Домен Active Directory - постоянно блокируются учетные записи

Все началось с того что пара пользователей стали регулярно блокироваться. Стандартный поиск по «Просмотр событий» показал вот такую картину:

```
Компьютер попытался проверить учетные данные учетной записи.

Пакет проверки подлинности: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Учетная запись входа:    TESTER
Исходная рабочая станция:
Код ошибки: 0xc000006a
```

Хочется отметить, что «Исходная рабочая станция» - пусто, никаких данных нет.

Так же в логах присутствовали коды ошибок 0xc000006a и 0xc0000234

Интернет подсказал что они означают:

```
0xc000006a — An invalid attempt to login has been made by the following
user.
0xc0000234 — The user account has been automatically locked because too many
invalid logon attempts or password change attempts have been requested.
```

Гугление и чтение умных и полезных статеек (например вот: https://habrahabr.ru/company/netwrix/blog/148501/) привели к необходимости включить расширенный лог - на контроллерах домена включил

```
nltest /dbflag:0x2080ffff
```

не забыть потом выключить командой

```
nltest /dbflag:0x0
```

и начал анализировать результат в файле C:\Windows\debug\netlogon.log руками или чем-то вроде

```
type C:\Windows\debug\netlogon.log | findstr MYLOGIN
```

И источник проблемы был найден - из дружественного домена приходило огромное количество запросов на авторизацию, нечто вроде:

```
10/13 21:32:39 [LOGON] MY-DOMAIN: SamLogon: Transitive Network logon of MY-
DOMAIN\TESTER from  (via DC03) Entered
10/13 21:32:39 [LOGON] MY-DOMAIN: SamLogon: Transitive Network logon of MY-
DOMAIN\TESTER from  (via DC03) Returns 0xC000006A
```

Понятно, работает какая-то зараза. Ну что же - мяч не на нашей стороне и это уже хорошо.

Через некоторое время коллеги ответили - действительно, долбились через их RDP-сервера. Прикрутили скриптик, блокирующий перебирателей и наступила тишина. Кстати, на свежеподнятом linux-сервере я всегда первым делом ставлю fail2ban, это уже рефлекс.

Решений существует куча, например:

- ipban - https://github.com/digitalruby/ipban
- RDP Defender 2.4
- EvlWatcher - http://nerderies.blogspot.com/
- fail2ban - http://dmurr.ru/fail2ban-%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0-%D1%81-nat-rdp/
- fail2ban - https://wqweto.wordpress.com/2013/12/10/how-to-use-fail2ban-with-terminal-servers-rdsh-farm/
- http://nerderies.blogspot.com/2012/12/automatically-banning-ips-with-windows.html
- https://cyberarms.net/security-insights/security-lab/remote-desktop-logging-of-ip-address-(security-event-log-4625).aspx - Introducing TLS/SSL as Remote Desktop authentification, Windows does not log the source IP address of the failed login anymore. Within the event log you will just find the audit failure 4625 with NULL SID and no IP address.
- http://psscripts.blogspot.com/2012/12/automatically-block-rdp-attacks-on-your.html

Как вариант защиты пользователей - можно разрешить вход только с определенных компьютеров чтобы обезопасить учетные записи (Учетная запись пользователя → Свойства → Учетная запись → Вход на... → Только на указанные компьютеры).

rdp, block, блокировка учетных, записей, блокировка пользователей, 0xc000006a, 0xc0000234, MICROSOFT AUTHENTICATION PACKAGE V1 0, перебор паролей, evil watcher