WSS:
The Essentials

+82 2 448 3435
서울특별시 서초구 마방로2길 84 (포엠아이2빌딩) 4층
umvwebsecurity.com

2025.04.19

SKT 유심 해킹

이미지출처: NewsWay

2022년 6월, SK텔레콤 서버에 최초로 웹쉘이 몰래 심어졌으며, 2025년 5월에 들어서야 발견.

이 웹쉘를 이용하여 정교한 백도어 멀웨어인 BPFDoor 악성코드가 HSS서버 감염되었으며, 총 25종의 악성코드가 SKT 내부시스템에서 발견됨.

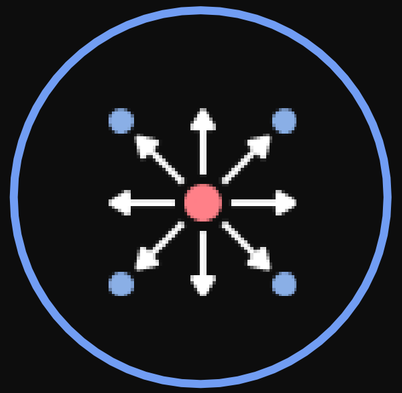
사용자 데이터를 저장하는 서버도 감염되었으며, 약 2,500만 명에게 영향을 미침.

출처: 조선
출처: 과학기술정보통신부

SKT 해킹 과정

피싱이나 웹 서버 취약점을
이용해 SKT 웹서버에 침투

웹서버에 침입한 뒤, 웹쉘을
업로드하여 SKT내부시스템에 대한
APT
공격을 위한 권한 확보



점차 권한을 상승시키고
네트워크 내부로 이동

결국, 텔레콤 인프라의 핵심인
HSS 서버에 침투하여 정보를
탈취

출처:The Elec
Sygnia
KBS

2024.09.12

이미지출처: SBS뉴스

모두투어 악성코드에 고객정보 유출

"…홈페이지에 악성코드가 들어가 회원 정보와 비회원으로 예약 시 입력된 정보 일부가 유출됐다"고 공지를 통해 밝혔다.

공지에 따르면 악성코드 삽입 시점은 올해 6월이다. 유출 정보는 한글·영문 이름, 아이디, 생년월일, 휴대전화 번호, 중복정보 등인 것으로 전해졌다. 유출 범위는 정보 주체에 따라 상이하다.

모두투어는 유출 사실 인지 후 악성코드를 즉시 삭제했다고 했다. 또 외부에서 접속된 IP를 차단했으며 홈페이지 취약점 점검과 보완 조치를 완료한 상태"라며 "침입방지시스템, 웹방화벽, 웹쉘 탐지시스템 등 보안장비 수준을 높였다"고 밝혔다. "

출처: ZDNET

2024.07.26

이미지출처: Rewards for Justice

“美 국무부가 현상수배한 北해커, 어떻게 NASA 뚫었나 봤더니…”

“… 림종혁은 미국 의료보험사와 항공우주국(NASA), 군사기지 등 미국 내 11개주의 17개 기관을 공격하는데 관여한 혐의를 받는다. 또 미시간과 캘리포니아 방산기업 컴퓨터 시스템과 텍사스·조지아 공군기지에도 접근한 것으로 드러났다.”

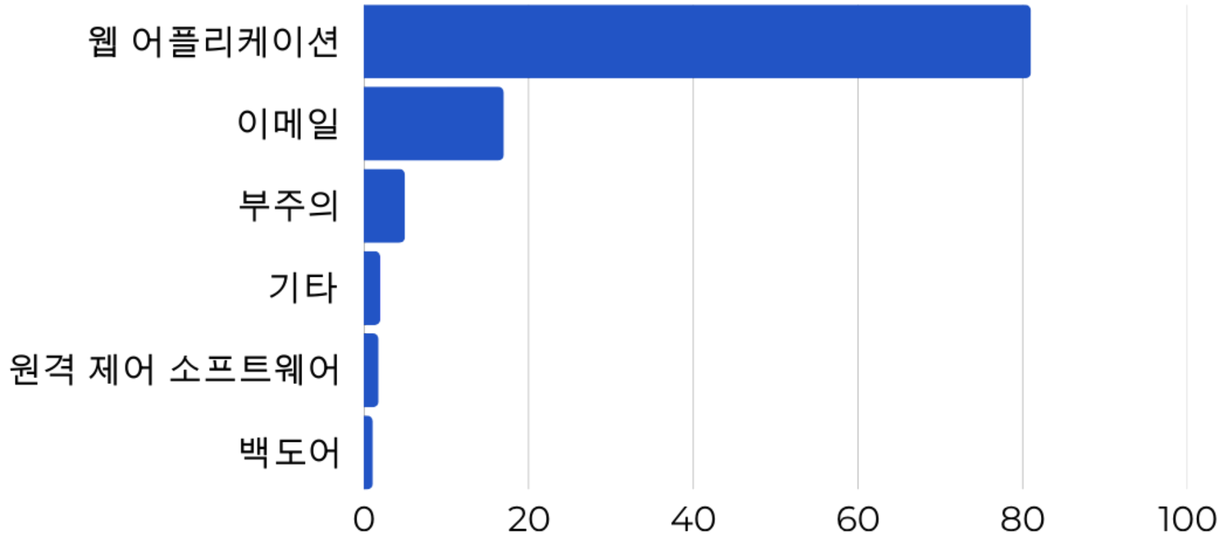
“ … 안다리엘은 평양과 신의주에 기반을 두고 있는 북한 정찰총국 3국 산하 국가배후 해킹조직이다.”

“… 안다리엘은 로그포제이(Log4j) 등 알려진 취약점을 악용해 웹 서버에 광범위한 공격을 자행하고 있다. 이를 통해 웹 서버에 설치된 악성 스크립트 파일인 '웹쉘'을 유포하고, 중요 정보와 응용 프로그램에 접근해 추가적인 공격을 진행한다.”

“… 한·미·영 보안당국은 주요 인프라 조직에 취약점 패치를 적시에 적용할 것을 권고한다. 아울러 웹쉘로부터 웹 서버를 보호, 악성 활동에 대한 엔드포인트를 모니터링, 인증· 원격 접근 보안 강화를 권장한다.”

출처: 뉴시스

웹 서버 해킹의 증가



2020년 8월부터 2021년 1월까지 매월 평균 140,000건의 웹쉘을 이용한 공격 발생 횟수를 기록했으며, 해마다 두배 이상 증가했습니다. [1]

또한, 2022년에 약 80%의 보안 사고는 웹어플리케이션을 통해 일어났습니다. [2]

2024년 4분기 사고 보고를 따르면 35%의 보안 사고에서 웹쉘이 취약한 웹 어플리케이션을 침투하기 위해 사용됐습니다. [3]

출처: [1] Microsoft Security Blog
[2] Verizon 2023 DBIR
[3] Cisco Talos Incident Response Trends

웹쉘

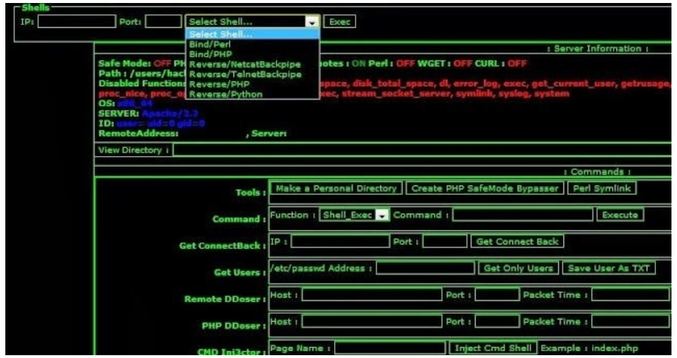
웹쉘이란 웹 서버에 침투하여 , 루트 권한을 가지고 공격자가 원격으로 서버를 제어할 수 있게 하고 지속적인 접근을 통해 악의적인 공격을 가능하게 해주는 악성코드입니다.

방화벽이나 IDS/IPS 같은 Network 보안장비는 웹쉘을 효과적으로 잡지 못합니다.

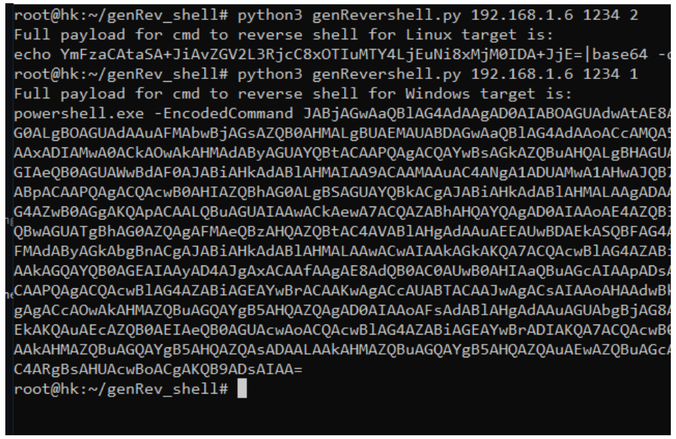
웹쉘은 인코딩되고, 쪼개져서 들어오는 경우에는 기존 장비로는 탐지하기가 매우 어렵습니다.

따라서 웹쉘은 사이버 해커들에게는 인기 있는 해킹도구가 됩니다. 한 번 성공적으로 심어진 웹쉘은 시스템에 대한 장기적인 백도어 접근을 제공합니다.

웹쉘은 추가적인 피해와 침해를 가하는 완벽한 APT공격의 도구가 됩니다.



이미지출처: Shreshta Blog



이미지출처: GitHub

WSS

WSS는 웹쉘이 웹서버에 침투되는 즉시, Real Time으로 제거합니다.

실시간 탐지 및 대응

WSS는 FIM(File Integrity Monitoring)과 유사한 기능에 실시간 격리 기능을 결합하여, 웹쉘 스크립트가 웹 서버에 업로드되는 순간 즉시 탐지하고 격리합니다.

높은 탐지율

패턴, 해시값, 시그니처, 알고리즘 기반의 탐지 방식을 통해 높은 탐지율과 정확도를 자랑합니다.

WSS: 사이버해킹의 마지막 방어선

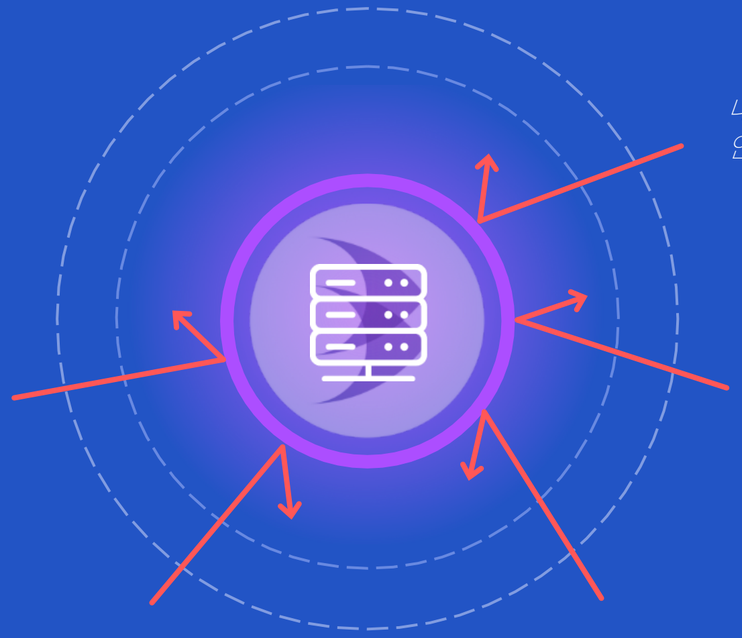
개념은 간단합니다:

웹 엎프리케이션은 약 80%의 데이터 침해 사고에서 주 대상입니다.

웹 서버단에서 악성코드를 차단하여 대부분의 침투형 사이버 공격을 효과적으로 방어할 수 있습니다.

WSS는 이 역할을 수행하며, 침해가 본격적으로 시작되기 전에 최후의 방어선을 제공합니다.

출처: Verizon 2023 DBIR



WAF면 웹쉘이 해결되지 않나요?

웹쉘 탐지율

WAF(Web Application Firewall)은 네트워크 DMZ단에서 트래픽을 검사하여 웹 어플리케이션을 보호하는 네트워크 장비입니다.

WAF는 한정된 웹쉘 패턴을 가지고 있어 일부 웹쉘을 탐지할 수 있지만, 암호화된 웹쉘은 탐지가 어렵고, 기존에 내부에 존재하고 있던 웹쉘은 발견하기가 힘든 상황등 여러가지 한계로 인하여 웹쉘 탐지 효율이 낮습니다.

SKT, 북한의 NASA 해킹, MOVEit 악용 사례 등 유명한 웹쉘 기반 데이터 유출 사건은 WAF가 운영되고 있었지만 해킹사고가 발생했습니다.

*탐지율과 사양은 제품마다 다를 수 있습니다

EDR도 웹쉘탐지 하지 않나요?

서버 EDR은 데이터 수집 및 행동/이상 기반 탐지를 사용하여 서버, PC 및 기타 엔드포인트에서 의심스러운 활동을 감지합니다.

서버 EDR은 광범위한 탐지 범위를 제공하지만, 그 결과로 자원 소모가 많고 비용이 높습니다.

행동 기반 탐지는 정확도에 문제가 있으며, 피해 가 발생한후에 탐지됩니다.

*EDR = Endpoint Detection & Response

경량화된 퍼포먼스

WSS는 자원 소모를 최소화하여 (≤1% CPU로 작동 가능), 안정적인 웹 서버 서비스를 보호해줍니다.

실시간 탐지

WSS는 웹 서버의 파일 시스템에서 웹쉘 스크립트를 발견하는 즉시 탐지하고, 피해가 발생하기 전에 실시간으로 격리합니다.

케이스 스터디

Hyundai Card

[개요]
웹쉘로 인한 해킹 사고 발생함으로 당사로 직접 Contact 진행하여 당사에서 WSS를 통해 유입된 웹쉘을 모두 탐지하여 조치 완료.

[향후 진행 사항]
탐지 및 조치 완료와 동시에 계약 진행 완료
한번 해킹 된 곳으로 하루에도 몇십개의웹쉘이 업로드가 되었음에도 WSS를 통해서 탐지 및 조치하여서 해킹 피해에 대응함.

kobaco
한국방송광고진흥공사

[개요]
국정원 감사에서 파일 보호 항목에 미흡 판정을 받게 되어 웹쉘 탐지 솔루션을 도입하게 됨.
비교 경쟁을 통해 WSS로 결정 후 도입 완료.

[향후 진행 사항]
비교 경쟁(메티아이, 쉘캅)을 통해서 WSS로 결정 후 도입하게 됨으로 국정원 감사에서 파일 보호 항목에 적합 판정을 받게 됨.

케이스 스터디

하나금융그룹

[개요]
기존 사용중인 메티아이(MetiEye) EOS 이슈와 유지보수 미흡, 탐지 성능 관련 이슈로 경쟁을 통해 솔루션 재 도입.

[향후 진행 사항]
제품 성능 평가, 설치 속도, 유지보수 관련 내용 평가를 통해서 WSS 제품으로 선정되어 도입.
도입 후 요청사항에 대한 대응이 빠르고 유지보수면에서 기존 제품대비 상당히 개선되었다는 평가를 받았음. 성능면에서도 기존 제품 대비 우수함 평가 받음.

SUPREME COURT OF KOREA 대법원
SUPREME COURT OF KOREA

[개요]
한국 대법원은 북한 라자루스 그룹의 해킹으로 1,000GB 분량의 법원 문서가 유출된 뒤, 2023년 초 WSS를 도입했습니다. WSS는 실시간 모니터링, AI 기반 이상 탐지, 자동화된 사고 대응을 통해 탐지 속도와 포렌식 역량을 강화하며, 운영에 지장을 주지 않는 경량 솔루션으로 평가받았습니다.

[향후 진행 사항]
대법원은 WSS의 지속적인 관리를 통해 시스템을 안정적으로 운영할 계획입니다. 또한, 추가 보안 기능 도입 및 보안 정책 강화를 통해 데이터 보호와 사이버 위협 대응력을 한층 높일 예정입니다.

레퍼런스

Web Server Safeguard (WSS)는 18여년동안 뱅킹,기업 그리고 공공기관으로부터 많은 사랑과 신뢰를 받아왔습니다.

300+
곡객사

30K+
에이전트 운영 중

10+
특허 및 인증

공공/관공서

Ministry of National Defense Republic of Korea
SEOUL METROPOLITAN GOVERNMENT
Ministry of Foreign Affairs Republic of Korea
KORAIL
THE REPUBLIC OF KOREA CHEONG WA DAE
Kdata Korea Data Agency

금융

LOTTECARD
SK securities
SAMSUNG CARD
Hyundai Capital
BC CARD
NH Bank
Hana Financial Group

기업

SAMSUNG SAMSUNG SDS
cafe24
Gmarket
S-OIL Corporation
CJ CHEILJEDANG
SHINSEGAE
GS
dun & bradstreet
ebay
Prudential
AhnLab
TOYOTA
Deloitte.
Hanwha
gabia.

Why WSS?

높은 탐지율

패턴, 알고리즘, 해시값, AI 기반 탐지 방법을 이용한 효율적이고 신뢰성 있는 실시간 탐지를 수행합니다.

경량화

WSS는 웹서버의 최소한의 리소스를 (CPU ≤ 1%)만 이용하며 웹서버 서비스에 영향을 미치지 않습니다.

자동화

WSS는 웹쉘을 자동으로 격리하고, 탐지대상인 웹서버의 홈 디렉토리를 자동으로 찾아 설정합니다.

효율성

WSS는 관리 및 운영이 용이하며 , 웹쉘 탐지에 최적화되어 있습니다.

위치

2008년 대한민국 서울에서 설립된 UMV는
전 세계 웹 보안을 강화하기 위해 유럽과 중앙아시아로
기업 활동을 확장해왔습니다

본사

Seoul, South Korea

4F FourMI2 Bldg. 84 Mabang-ro 2gil, Seocho-Gu,
Seoul, South Korea

+82 2 448 3435

현지법인

İstanbul, Türkiye

Polat İs Merkezi, Mecidiyekoy Mah., Cemal Sahir Sok.,
No:29/32, Sisli, İstanbul, Türkiye

+90 212 266 21 88

현지법인

Almaty, Kazakhstan

630, 6th Floor, Prospekt Zhibek Zholy, 50/1 Medeuskij
rajon, Almaty, Kazakhstan

+7 700 980 7428

Contact Us

"WSS, 완성된 웹보안을 위한 최적의 선택"

문의처 sales@umvglobal.com umvwebsecurity.com