Application Password Decrypter

baadc0de

http://baadc0de.blogspot.com

개요

1. **Application Password Decrypter**

2. **기존 연구 소개**
   - Database SQL Developers
   - Messengers

3. **향후 연구 토의**

Application Password Decrypter

Application Password Decrypter

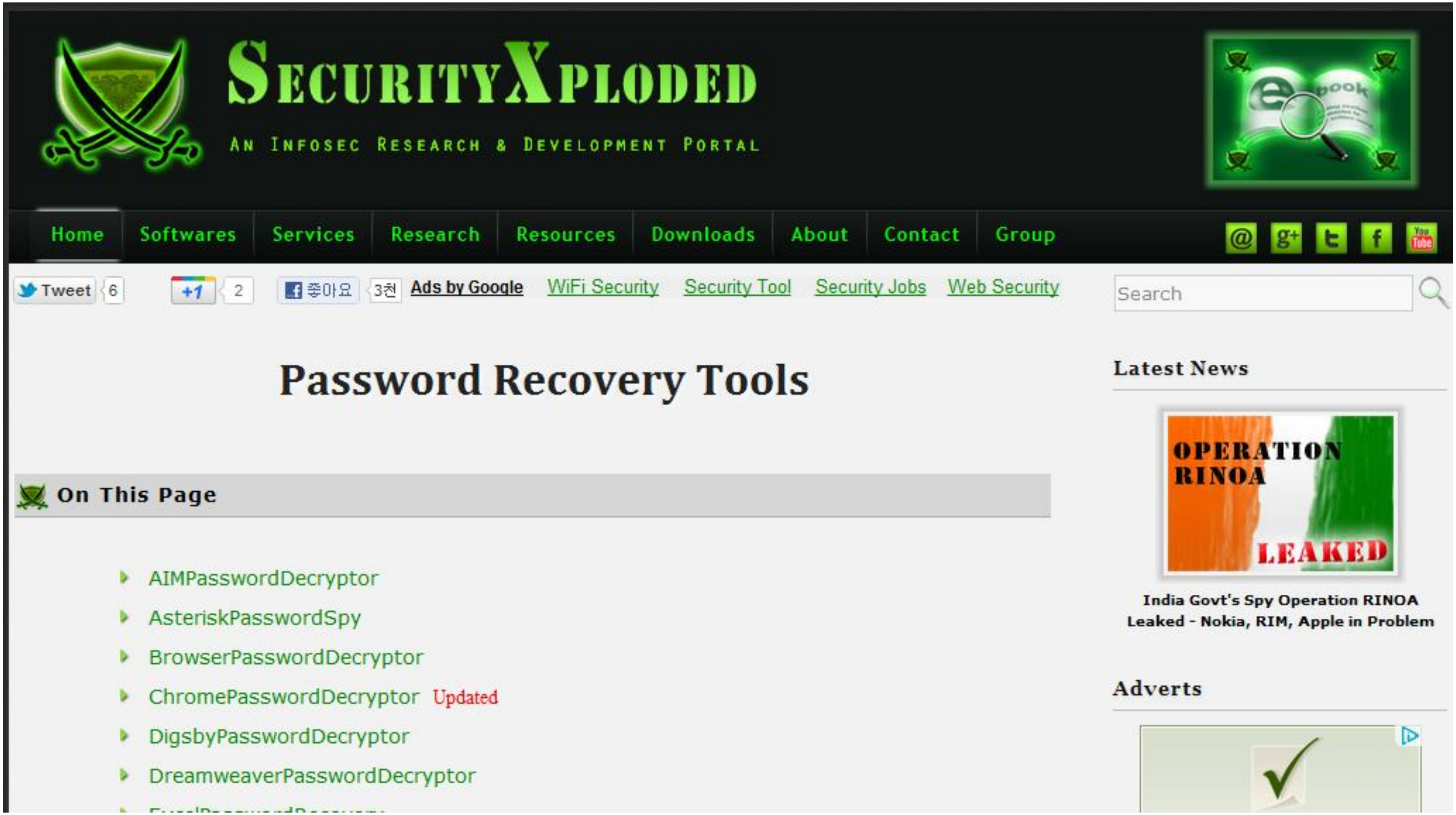
- **프로젝트 개요**
  - 패스워드 복호화 도구
  - ID & Password를 저장하는 모든 프로그램을 대상
  - 웹브라우저, 메신저....등 (당신이 원하는 모든 것!)

- **멤버**
  - **baadc0de**
  - **posquit0**
  - **proneer**

Application Password Decrypter

SecurityXploded – Password Recovery Tools

- http://securityxploded.com/password-recovery-tools.php



Password Recovery Tools

On This Page

- AIMPasswordDecryptor
- AsteriskPasswordSpy
- BrowserPasswordDecryptor
- ChromePasswordDecryptor Updated
- DigsbyPasswordDecryptor
- DreamweaverPasswordDecryptor

Latest News

India Govt's Spy Operation RINOA Leaked - Nokia, RIM, Apple in Problem

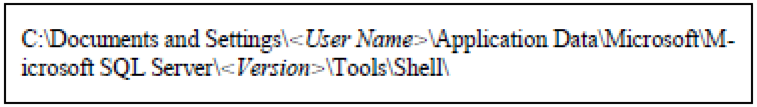
Adverts

기존 연구 소개

- Database SQL Developers
- Messengers

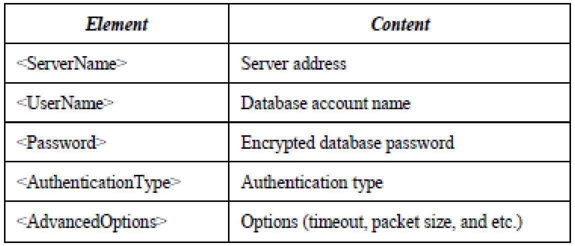
Microsoft SQL Server Management Studio

- 설정파일 경로



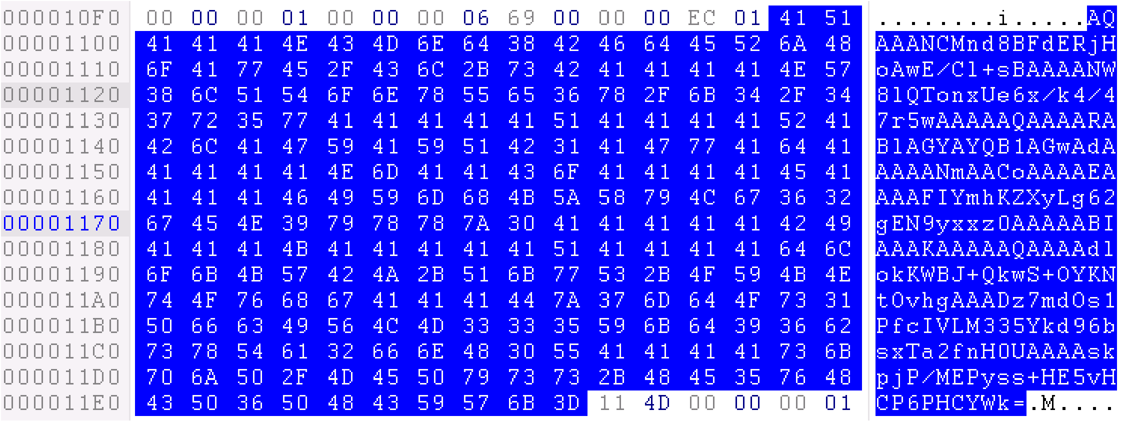
C:\Documents and Settings\<*User Name*>\Application Data\Microsoft\Microsoft SQL Server\<*Version*>\Tools\Shell\

- RegSrvr.xml (즐겨찾는 서버 등록)



Element	***Content***
<ServerName>	Server address
<UserName>	Database account name
<Password>	Encrypted database password
<AuthenticationType>	Authentication type
<AdvancedOptions>	Options (timeout, packet size, and etc.)

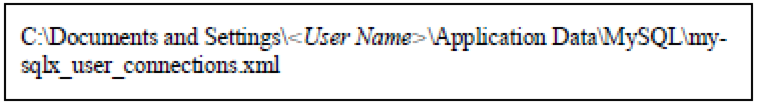
- Base64 인코딩된 패스워드



```
000010F0  00 00 00 01 00 00 00 06 69 00 00 00 EC 01 41 51  ........i.....AQ
00001100  41 41 41 4E 43 4D 6E 64 38 42 46 64 45 52 6A 48  AAANCMnd8BFdERjH
00001110  6F 41 77 45 2F 43 6C 2B 73 42 41 41 41 41 4E 57  oAwE/Cl+sBAAAANW
00001120  38 6C 51 54 6F 6E 78 55 65 36 78 2F 6B 34 2F 34  8lQTonxUe6x/k4/4
00001130  37 72 35 77 41 41 41 41 41 51 41 41 41 41 52 41  7r5wAAAAAQAAAARA
00001140  42 6C 41 47 59 41 59 51 42 31 41 47 77 41 64 41  BlAGYAYQB1AGwAdA
00001150  41 41 41 41 4E 6D 41 41 43 6F 41 41 41 41 45 41  AAAANmAACoAAAAEA
00001160  41 41 41 46 49 59 6D 68 4B 5A 58 79 4C 67 36 32  AAAFIYmhKZXyLg62
00001170  67 45 4E 39 79 78 78 7A 30 41 41 41 41 41 42 49  gEN9yxxz0AAAAABI
00001180  41 41 41 4B 41 41 41 41 41 51 41 41 41 41 64 6C  AAAKAAAAAQAAAAdl
00001190  6F 6B 4B 57 42 4A 2B 51 6B 77 53 2B 4F 59 4B 4E  okKWBJ+QkwS+OYKN
000011A0  74 4F 76 68 67 41 41 41 44 7A 37 6D 64 4F 73 31  tOvhgAAADz7mdOs1
000011B0  50 66 63 49 56 4C 4D 33 33 35 59 6B 64 39 36 62  PfcIVLM335Ykd96b
000011C0  73 78 54 61 32 66 6E 48 30 55 41 41 41 41 73 6B  sxTa2fnH0UAAAAsk
000011D0  70 6A 50 2F 4D 45 50 79 73 73 2B 48 45 35 76 48  pjP/MEPyss+HE5vH
000011E0  43 50 36 50 48 43 59 57 6B 3D 11 4D 00 00 00 01  CP6PHCYWk=.M....
```

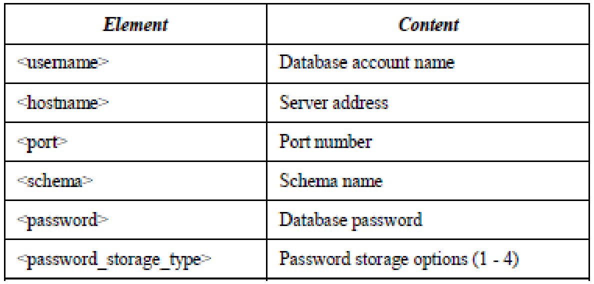
MySQL Query Browser

- 접속 기록 저장 파일



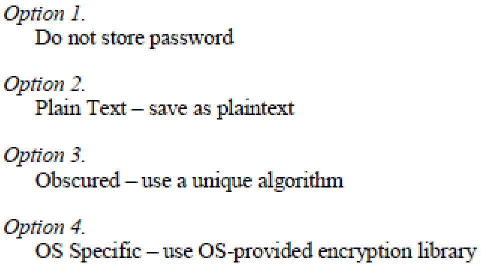
C:\Documents and Settings\<*User Name*>\Application Data\MySQL\my-sqlx_user_connections.xml

- mysql_user_connecton.xml



Element	***Content***
<username>	Database account name
<hostname>	Server address
<port>	Port number
<schema>	Schema name
<password>	Database password
<password_storage_type>	Password storage options (1 - 4)

- 패스워드 저장 옵션



Option 1.
Do not store password

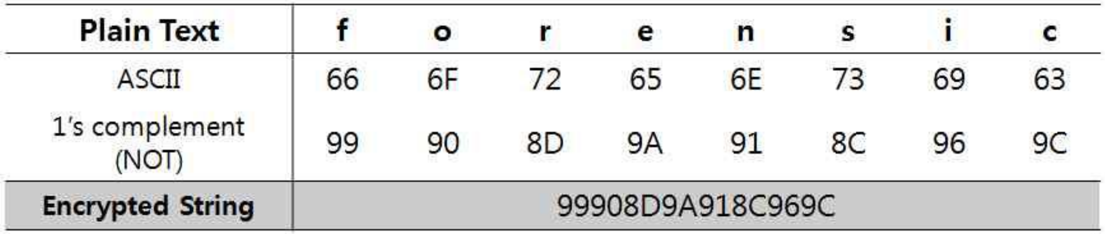
Option 2.
Plain Text – save as plaintext

Option 3.
Obscured – use a unique algorithm

Option 4.
OS Specific – use OS-provided encryption library

MySQL Query Browser (cont'd)

- 암/복호화 방식
  - Obscured – 자체 함수

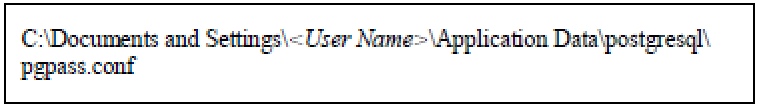


Plain Text	f	o	r	e	n	s	i	c
ASCII	66	6F	72	65	6E	73	69	63
1's complement (NOT)	99	90	8D	9A	91	8C	96	9C
Encrypted String	99908D9A918C969C							

  - OS Specific – OS 자체 함수 이용
    - ✓ CryptProtectData – 암호화
    - ✓ CryptUnprotectData – 복호화
    - ✓ 암호화된 바이너리를 Base64 text로 저장

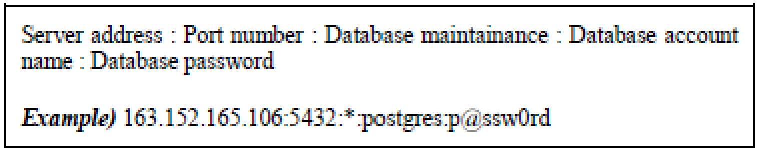
PostgreSQL pgAdmin III

- 접속 기록 저장 파일



C:\Documents and Settings\<*User Name*>\Application Data\postgresql\pgpass.conf

- 저장 방식

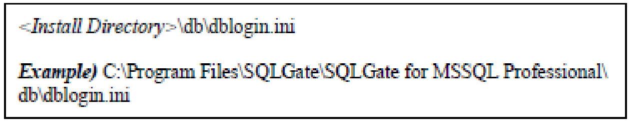


Server address : Port number : Database maintainance : Database account name : Database password

Example) 163.152.165.106:5432:*:postgres:p@ssw0rd

SQLGate for MSSQL, MySQL, and Oracle

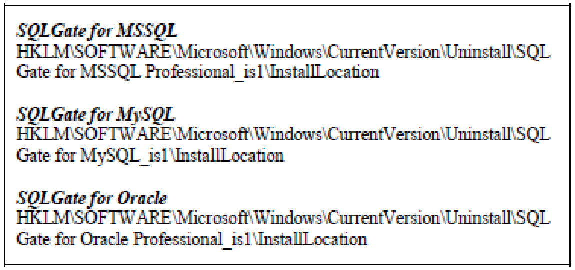
- 설정 파일 경로



```
<Install Directory>\db\dblogin.ini

Example) C:\Program Files\SQLGate\SQLGate for MSSQL Professional\
db\dblogin.ini
```

- 프로그램 설치 경로

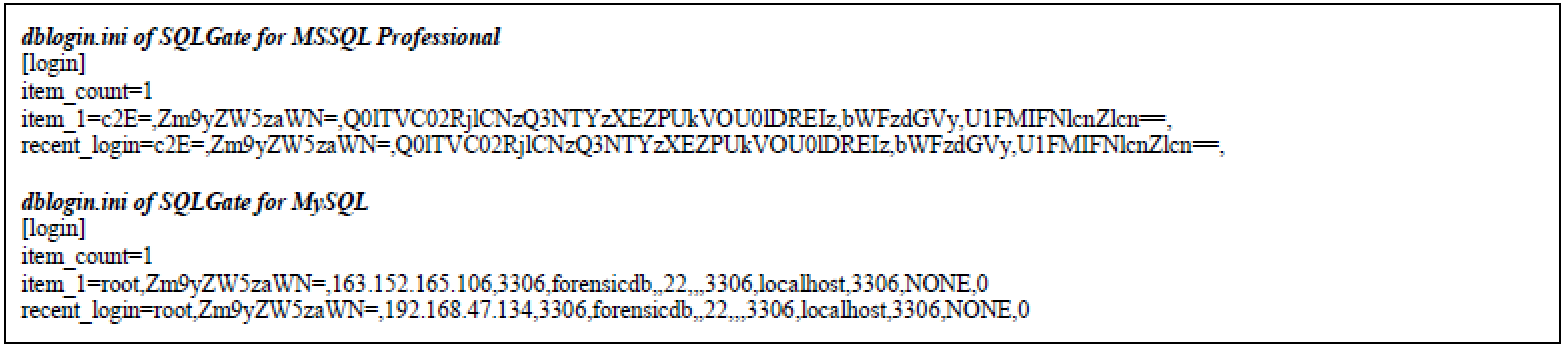


```
SQLGate for MSSQL
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SQL
Gate for MSSQL Professional_is1\InstallLocation

SQLGate for MySQL
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SQL
Gate for MySQL_is1\InstallLocation

SQLGate for Oracle
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SQL
Gate for Oracle Professional_is1\InstallLocation
```

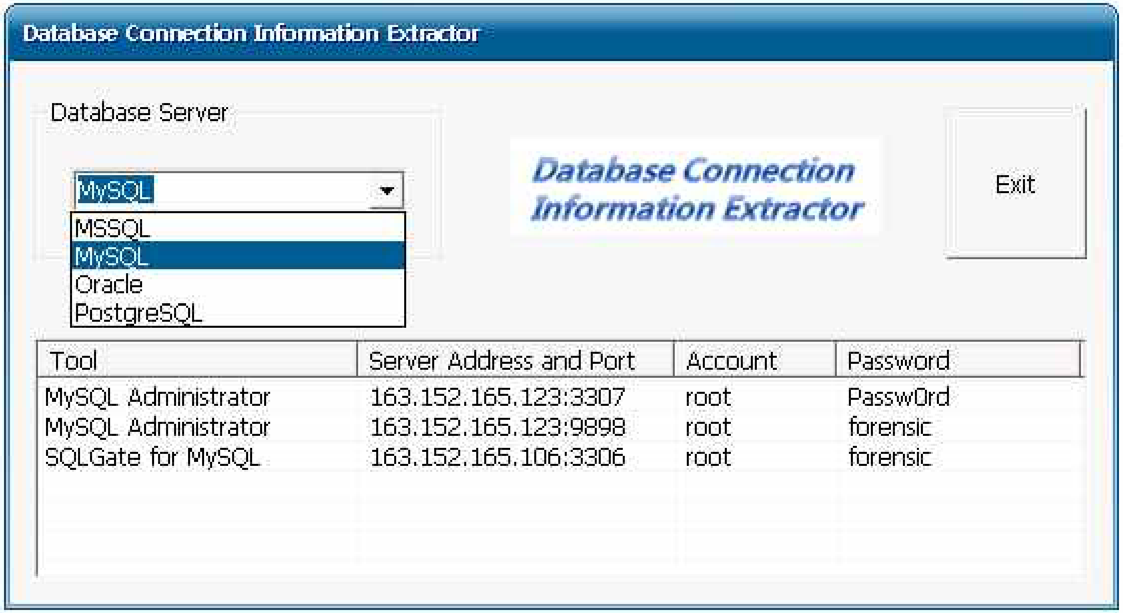
- 설정파일 (dblogin.ini) – Base64 이용



```
dblogin.ini of SQLGate for MSSQL Professional
[login]
item_count=1
item_1=c2E=,Zm9yZW5zaWN=,Q0lTVC02RjlCNzQ3NTYzXEZPUkVOU0lDREIz,bWFzdGVy,U1FMIFNlcnZlcn==,
recent_login=c2E=,Zm9yZW5zaWN=,Q0lTVC02RjlCNzQ3NTYzXEZPUkVOU0lDREIz,bWFzdGVy,U1FMIFNlcnZlcn==,

dblogin.ini of SQLGate for MySQL
[login]
item_count=1
item_1=root,Zm9yZW5zaWN=,163.152.165.106,3306,forensicdb,,22,,,3306,localhost,3306,NONE,0
recent_login=root,Zm9yZW5zaWN=,192.168.47.134,3306,forensicdb,,22,,,3306,localhost,3306,NONE,0
```

Database Connection Information Extractor



Database Server: MySQL

Tool	Server Address and Port	Account	Password
MySQL Administrator	163.152.165.123:3307	root	Passw0rd
MySQL Administrator	163.152.165.123:9898	root	forensic
SQLGate for MySQL	163.152.165.106:3306	root	forensic

Messengers

- MSN Messenger
- NateOn
- Yahoo Messenger
- Misslee Messenger
- BuddyBuddy
- …

공개 불가

향후 연구 토의

향후 연구 토의

1. 대상 프로그램 선정
2. 개발언어, 코딩규칙 및 개발환경(코드공유 등)
3. 발생 가능한 법적 이슈 검토

Q&A