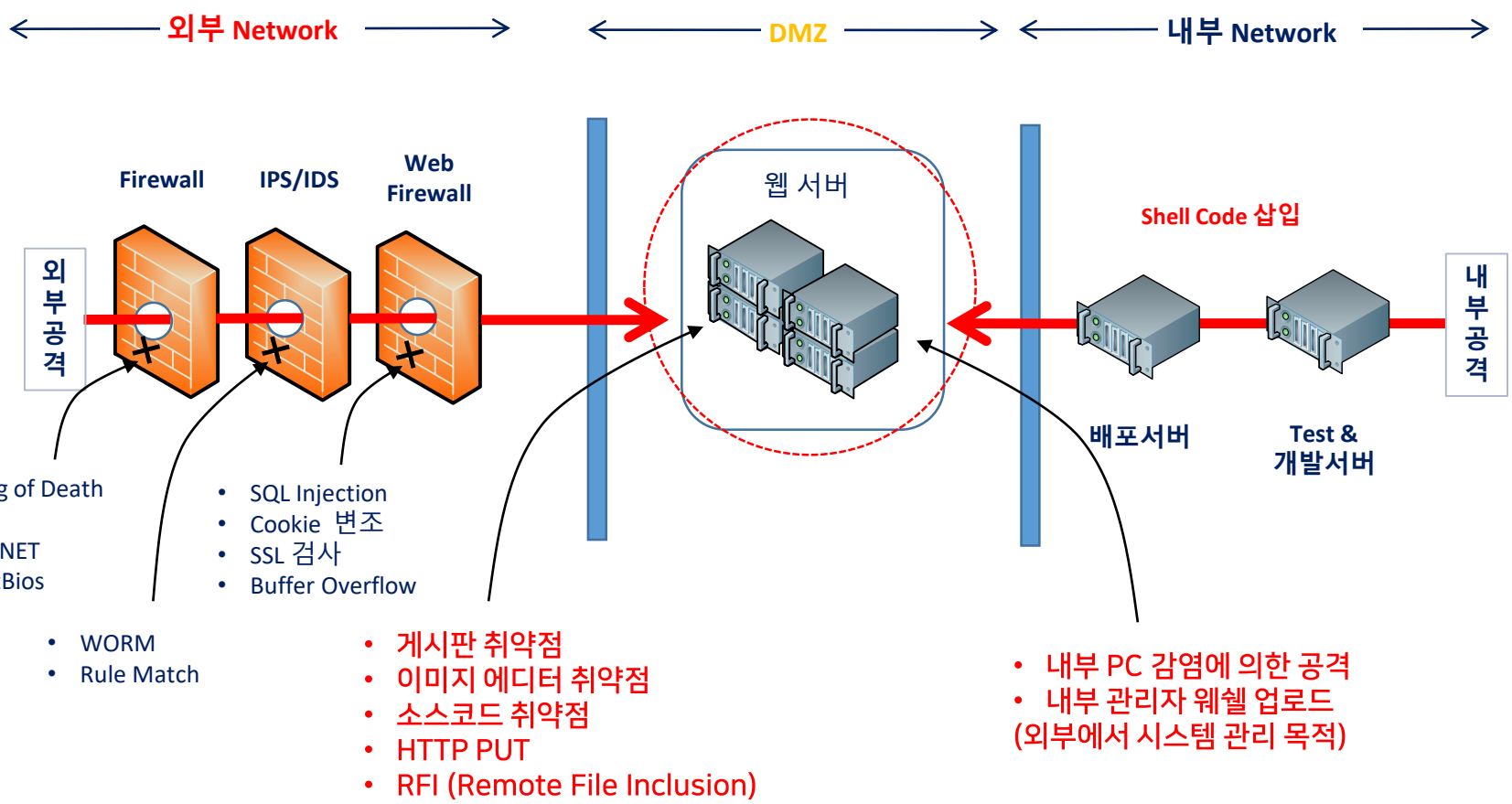
ShellMonitor

1) 웹쉘 위험성

웹쉘은 원격에서 대상 웹서버에 명령을 수행 할 수 있도록 작성한 웹스크립트 (asp, jsp, php, cgi) 파일로, 웹을 이용하여 시스템 명령어를 수행하므로 방화벽의 영향을 받지 않고 서버 제어(방화벽이 접근을 허용하는 웹서비스 포트/80Port를 이용)를 할 수 있습니다. 이러한 웹서버 악성코드의 공격을 통하여 공격자는 웹페이지 소스코드를 열람하거나, 서버의 파일 및 데이터 베이스 자료를 불법적으로 탈취하며, 악성코드 유포지URL 또는 악성스크립트(iframe)을 삽입을 통해 웹에 접속하는 고객 PC에 대량으로 악성코드를 유포시켜 DDoS 공격의 원인이 되기도 합니다.

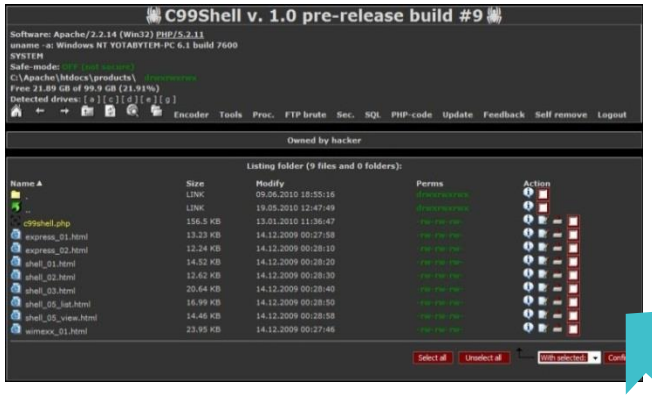
√ 시스템 명령어	✓ 네트워크 명령어	✓ 시스템 파일 접근	√ DB 접근	√ 사용자 PC
' 시스템 정보 열람 ' 시스템 Shutdown ' 특정프로그램 정지/삭제 (Anti-virus 프로그램 등)	' 포트 스캐너 ' TELNET, SSH, FTP 접속 (내부 네트워크 접근 가능)	' 해킹 툴 업로드 (키로그, 백도어) ' 파일수정(악성코드삽입) ' 시스템 파일 삭제 ' 모든 시스템 디렉토리 열람	' 데이터 유출, 변경, 삭제	' 악성코드 감염 ' 데이터 유출 ' 관리자의 주요 시스템 접속정보 유출 ' DDoS 공격 유발

2) 웹쉘 침투경로

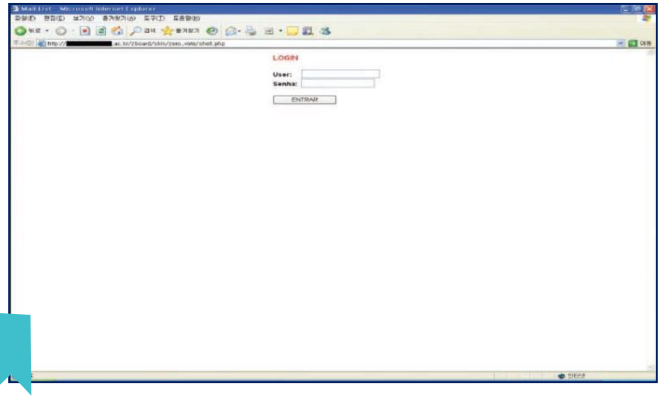

외부 Network
DMZ
내부 Network
Firewall
IPS/IDS
Web Firewall
웹 서버
Shell Code 삽입
외부공격
내부공격
배포서버
Test & 개발서버
• Ping of Death
• FTP
• TELNET
• NetBios
• SQL Injection
• Cookie 변조
• SSL 검사
• Buffer Overflow
• WORM
• Rule Match
• 게시판 취약점
• 이미지 에디터 취약점
• 소스코드 취약점
• HTTP PUT
• RFI (Remote File Inclusion)
• 내부 PC 감염에 의한 공격
• 내부 관리자 웨쉘 업로드
(외부에서 시스템 관리 목적)

2) 웹쉘의 진화

① 기본형 : 파일/디렉토리 조작, DB 조작 등

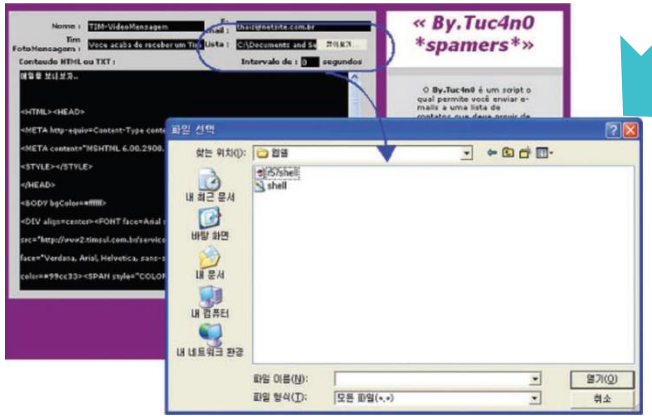


② 암호가 설정되어 업로드 한 사람만 조작 가능

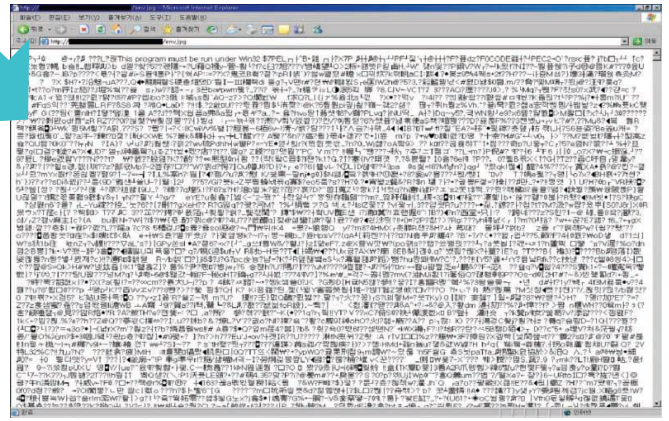


악성코드는
계속 진화하고
발전함

③ 변종 : 기존 웹서버 악성코드를 수정하여 기능 추가

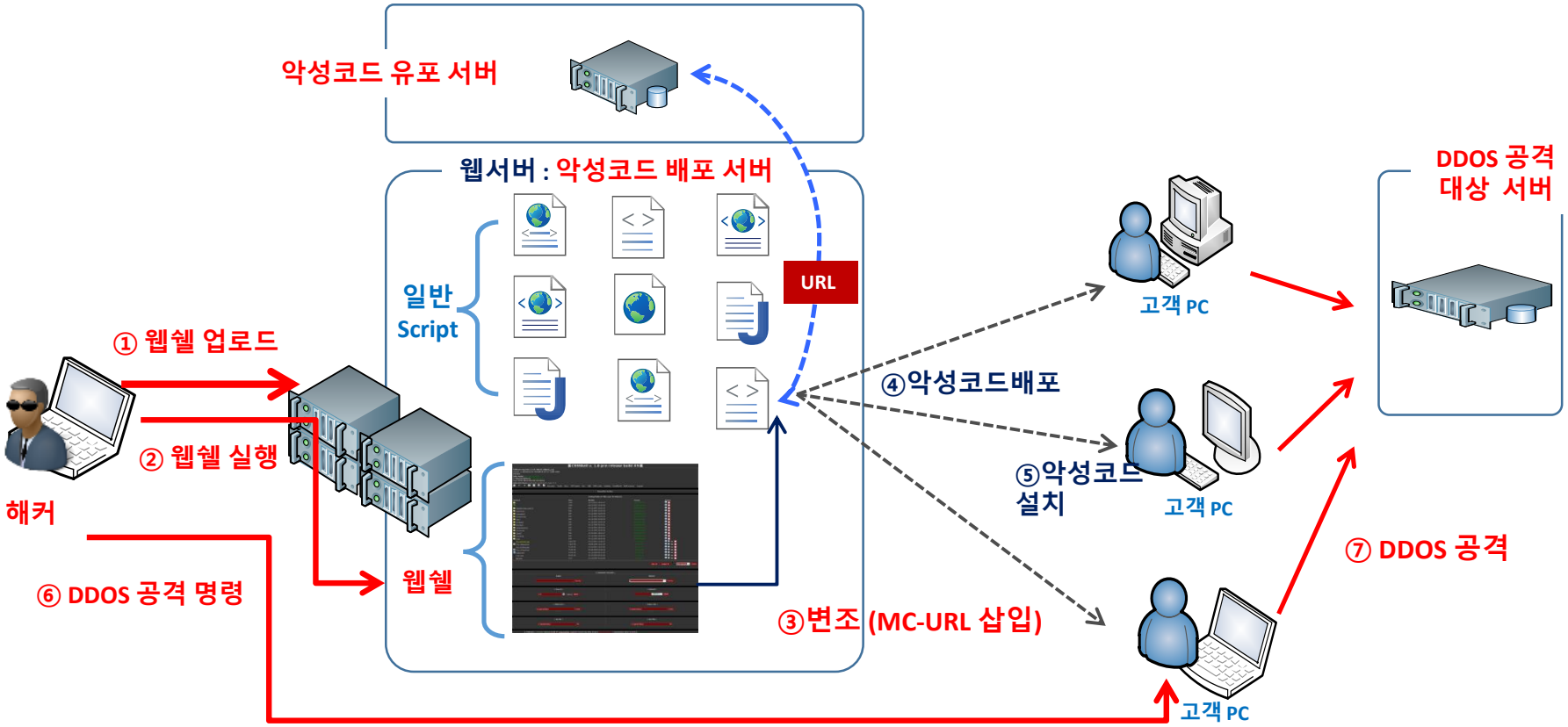


④ 암호화 된 웹서버 악성코드



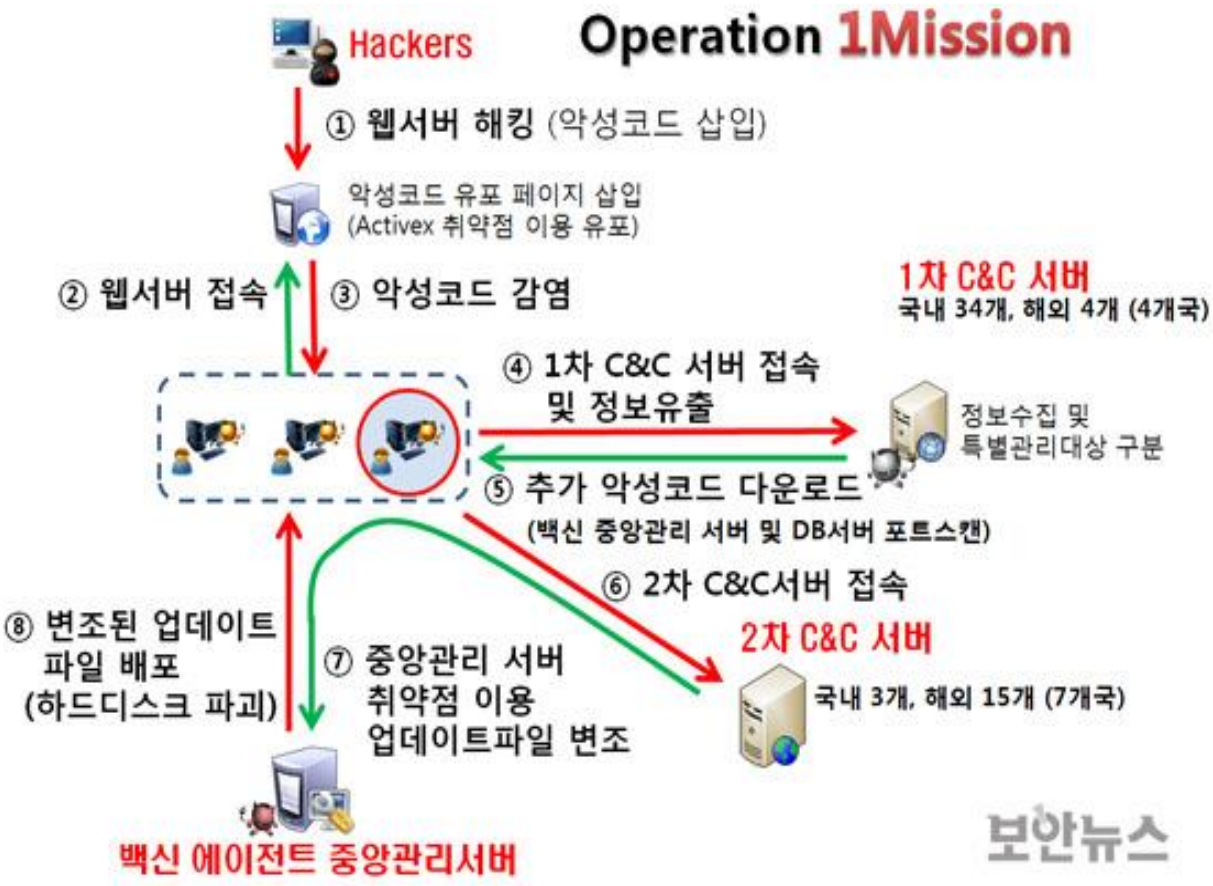
1) 웹쉘을 통한 DDoS 공격

- 2011년 3월 4일 DDoS 공격 추정.



2) 3.20 사이버테러 내부 침입 경로

- 악성코드 유포 진원지 및 은닉용 경유지 49개 확인
- 2012년 06월부터 해킹진행
- 악성코드 76종 확인
- 1차 Base64로 엔코딩된 웹쉘을 기 사작성 웹서버에 침투 => 백신업데이트 서버를장악 => 내부업무 포탈에 악성코드 은닉 => 내부에서 외부로 접속하여 서버관리자 PC 악성코드삽입 => DB삭제
- 2차 날씨닷컴 사이트
- 3차 YTN(웹=>개발서버=>내부서버)
- 4차 대북보수단체 홈페이지



*** 2013년 04월 09일 보안뉴스 기사 참조**

3) 주요 해킹사례

발생시기	업체명	피해 사례	해킹 원인
2008년 01월	**옥션**	**1,863만명** 고객 정보 유출	**웹쉘**
2011년 03월	**3.3 DDoS 대란**		**웹쉘** 및 악성URL
2011년 05월	**현대캐피탈**	**175만명** 고객 정보 유출	**웹쉘**
2011년 07월	**네이트**	**3,500만명** 고객 정보 유출	악성URL
2012년 05월	**EBS 교육방송**	**400만명**(추정) 고객 정보 유출	**웹쉘**
2013년 03월	**3.20 사이버테러**	**방송사** (KBS·MBC·YTN 등) **금융기관** (농협·신한·제주은행·NH생명보험·NH손해보험 등)	웹쉘 및 악성URL을 이용한 보안 Activex를 가장한 악성코드 유포
2013년 06	**6.25 사이버테러**	새누리당 250만명·군장병 30만명·청와대 20만명 신상정보 유출 우려	WAS 취약점 혹은 게시판 글쓰기를 통한 파일 업로드 및 다운로드 취약점 이용한 웹쉘 삽입

4) 웹서버 악성코드 관련 기사

[특집] 웹해킹의 시작은 '웹쉘'로부터

2011.06.02 [이데일리 시큐리티]
펜타시큐리티시스템 사업기획부 박재홍 과장

"해킹 당한 웹서버 중 웹쉘이 발견된 웹서버는 총 91%"

웹쉘이 설치되면 해커는 보안 시스템을 우회하여 별도의 인증 절차 없이 피해시스템에 손쉽게 접속하는 것이 가능하다. 접속한 피해시스템에서 임의의 명령어를 실행해도 보호 조치가 힘든 상태라고 보면 된다. 아울러 피해시스템의 파일을 수정, 복사, 삭제와 같은 시스템 제어가 가능하고, 웹소스 코드에 악성 스크립트를 삽입하여 해당 웹서버에 접속한 일반 사용자들의 PC를 공격하거나 피해시스템과 연결된 데이터베이스의 정보도 유출할 수 있는 등 매우 큰 피해를 입힐 수 있는 도구이다.

웹쉘에 의한 국내 사이트들의 피해
인터넷침해대응센터(www.krcert.or.kr)에서는 해킹 당한 웹서버 중 웹쉘이 발견된 웹서버는 총 91%의 분포를 보였다고 한다. 웹 취약점을 발견 후 해커들은 제일 먼저 웹쉘을 설치하고, 다음 순서로 웹서버의 시스템 권한을 획득하는 순서로 진행된다. 이후 해커는 웹쉘을 이용하여 해킹한 로그 및 흔적을 지우는 과정을 수행한다. 이렇게 되면 웹쉘 접속 시 해커의 웹브라우저에 원격으로 윈도우탐색기가 실행되는 것과 비슷한 상태가 된다. 필자는 예전 웹 방화벽 엔지니어로 근무할 때 종종 고객 웹서버에 웹쉘이 설치된 광경을 보고 놀라지 않을 수 없었다. 실제로 웹쉘은 적합한 보안 제품을 이용하지 않으면 탐지가 어렵기 때문에 해킹에 광범위하게 사용되고 있다. - 하략 -

중국 해커들이 비번 보고 있다. 웹셸 '충격파'

2011.04.19 [전자신문] 장윤정기자

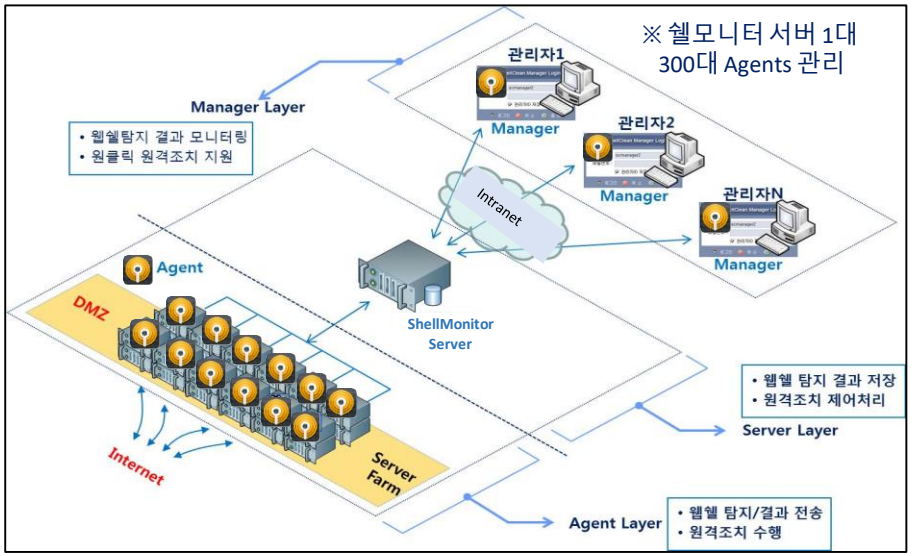
"사이트당 300만원만 주면 개인정보 열람 권한을 넘겨주겠다."

지난 18일 오후 전자신문 기자와 국내 해커 A씨(22)가 중국 QQ 메신저에 접속하자 '007'이라는 닉네임의 중국 해커가 파격적인 제안을 했다. 그는 국내 모 채팅사이트 사용자의 인적사항과 비밀번호 데이터베이스(DB)를 가지고 있다고 자랑했다.

신원불상의 중국해커가 국내 20여개 이상의 사이트에 웹쉘 등을 심어 개인정보를 거래하겠다고 제의하는 인터넷채팅 화면
"못 믿겠다. 사실관계를 증명하라"고 메신저를 입력하자 그는 그 사이트에 접속해 회원가입하면 바로 비밀번호를 맞혀 보겠다고 했다. 취재진이 설마 하는 마음으로 회원에 가입하자 그 중국 해커는 단번에 '비밀번호'를 맞혔다.

-하략-

1) 제품 개요

제품명	쉘모니터 (ShellMonitor)
버전	ShellMonitor v2.0
출시 연/월	2010년 06월
제조사(국명)	㈜유엠브이기술 (대한민국)
솔루션 구조	

1) 제품 개요 (상세)

쉘모니터(ShellMonitor)는 웹서버 파일시스템의 변동을 실시간으로 인지하여 실시간 삽입되는 웹서버 악성코드 및 악성코드 유포지URL을 여부를 즉시 검사하고, 관리자에게 통보하여 검역 조치 합니다.

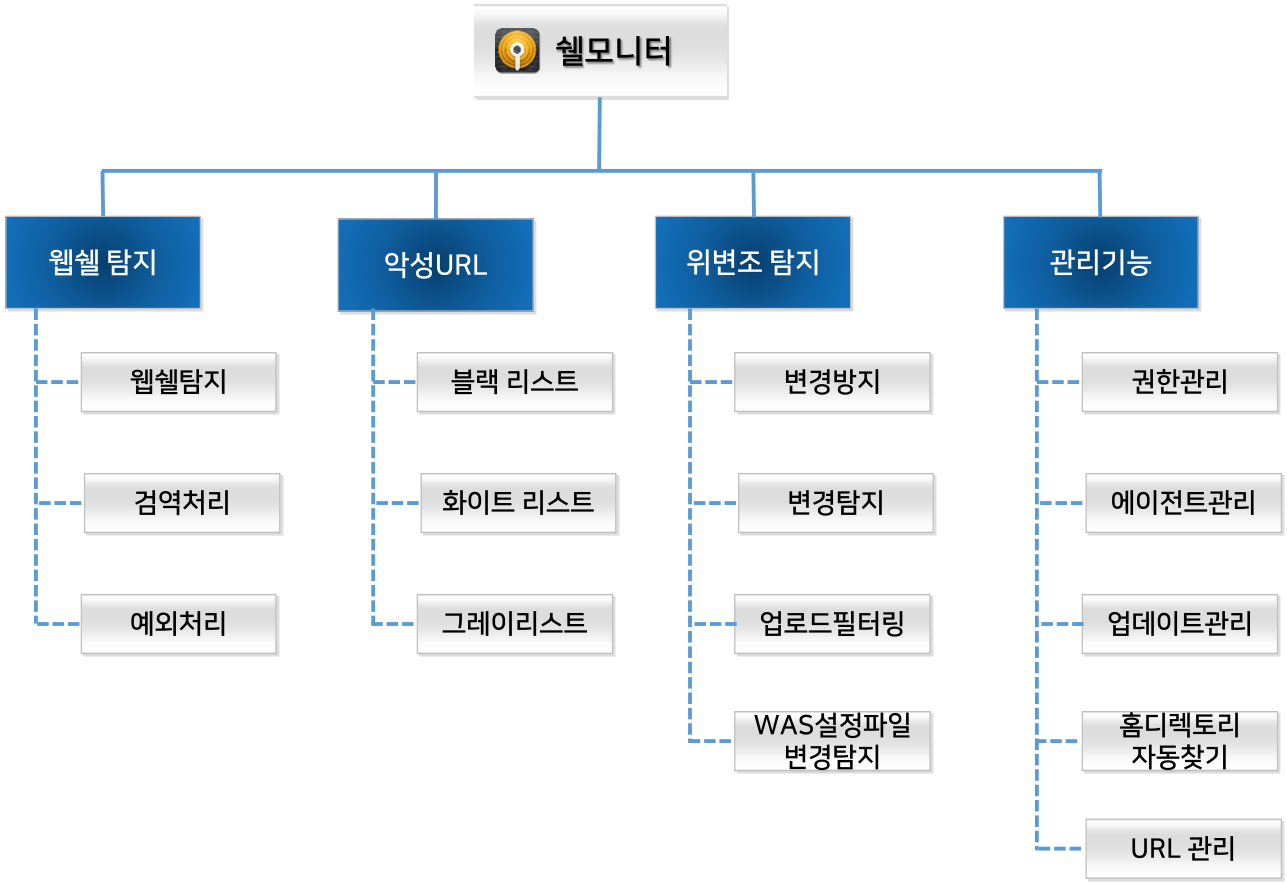
√ 웹쉘 및 악성코드 유포지URL 실시간 탐지 / 검역 조치
√ 대규모 웹서버를 위한 중앙집중식 관리지원 및 자동 업그레이드 지원
√ 소스파일 변경방지, 임계치 설정에 의한 파일변경 탐지
√ 악의적인 권한변경에 대응하는 웹서버 설정파일 변경탐지
√ 업로드 필터링, E-Mail/SMS/ESM 연동 기능, 자원 모니터링 기능 제공

쉘모니터(ShellMonitor) 탐지/조치 절차

2) 특장점

실시간 탐지	• 웹 어플리케이션 파일의 임의 생성 및 변조를 실시간으로 탐지 하는 기능 • 임의 생성 및 변조 즉시 탐지 하고 처리 가능하여야 함.
웹쉘 패턴	• ASP, JSP, PHP 등 다양한 웹 스크립트 탐지 지원 • 지속적인 R&D를 통한 최신/진화하는 웹쉘 탐지 패턴 보유
엔터프라이즈 환경 지원	• 엔터프라이즈 환경에 대응하는 운영 방식 제공 • 대량의 웹 서버 중앙 집중 관리 가능 • ESM(Enterprise Security Management) 연동 지원
서비스 지향성	• 쉘모니터 에이전트에 의한 웹 서비스에 미치는 영향 최소화 • 서버 자원(CPU 및 메모리) 제어 가능

3) 기능 구성도


쉘모니터
웹쉘 탐지
악성URL
위변조 탐지
관리기능
웹쉘탐지
검역처리
예외처리
블랙 리스트
화이트 리스트
그레이리스트
변경방지
변경탐지
업로드필터링
WAS설정파일 변경탐지
권한관리
에이전트관리
업데이트관리
홈디렉토리 자동찾기
URL 관리

4) 기능 리스트

주요기능	• 탐지 방법 및 대상	전체 탐지	탐지 대상 디렉토리 내의 모든 파일 탐지
		실시간 탐지	실시간 변경 파일 탐지
		탐지 대상	웹쉘, 악성코드유포지URL, 개인정보, 웹서버 설정파일
	• 탐지내역 조치	검역 조치	탐지된 웹쉘 검역
		부분 검역	탐지된 악성코드유포지 URL 부분 검역
		자동 검역	잘 알려진 웹쉘(약 400개 이상) 자동 검역
		예외 조치	탐지된 파일 예외 조치
부가기능	• 악성코드 유포지 URL 관리	GRAY LIST	탐지된 모든 URL
		BLACK LIST	악성코드 유포지 URL
		WHITE LIST	사용되는 URL
	• 업로드필터링		업로드파일 탐지
	• 파일 변경방지		파일 변경 방지
	• 파일 변경탐지		변경된 파일 탐지
	• 홈디렉토리 자동찾기		Web Root 디렉토리 자동 찾기
	• 웹서버 파일 설정 관리		웹 서버 설정 파일 변경 탐지
	• DB서버 탐지		개인정보, 웹쉘
관리기능	• 탐지알림		관제화면 알림, email, SMS, ESM 연동
	• 권한 관리		계정 및 사용자 권한 관리
	• 기타 기능		통계 및 리포팅, 시스템 자원 사용율 모니터링

5) 솔루션 세부기능 소개

관리서버 기능	. 많은 에이전트 중앙에서 효율적인 관리 지원 (패턴/에이전트 업데이트, 탐지내역 중앙 관리, 탐지규칙 적용 등)
패턴 내용	. 정규 표현식을 사용한 유사/변형 악성코드 탐지 . 휴리스틱(Heuristic) 코드분석을 통한 탐지 패턴에 없는 위험 패턴 탐지 . 알려진 웹쉘의 시그니처를 이용한 자동 검역 지원
부가기능	. 홈페이지 위변조 탐지/방지 기능 제고 - 소스코드 위변조 탐지 방지 - 소스코드 형상관리 제공
솔루션 자체 보안 방안	. 인증서 발행/인증 방식을 통한 에이전트와 서버 구간 보안 강화 . 관리서버 H/A 구성으로 365일 무중단 서비스 . 시스템(O/S) 및 DBMS에 대해 KT, SKT, 삼성으로부터 취약점 점검 완료

1) ㈜유엠브이기술 소개

“ 통합 웹서버 보안 - 악성코드(웹쉘) / 악성 URL /개인정보/ 홈페이지 위변조탐지 & 방어 솔루션 쉘모니터” 개발기업

- 국내외 최초로 상용 웹 악성코드(웹쉘) 탐지 솔루션 “쉘모니터(ShellMonitor)” 개발
- 삼성 Group,한국통신(KT), SK ,BC Card,안철수 연구소 보안관제 서비스 등에 납품 기술력이 검증된 기업
- “웹쉘탐지”를 시작으로 “악성URL 탐지”,” 개인정보(File &DB)탐지”, “홈페이지 위/변조탐지” 등을 실시간으로 탐지 처리 가능한 통합 웹서버 보안솔루션 개발
- GS 인증 획득 (Certificate No.: 11-0184) –TTA
- CC 인증획득 (Certificate No.: ISIS-0376-2012) – 국정원
- “실시간 웹쉘 탐지 및 방어 시스템 및 방법” 및 “파일의 위변조 탐지 시스템 및 그 방법” 포함 5건 특허 취득

회 사 명	㈜유엠브이기술 / UMV Inc.
대표 이사	방윤성
설 립 일	2008년 2월27일
주 소	서울시 서초구 양재동 316-6 흥아빌딩 2층
연락처	02-448-3435 / http://www.umv.co.kr

2) 주요 고객사

No.	부문	고객사	비고
1	공공	청와대	
2		서울특별시청	
3		대검찰청	
4		서울특별시 보라매병원 (서울시 산하병원)	
5		한국과학기술정보연구원 (KISTI)	
6		공무원연금공단	
7		문화재보호재단	
8	금융	외환은행	
9		산업은행	
10		BC카드	
11		푸르덴셜 생명	
12		코스콤	
14		한국거래소(KRX)	
15		현대라이프	인터넷 뱅킹
16		현대 캐피탈, 현대카드, 현대커머셜	인터넷 뱅킹
17	기업	SKT	
18		KT	
19		삼성그룹	삼성 전 계열사
20		ebay코리아 (지마켓, 옥션)	
21		GS칼텍스	
22		SBS컨텐츠허브	

Eyeon Security

Information security company

감 사 합 니 다.