

스팸 문자 무단 발송 사고 분석

PLAINBIT / 권기업 선임연구원

PLAINBIT

목차

- 왜 이 주제를?
- 스팸문자를 어떻게 보냈는가?
- 무엇을 할 것인가?

왜 이 주제를?

PLAINBIT

스팸문자의 기억

- 스팸문자는 어디서 발송될까? 얼마나 발송될까?

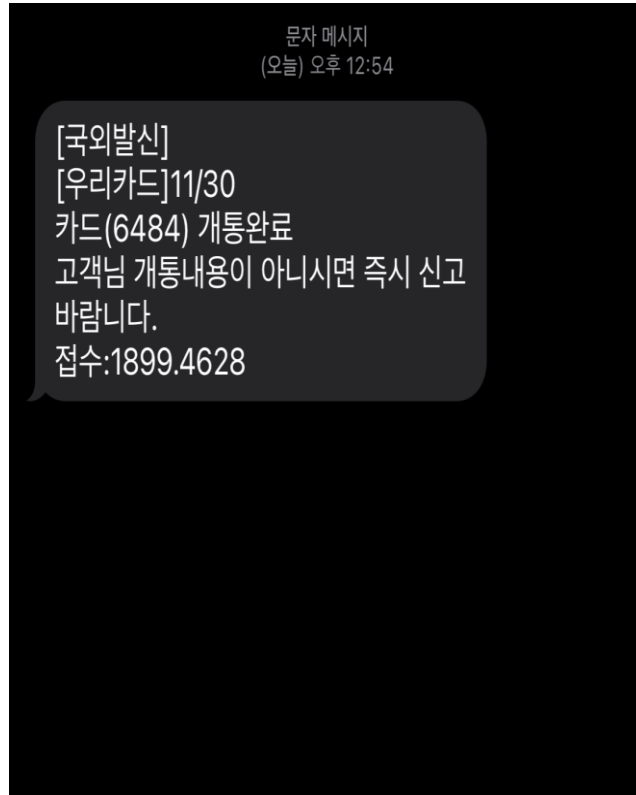


사진1. 국외 스팸 문자

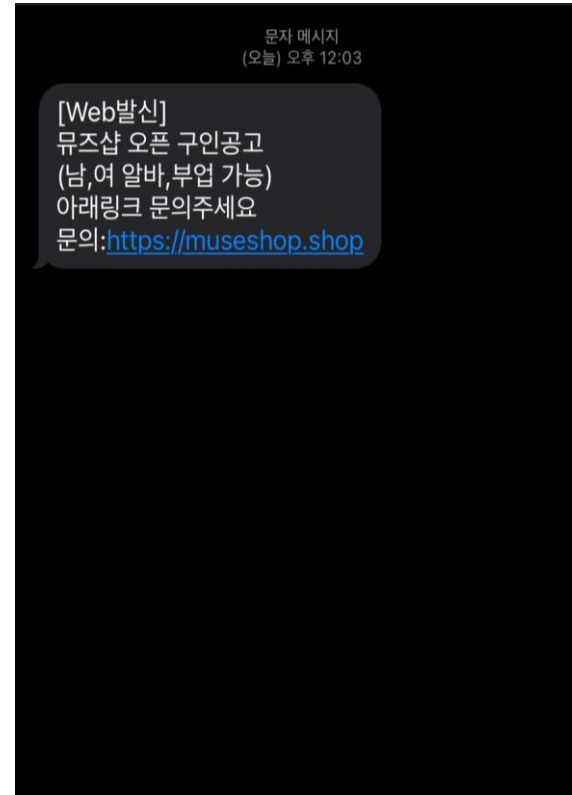


사진2. 국내 스팸 문자(with 링크)

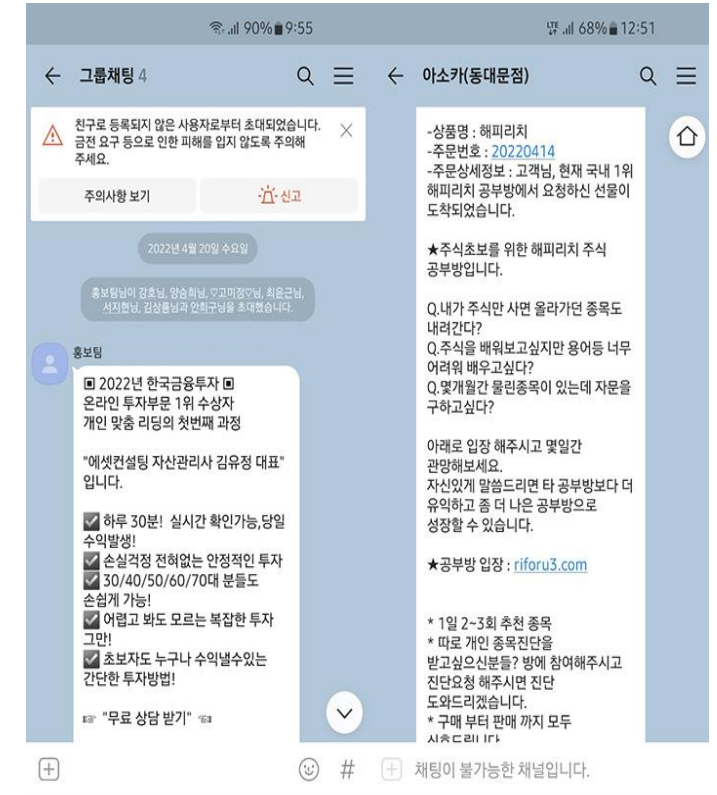


사진3. 카카오톡 스팸
(출처 : 가글하드웨어)

스팸 문자 조사

- 스팸문자는 어디서 발송될까? 얼마나 발송될까?

| 구 분 | | | '22년 상반기 | '22년 하반기 | '23년 상반기 | 증감 비교 (전반기 대비) | |
|-------------------------|---------------------|-----|----------|----------|-----------|-------------------|-------------|
| KISA 스팸 신고 ·탐지 | 휴대 전화 (신고·탐지) | 음성 | 990만건 | 447만건 | 461만건 | 3.1% ↑ | (14만건 ↑) |
| | | 문자 | 1,163만건 | 1,277만건 | 1억89만건 | 690.1% ↑ | (8,812만건 ↑) |
| | | 계 | 2,153만건 | 1,724만건 | 1억550만건 | 511.9% ↑ | (8,826만건 ↑) |
| | 이메일 (탐지) | 국내발 | 23만건 | 3만건 | 4만건 | 33.3% ↑ | (1만건 ↑) |
| | | 국외발 | 1,053만건 | 954만건 | 480만건 | 49.7% ↓ | (474만건 ↓) |
| | | 계 | 1,076만건 | 957만건 | 484만건 | 49.4% ↓ | (473만건 ↓) |
| | 합 계 | | 3,229만건 | 2,681만건 | 1억1,034만건 | 311.6% ↑ | (8,353만건 ↑) |

출처 : 한국인터넷진흥원 불법스팸대응센터
2023년 상반기 스팸 유통현황

◀ 스팸 유통현황 요약

[휴대전화 문자스팸 발송경로별 신고 · 탐지 비율]

| 발송경로 | | '22년 상반기 | '22년 하반기 | '23년 상반기 | 증감 (전반기 건수) |
|----------------|-----|----------|----------|----------|----------------|
| 대량문자 발송서비스 | 계 | 95.1% | 95.8% | 97.3% | 690.6% ↑ |
| | 국내발 | 85.1% | 85.9% | 83.1% | 653.6% ↑ |
| | 국외발 | 10.0% | 9.9% | 14.2% | 1,010.6% ↑ |
| 휴대전화 서비스 | | 3.8% | 3.6% | 2.7% | 482.4% ↑ |
| 기타(유선·인터넷전화 등) | | 1.1% | 0.6% | 0.0% | 62.3% ↓ |
| 합계 | | 100.0% | 100.0% | 100.0% | 678.6% ↑ |

문자 스팸 발송경로별 신고 및 탐지 비율 ▶

스팸 문자 무단 발송 사고

- 피해 금액
 - 23년도 상반기 스팸 문자 총 건수 : 1억 89만 건
 - 스팸 문자의 총 이용료 금액(1건당 평균 10원) : 10억 8천 9백만원
 - 만약 업체가 공격을 당해 스팸문자를 보내게 되면 문자 이용료를 내야 하나?
 - ✓ 2011년 9월 18일 법원 판결
 - ✓ 계정 해킹을 통해 발송된 스팸 문자는 요금 지급을 하지 않아도 됨

法 “해킹당해 발송된 스팸 문자는 요금 안 내도 돼”

송원형 기자

입력 2011.09.18. 15:23

가



문자 전송 프로그램의 아이디와 비밀번호를 해킹당해 누군가 그 프로그램으로 문자 수백만건을 보냈다면 프로그램 제공자에게 요금을 내야할까. 이런 경우 요금을 내지 않아도 된다는 법원의 판결이 나왔다.

서울중앙지법 민사43단독 박정길 판사는 문자메시지 전송 업체 운영자 장모씨가 A사를 상대로 낸 통신요금 청구 소송에서 원고 패소 판결했다고 18일 밝혔다.

사진4. 2011년 법원 판결 기사
(출처 : 조선일보)

스팸 문자 조사

- 문자 발송 기능 페이지를 가지고 있는 업체 공격
- 문자 발송 기능의 프로그램의 계정 탈취



사진5. 문자 발송 페이지
(출처 : 문자나라)



문자 메시지는 물론 카카오 알림톡 으로도 알림 메시지를 발송 할 수 있습니다.

사진6. 학원 등원 문자
(출처 : 365manager.co.kr)

스팸 문자 무단 발송 사고

- 23년 7월, 8월 사고 다수 발생
- 공격 대상
 - 문자 발송 페이지 보유 업체
 - 문자 발송 서비스 업체

문자 무단 발송 사고 신고 시기



스팸 문자 무단 발송 사고

- 공격 유형
 - 관리자 계정 탈취 후 정상 문자 발송 서비스 이용
 - 서버 내 악성파일 삽입 후 문자 발송 데이터 베이스에 스팸문자 내용 삽입
 - 문자 발송 데이터베이스 계정 탈취 후 직접 삽입

스팸문자를 어떻게 보냈을까?

PLAINBIT

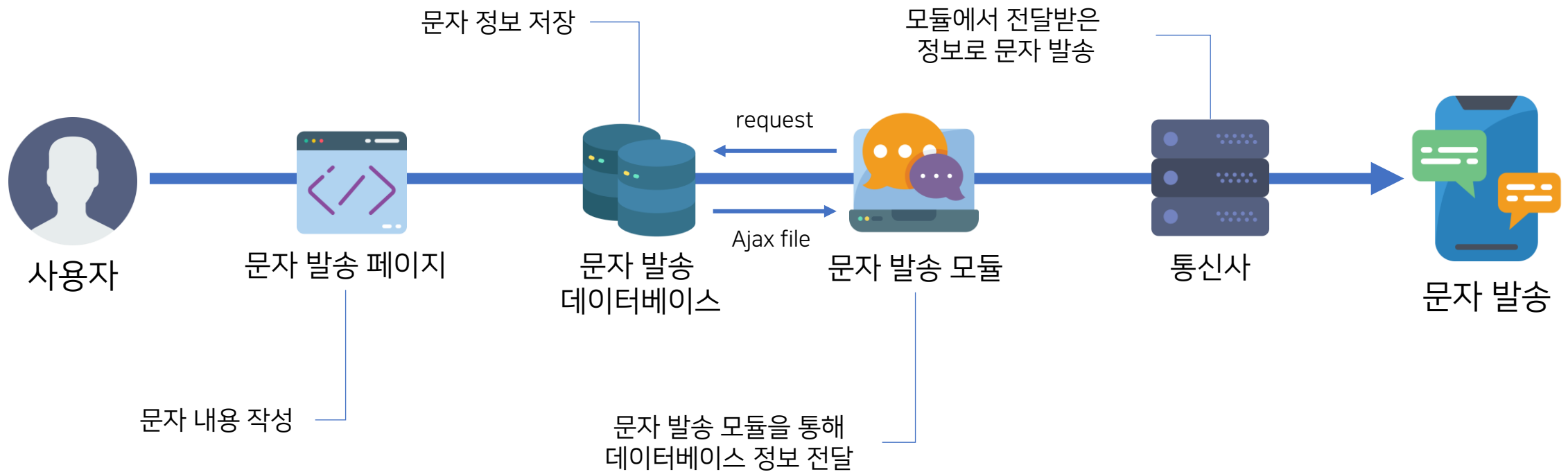
스팸문자를 어떻게 보냈을까?

스팸 문자 무단 발송 사고 분석

출처 : Mitre "ATT&CK matrix"

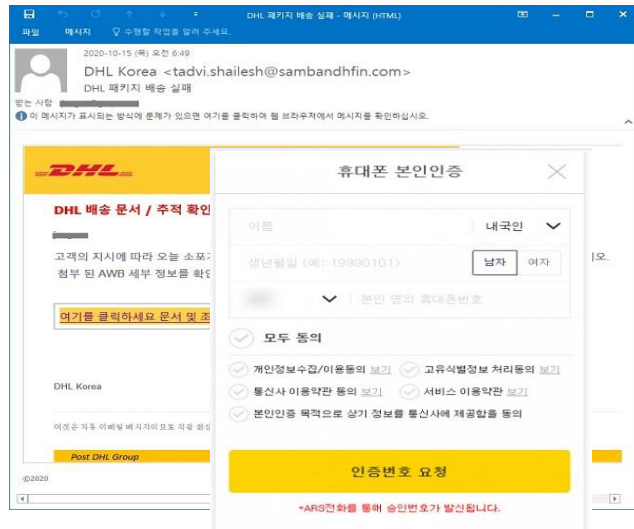
| Reconnaissance | Resource Development | 최초 침투 | Execution | 지속 | Privilege Escalation | Defense Evasion | Credential Access | 발견 | Lateral Movement | Collection | 명령제어 | 유출 | Impact |
|--|-------------------------------|------------------------------------|---------------------------------------|--|--|---|--|----------------------------------|---|--|---------------------------------------|--|--------------------------------|
| 10 techniques | 8 techniques | 10 techniques | 14 techniques | 20 techniques | 14 techniques | 43 techniques | 17 techniques | 32 techniques | 9 techniques | 17 techniques | 17 techniques | 9 techniques | 14 techniques |
| Active Scanning (3) | Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation (6) | Abuse Elevation Control Mechanism (5) | Abuse Elevation Control Mechanism (5) | Adversary-in-the-Middle (3) | Account Discovery (4) | Exploitation of Remote Services | Adversary-in-the-Middle (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Acquire Infrastructure (8) | Drive-by Compromise | Command and Scripting Interpreter (9) | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Accounts (3) | Exploit Public-Facing Services (4) | Container Administration Command | Boot or Logon Autostart Execution (14) | Account Manipulation (6) | BITS Jobs | Credentials from Password Stores (6) | Browser Information Discovery | Lateral Tool Transfer | Audio Capture | Content Injection | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Compromise Infrastructure (7) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts (5) | Boot or Logon Autostart Execution (14) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Automated Collection | Data Encoding (2) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Gather Victim Org Information (4) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Browser Extensions | Boot or Logon Initialization Scripts (5) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (8) | Browser Session Hijacking | Data Obfuscation (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Phishing for Information (4) | Establish Accounts (3) | Phishing (4) | Inter-Process Communication (3) | Compromise Client Software Binary | Create or Modify System Process (4) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Dynamic Resolution (3) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | Obtain Capabilities (6) | Supply Chain Compromise (3) | Native API | Create Account (3) | Domain Policy Modification (2) | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Encrypted Channel (2) | Firmware Theft | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) | Stage Capabilities (6) | Trusted Relationship | Scheduled Task/Job (5) | Create or Modify System Process (4) | Domain Policy Modification (2) | Direct Volume Access | Modify Authentication Process (8) | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository (2) | Fallback Channels | Financial Theft | Firmware Corruption |
| Search Open Websites/Domains (3) | | Valid Accounts (4) | Serverless Execution | Event Triggered Execution (16) | Escape to Host | Execution Guardrails (1) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Ingress Tool Transfer | Network Denial of Service (2) | Inhibit System Recovery |
| Search Victim-Owned Websites | | | Shared Modules | Event Triggered Execution (16) | Exploitation for Privilege Escalation | Exploitation for Defense Evasion | Multi-Factor Authentication Request Generation | Device Driver Discovery | | Data from Local System | Multi-Stage Channels | Resource Hijacking | Service Stop |
| | | | Software Deployment Tools | External Remote Services | Hijack Execution Flow (12) | File and Directory Permissions Modification (2) | Network Sniffing | Domain Trust Discovery | | Data from Network Shared Drive | Non-Application Layer Protocol | System Shutdown/Reboot | |
| | | | System Services (2) | Hijack Execution Flow (12) | Process Injection (12) | Hide Artifacts (11) | OS Credential Dumping (8) | File and Directory Discovery | | Data from Removable Media | Non-Standard Port | | |
| | | | User Execution (3) | Implant Internal Image | Scheduled Task/Job (5) | Hijack Execution Flow (12) | Steal Application Access Token | Group Policy Discovery | | Data Staged (2) | Protocol Tunneling | | |
| | | | Windows Management Instrumentation | Modify Authentication Process (8) | Valid Accounts (4) | Impersonation | Steal or Forge Authentication Certificates | Log Enumeration | | Email Collection (3) | Proxy (4) | | |
| | | | | Office Application Startup (6) | Power Settings | Indicator Removal (9) | Steal Web Session Cookie | Network Service Discovery | | Input Capture (4) | Remote Access Software | | |
| | | | | Pre-OS Boot (5) | Scheduled Task/Job (5) | Masquerading (9) | Unsecured Credentials (8) | Network Share Discovery | | Screen Capture | Traffic Signaling (2) | | |
| | | | | Scheduled Task/Job (5) | Server Software Component (5) | Modify Authentication Process (8) | | Password Policy Discovery | | Video Capture | Web Service (3) | | |
| | | | | Traffic Signaling (2) | | Modify Cloud Compute Infrastructure (5) | | Peripheral Device Discovery | | | | | |
| | | | | | | Modify Registry | | Permission Groups Discovery (3) | | | | | |
| | | | | | | Modify System Image (2) | | Process Discovery | | | | | |
| | | | | | | Network Boundary Bridging (1) | | Query Registry | | | | | |
| | | | | | | | | Remote System Discovery | | | | | |
| | | | | | | | | Software Discovery | | | | | |

문자 발송 프로세스

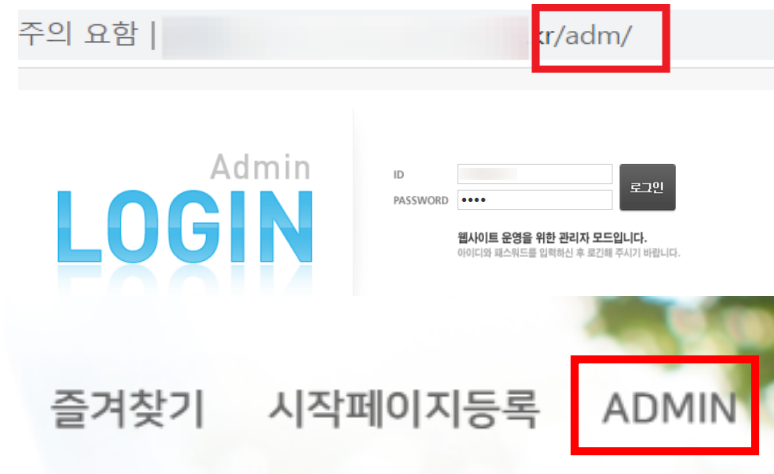


최초 침투

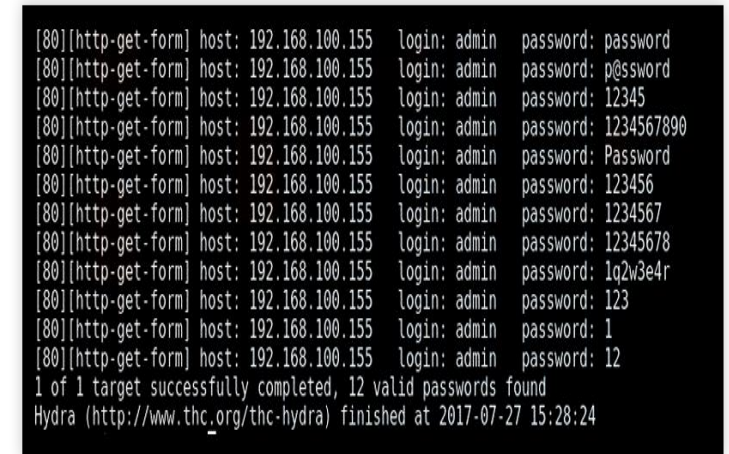
- 관리자 계정 탈취



관리자 대상 피싱 공격



관리자 로그인 페이지 접근 제어 미흡



관리자 계정 무작위 대입공격

최초 침투

- 파일 업로드 취약점 활용
 - 악성파일을 삽입을 위해 접근
 - 파일 업로드 가능한 페이지 중 업로드 파일에 대한 검사 부분이 미흡한 부분에 대하여 공격
 - 업로드 파일의 확장자를 변경하거나 전송간 파일의 확장자를 변경하여 전송

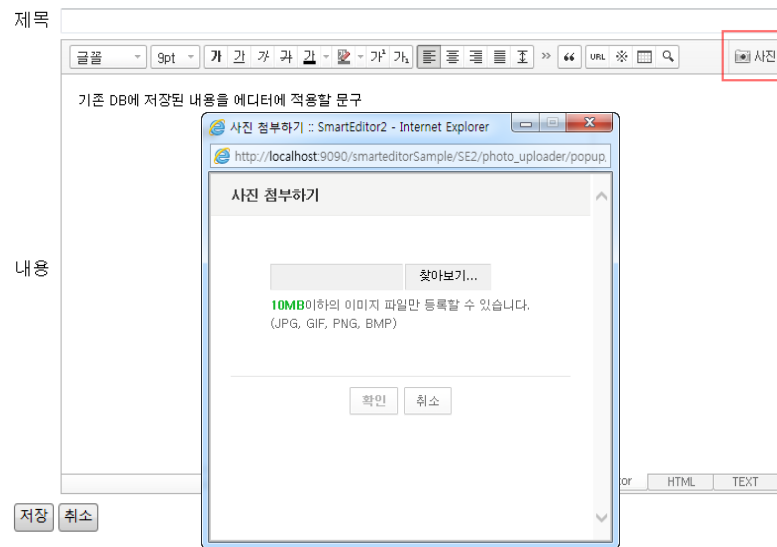


사진7. 확장자 변경

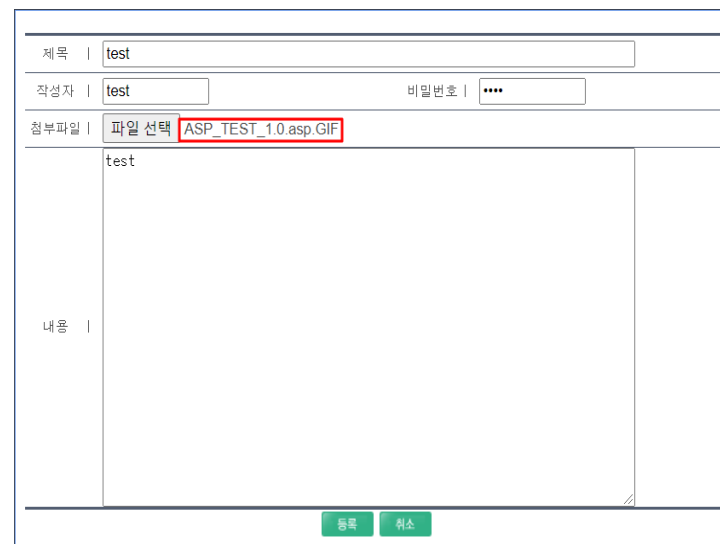


사진8. 이중 확장자 공격

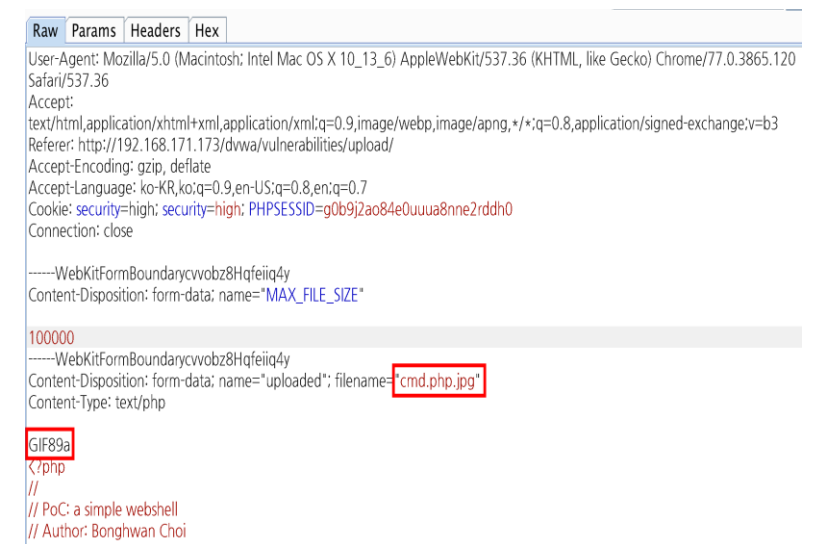
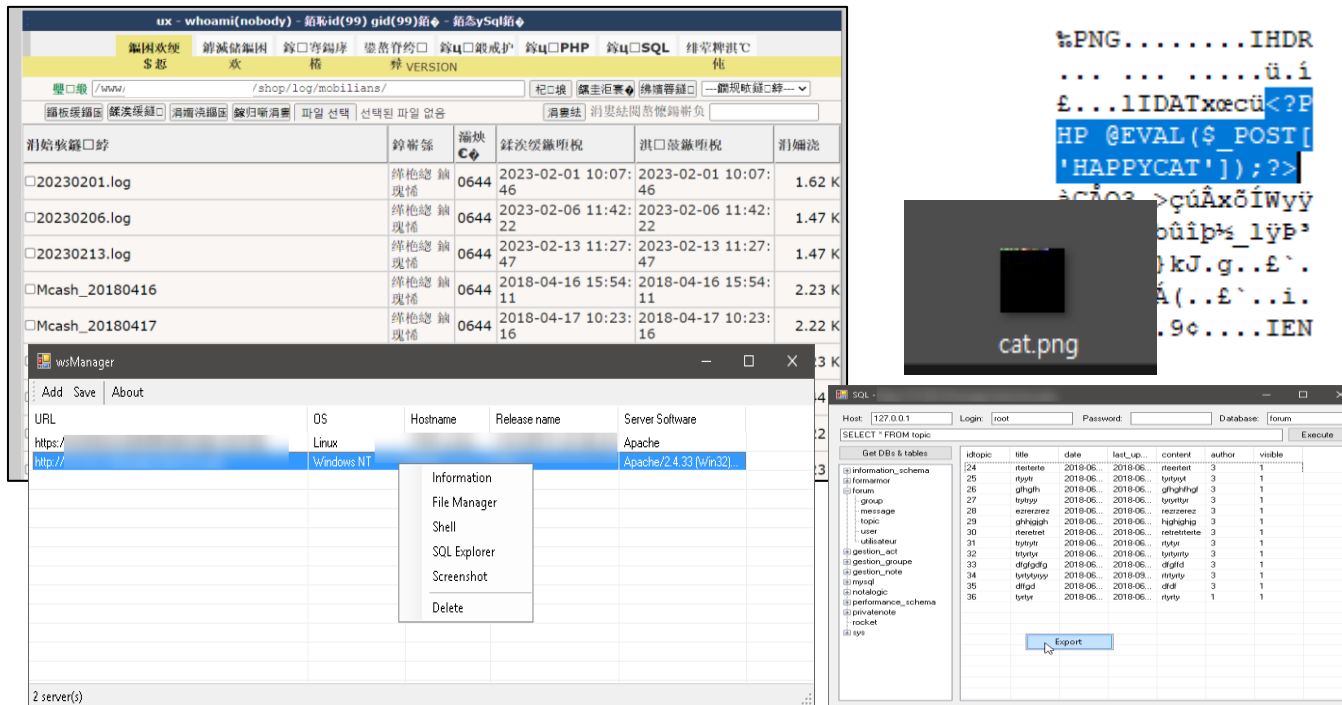


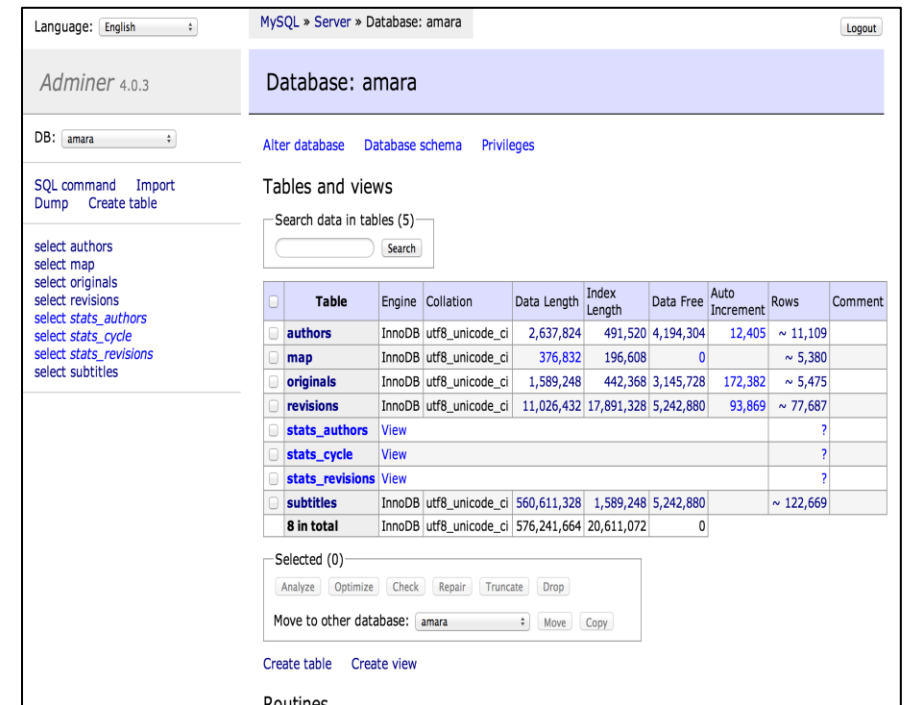
사진9. 전송간 타입 변경

지속

- 악성파일 삽입
 - 악성파일 종류



웹셀 & 웹셀 관리도구



데이터베이스 관리 도구
(Adminer)

지속

■ 악성파일 삽입

• 악성파일 종류

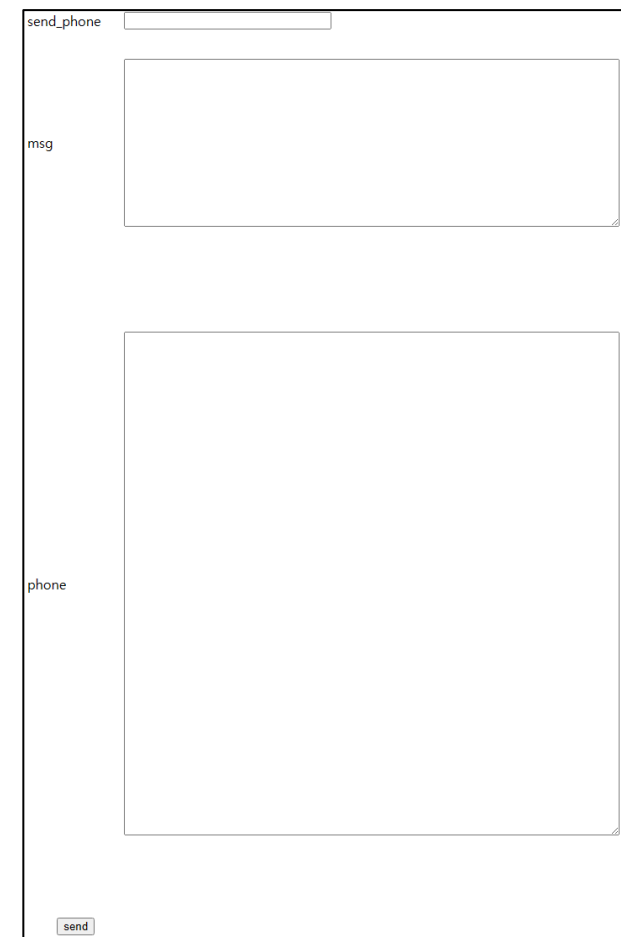
- ✓ 문자 발송 페이지 : 공격자가 문자 발송을 위해 별도 제작
- ✓ 공격자는 문자 발송에 관한 프로세스에 대한 이해가 높음
- ✓ 제작 전 필요한 메시지 발송 정보 (데이터베이스 접속정보, 문자메시지 전송 쿼리 등) 탈취

```
$host = "데이터 베이스 IP"
$uid = "데이터 베이스 계정"
$pwd = "데이터 베이스 패스워드"
$dbName = "데이터 베이스 이름"

$conn = mysql_connect $host $uid $pwd

$sql = "insert into mms_msg(테이블 명)
value('".$value."', '$sendPhone.', ~~)"
```

문자발송 페이지 소스코드 예시



문자발송페이지 예시

발견 혹은 유출

- 고객 정보 수집
 - 관리자 계정 로그인 후 회원 주소록, 회원 정보 페이지를 활용하여 정보 수집
 - 스팸문자 발송 대상으로 이용

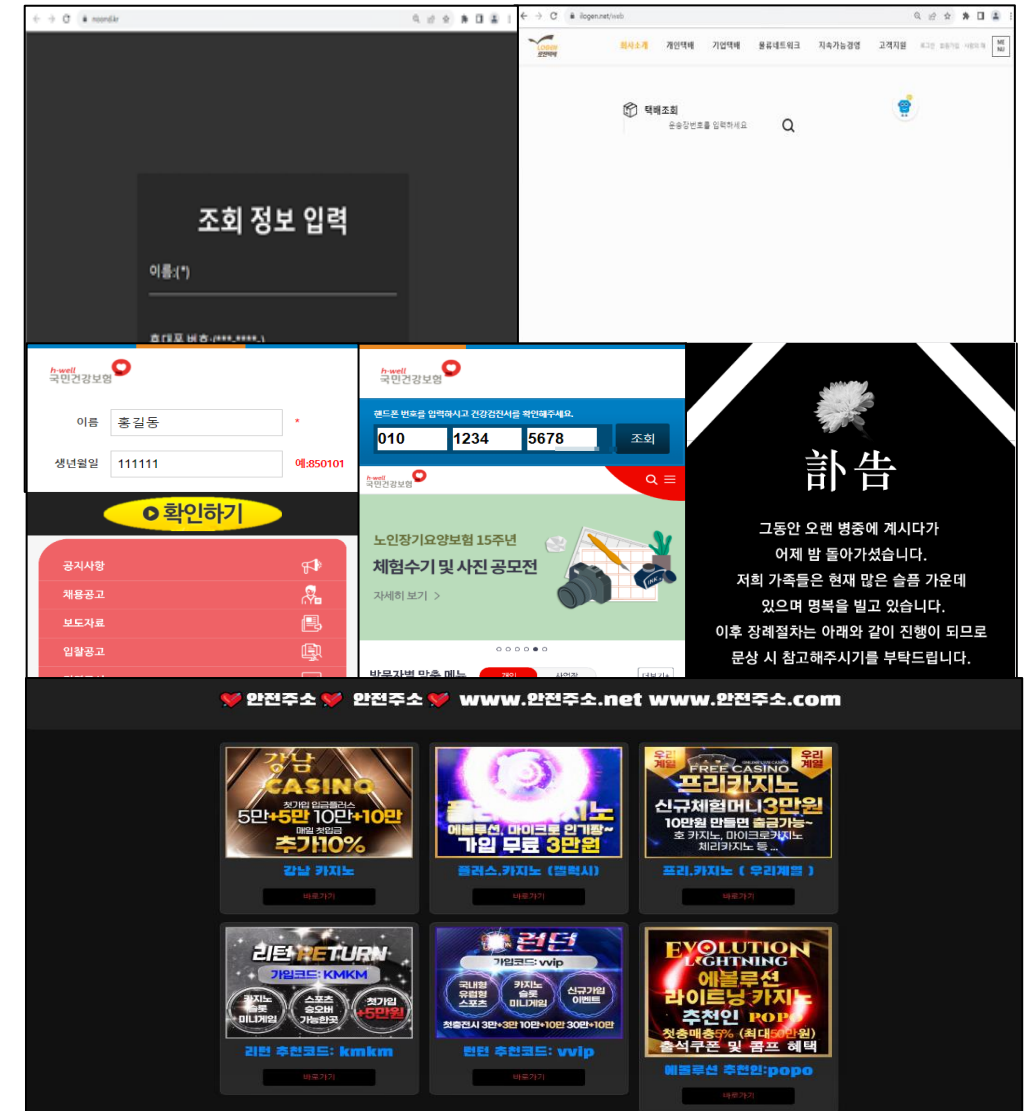
sms.php



The screenshot displays the 'sms.php' web interface. At the top, it shows '잔여 SMS 포인트 : 800,481 건' and a button 'SMS 포인트 충전하기'. Below this is a section titled '회원/일반 주소록' with tabs for '회원 주소록' and '일반 주소록'. The '회원 주소록' tab is active, showing a table with columns '번호', '이름', '아이디', and '핸드폰번호'. The table contains 10 rows of data, with the names redacted by a black box. A red box highlights the '전체선택' button at the bottom left of the table. To the right of the table is a '선택 발송 대상 0명' section with a large empty box and a '추가 >' button. At the bottom right, there is a blue button labeled 'SMS작성' with a red arrow pointing to it. The bottom of the page shows pagination: '1 [2] [3] [4] [5] [6] [7] [8] [9] [10] > [2550]'.

명령&제어

- 스팸 문자 발송
 - 대상 : 불 특정 다수 혹은 해당 업체의 고객
 - 종류 : SMS, 카카오톡 알림톡
 - 목적 :
 - ✓ 악성 앱 설치 유도
 - ✓ 피싱 페이지 유포
 - ✓ 불법 사이트 홍보(도박, 성인, 온라인 아르바이트, 온라인 마케팅 홍보)



무엇을 할 것인가?

PLAINBIT

무엇을 할 것인가?

문자 무단 발송 사고 대응

출처 : Mitre "d3fend matrix"

| Model | | | | 강화 | | | | 탐지 | | | | Isolate | | Deceive | | 제거 | | Restore | | | | | |
|---------------------------------|--------------------------------|--------------------------------|---------------------------------|--------------------------------------|----------------------------------|-------------------------------|----------------------------------|------------------------|---------------------------------|--------------------------------|--|-----------------------------------|-------------------------------------|---|----------------------------------|---------------------------------------|---------------------|------------------------|-----------------------------------|---------------|---------------------|-----------------------------|-----------------------|
| Asset Inventory | Network Mapping | Operational Activity Mapping | System Mapping | Application Hardening | Cri Hardening | e Hardening | Platform Hardening | File Analysis | Identifier Analysis | Message Analysis | Form Analysis | Form Monitoring | Process Analysis | User Behavior Analysis | Execution Isolation | Network Isolation | Decoy Environment | Decoy Object | Credenti Eviction | Eviction | Process Eviction | Restore Access | Restore Object |
| Asset Vulnerability Enumeration | Logical Link Mapping | Access Modeling | Data Exchange Mapping | Application Configuration Hardening | Biometric Authentication | Message Authentication | Bootloader Authentication | Dynamic Analysis | Homoglyph Detection | Sender MTA Reputation Analysis | Administrative Network Activity Analysis | File Integrity Monitoring | Database Query String Analysis | Authentication Event Thresholding | Executable Allowlisting | Broadcast Domain Isolation | Connected Honeynet | Decoy File | Account Locking | File Removal | Process Suspension | Restore Network Access | Reissue Credential |
| Configuration Inventory | Active Logical Link Mapping | Operational Dependency Mapping | Service Dependency Mapping | Dead Code Elimination | Certificate-based Authentication | Message Encryption | Disk Encryption | Emulated File Analysis | Identifier Activity Analysis | Sender Reputation Analysis | Byte Sequence Emulation | Firmware Behavior Analysis | File Access Pattern Analysis | Authorization Event Thresholding | Executable Denylisting | DNS Allowlisting | Integrated Honeynet | Decoy Network Resource | Authentication Cache Invalidation | Email Removal | Process Termination | Restore User Account Access | Restore Configuration |
| Data Inventory | Passive Logical Link Mapping | Operational Risk Assessment | System Dependency Mapping | Exception Handler Pointer Validation | Certificate Pinning | Transfer Agent Authentication | Driver Load Integrity Checking | File Content Analysis | Identifier Reputation Analysis | | Certificate Analysis | Firmware Embedded Monitoring Code | Indirect Branch Call Analysis | Credential Compromise Scope Analysis | Hardware-based Process Isolation | DNS Denylisting | Standalone Honeynet | Decoy Persona | Credential Revoking | | | Unlock Account | Restore Database |
| Hardware Component Inventory | Network Traffic Policy Mapping | Organization Mapping | System Vulnerability Assessment | Pointer Authentication | Credential Rotation | | File Encryption | File Content Rules | Domain Name Reputation Analysis | | Active Certificate Analysis | Firmware Verification | Process Code Segment Verification | Domain Account Monitoring | IO Port Restriction | Forward Resolution Domain Denylisting | | Decoy Public Release | | | | | Restore Disk Image |
| Network Node Inventory | Physical Link Mapping | | | Process Segment Execution Prevention | Credential Transmission Scoping | | Local File Permissions | File Hashing | File Hash Reputation Analysis | | Passive Certificate Analysis | Peripheral Firmware Verification | Process Self-Modification Detection | Job Function Access Pattern Analysis | Kernel-based Process Isolation | Hierarchical Domain Denylisting | | Decoy Session Token | | | | | Restore Email |
| Software Inventory | Active Physical Link Mapping | | | Segment Address Offset Randomization | Domain Trust Policy | | Software Update | | IP Reputation Analysis | | Client-server Payload Profiling | System Firmware Verification | Process Spawn Analysis | Local Account Monitoring | Mandatory Access Control | Homoglyph Denylisting | | Decoy User Credential | | | | | Restore Software |
| | | | | Stack Frame Canary Validation | Multi-factor Authentication | | System Configuration Permissions | | URL Reputation Analysis | | Connection Attempt Analysis | Operating System Monitoring | Process Lineage Analysis | Resource Access Pattern Analysis | System Call Filtering | Forward Resolution IP Denylisting | | | | | | | |
| | | | | | One-time Password | | TPM Boot Integrity | | URL Analysis | | DNS Traffic Analysis | Endpoint Health Beacon | Script Execution Analysis | Session Duration Analysis | | Reverse Resolution IP Denylisting | | | | | | | |
| | | | | | Strong Password Policy | | | | | | File Carving | Input Device Analysis | Shadow Stack Comparisons | User Data Transfer Analysis | | Encrypted Tunnels | | | | | | | |
| | | | | | User Account Permissions | | | | | | Inbound Session Volume Analysis | Memory Boundary Tracking | System Call Analysis | User Geolocation Logon Pattern Analysis | | Network Traffic Filtering | | | | | | | |
| | | | | | | | | | | | IPC Traffic Analysis | Scheduled Job Analysis | File Creation Analysis | Web Session Activity Analysis | | Inbound Traffic Filtering | | | | | | | |
| | | | | | | | | | | | Network Traffic Community Deviation | System Daemon Monitoring | | | | Email Filtering | | | | | | | |
| | | | | | | | | | | | Per Host Download-Upload Ratio Analysis | System File Analysis | | | | Outbound Traffic Filtering | | | | | | | |
| | | | | | | | | | | | Protocol Metadata Anomaly Detection | Service Binary Verification | | | | | | | | | | | |
| | | | | | | | | | | | Relay Pattern Analysis | System Init Config Analysis | | | | | | | | | | | |
| | | | | | | | | | | | Remote Terminal Session Detection | User Session Init Config Analysis | | | | | | | | | | | |
| | | | | | | | | | | | RPC Traffic Analysis | | | | | | | | | | | | |

계정 탈취

- 관리자계정은 2차 인증 적용
- 취약한 패스워드 이용 방지
 - 패스워드 정책 (NIST800-3B)
 - ✓ 너무 복잡하지 않게, 흔한 패턴 X
 - ✓ 길이는 길게 (문장, URL)

Free Password Hash Cracker

| Hash | Type | Result |
|-----------------------------------|------|----------|
| 0192023a7bbd732505161069df118b500 | md5 | admin123 |

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

| Hash | Type | Result |
|----------------------------------|------|------------|
| c3532229748606ac481e2d91c6a0423d | md5 | test123!@# |

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

기존 패스워드 크랙 결과
(위 : admin123, Test123!@#)

[Web발신]
본인확인을 위해 인증번호 221647
를 입력해 주세요

(어제) 05:11

본인확인을 위해 인증번호
(967835)를 입력해 주세요

[Web발신]
본인확인을 위해 인증번호
(135455)를 입력해 주세요

Google

870 715



Facebook

734 855



Instagram

424 372



2차 인증
(좌 : 휴대폰인증, 우 : OTP)

Free Password Hash Cracker

| Hash | Type | Result |
|----------------------------------|---------|------------|
| 4644c57c29ec15ae99fc2357f9dece19 | Unknown | Not found. |

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

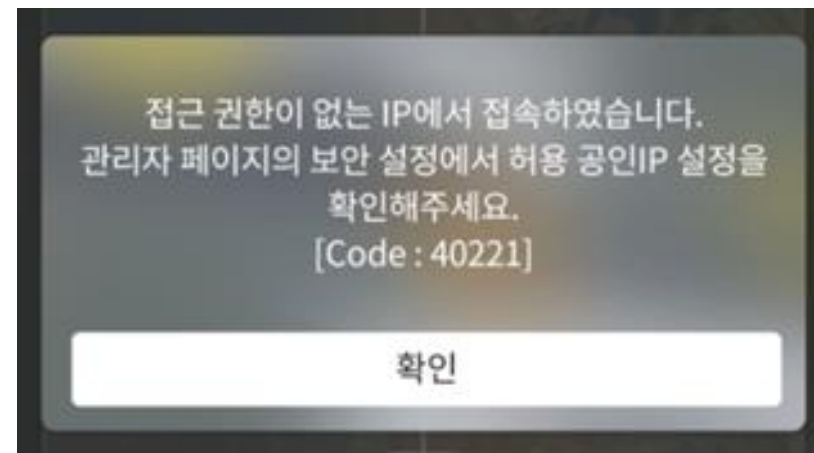
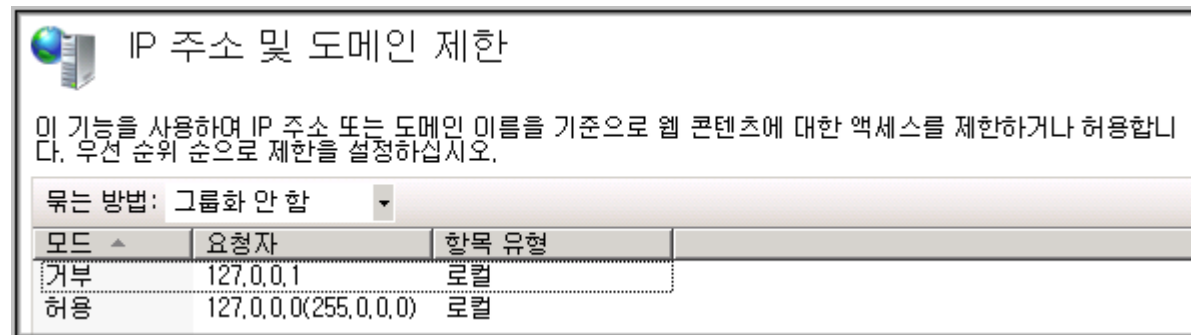
| Hash | Type | Result |
|----------------------------------|---------|------------|
| b7e618a1d45cd49bd335670d1440cc0e | Unknown | Not found. |

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

새로운 패턴, 문장형 패스워드 크랙 결과
(위 : test1#2#3,Today lunch is chicken)

관리자 로그인 페이지 노출 제거

- 허용된 IP 주소만 접속할 수 있도록 설정
- URL 직접 접근 불가
- URL 사용 시 유추하기 쉬운 문자 제외
 - /admin, /manager, /master ...
- 관리자 페이지 접근 시 2차 인증 도입



파일 업로드 취약점 대응

- 업로드 페이지 내 파일 검사 패턴 추가 (시큐어코딩)
 - 파일 확장자 검사
 - 파일 이중 확장자 검사(파일이름 특수문자 검사)
- 업로드 폴더 소유주 변경(관리자 보다 낮은 권한의 계정)
- 업로드 폴더 내 파일의 실행권한 제거
- 업로드 파일 이름 및 확장자를 외부 사용자가 추측할 수 없는 문자열로 변경

//업로드되는 파일명 난수화 기능

```
$str = "ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890abcdefghijklmnopqrstuvwxyz";  
$str = str_shuffle($str);  
$str = substr($str, 0, 30);
```

```
$upName = $str.$_FILES['CoverImage']['name'];  
$tempFile = $_FILES['CoverImage']['tmp_name'];  
$targetPath = $_SERVER['DOCUMENT_ROOT'] . $targetFolder;  
$targetFile = rtrim($targetPath, "/").".".$upName;
```

// 업로드 할 수 있는 파일의 확장자를 지정한다.

```
$fileTypes = array('jpg', 'jpeg', 'gif', 'png');  
$fileParts = pathinfo($_FILES['CoverImage']['name']);
```

```
if(in_array($fileParts['extension'], $fileTypes)) {  
    move_uploaded_file($tempFile, $targetFile);  
    echo $upName;  
} else {  
    echo "업로드 할 수 없는 형식의 파일입니다.";  
}
```

악성파일 삽입 대응

- 업로드 폴더에 대한 파일 검사

03

무료 웹 보안도구 보급
휘슬(WHISTL)



한국인터넷진흥원은 중소기업 및 비영리법인을 대상으로 홈페이지 보안 강화를 위해 악성코드(웹쉘)와 악성코드 은닉 사이트를 탐지하는 도구를 제작해 배포하고 있습니다.

안티 바이러스 서버용 백신

서버로 유입되는 다양한 악성코드, 바이러스, 랜섬웨어의 위협!!
Windows & Linux 환경에 최적화된 서버보안 안티바이러스 솔루션

```
(WebShell) C:\Users\ \Downloads\NeoPI-master>python neopi.py -s C:\ESD

[[ Total files scanned: 17 ]]
[[ Total files ignored: 0 ]]
[[ Scan Time: 1.691135 seconds ]]

[[ Top 10 signature match counts ]]
18      C:\ESD\pyspy.php
3        C:\ESD\b374k-2.5.php
```

| 웹쉘 탐지 솔루션 | 서버 백신 | 웹쉘 탐지 스크립트 |
|---------------------|----------------------------------|--------------------------------------|
| 유료, 무료 | 유료 | 무료 |
| 웹쉘 코드에 대한 패턴을 통한 탐지 | 웹쉘 파일에 대한 hash 값 악성 행위에 대한 탐지 | 웹쉘코드에 대한 패턴 탐지 기존 파일과의 차이점을 기반 탐지 |
| 웹쉘 특화 대응 | 웹쉘 포함 악성파일 대한 대응 | 다양한 기능의 스크립트 |

문자발송 데이터베이스

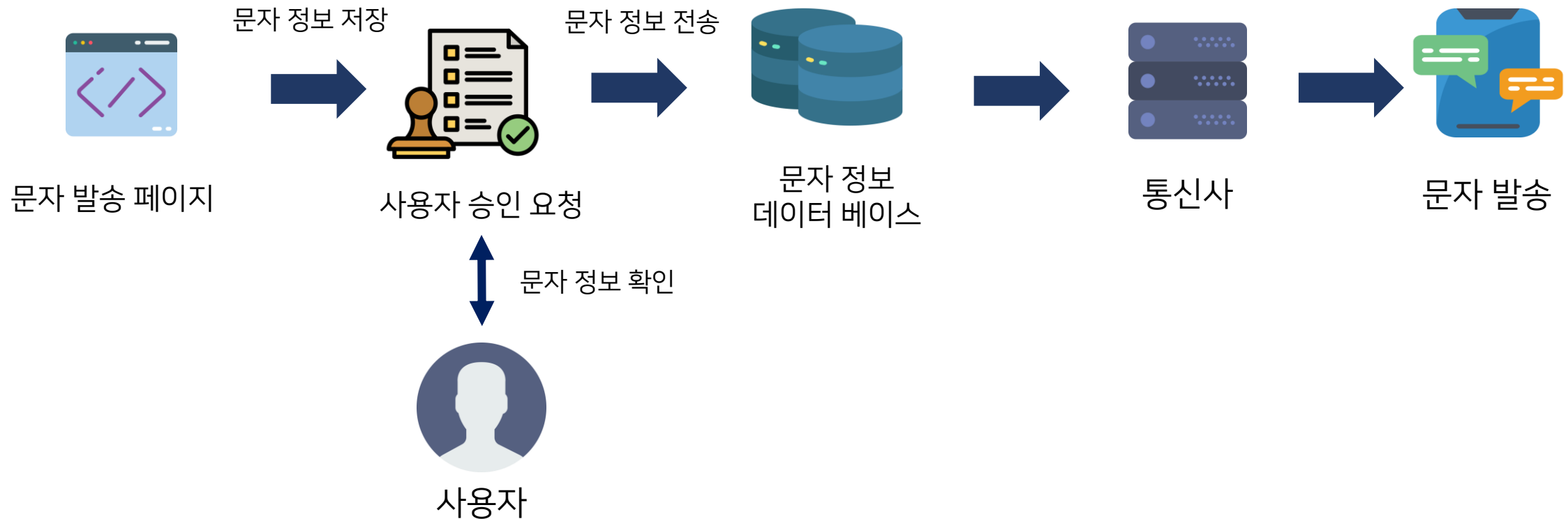
■ 데이터베이스 보안

출처 : 한국인터넷진흥원 “클라우드 취약점 점검 가이드” (2020.12)

| MY-SQL(MariaDB) | MS-SQL | MongoDB |
|------------------------------------|----------------------------------|-----------------------|
| 불필요한 계정 삭제 (최초 생성 계정, 테스트 계정 등) | | |
| 취약한 패스워드 사용 제한 | SYSADMIN 권한 제한 | 불필요한 데이터 베이스 및 테이블 제거 |
| 타 사용자에게 권한 부여 옵션 사용 제한 | SA 계정 패스워드 관리 | 데몬 실행 시 인증 옵션 사용 |
| DB 사용자 계정 정보 테이블 접근 권한 제한 | Guest 계정 사용 제한 | 관리자 계정 생성 여부 확인 |
| Root 권한으로 서버 구동 제한 | Registry Procedure Permission 제한 | 환경 설정 파일 접근 제어 |
| 환경설정 파일 접근 제어 | Xp_cmdshell 사용 제한 | http interface 접근 통제 |
| 암호 저장시 안전한 암호 알고리즘 사용 | - | 데이터베이스 접근 제한 설정 |
| 로그 활성화 | | |
| 최신 패치 적용 | | |

스팸문자 발송 간 대응

- 대량 문자 발송 전 문자 발송 사용자에게 2차 인증(제안)
 - 공격자가 계정 탈취 후 정상 발송 프로세스를 통해 스팸문자를 보낼 때
 - 대량 문자 발송 시 2차 인증을 통해 문자 내용 확인 후 전송 (사용자의 휴대폰으로 안내)



감사합니다

Thank you for your attention.

PLAINBIT