«DCShadow» – это техника скрытого внедрения изменений в базу Active Directory, при которой атакующий временно регистрирует свою машину как контроллер домена и осуществляет подмену атрибутов объектов через механизм репликации. В отличие от «DCsync», которая запрашивает данные, «DCShadow» внедряет данные в AD, не вызывая стандартных путей журналирования (LSASS, LDAP и т.д.).

Для выполнения атаки «DCShadow» необходима учётная запись с правами «Domain Admin» или эквивалентными (для регистрации фейкового контроллера).

На рисунке 1 представлен процесс подготовки команды lsadump::dcshadow, в которой указывается объект (создаваемый пользователь), его атрибуты и местоположение в AD.

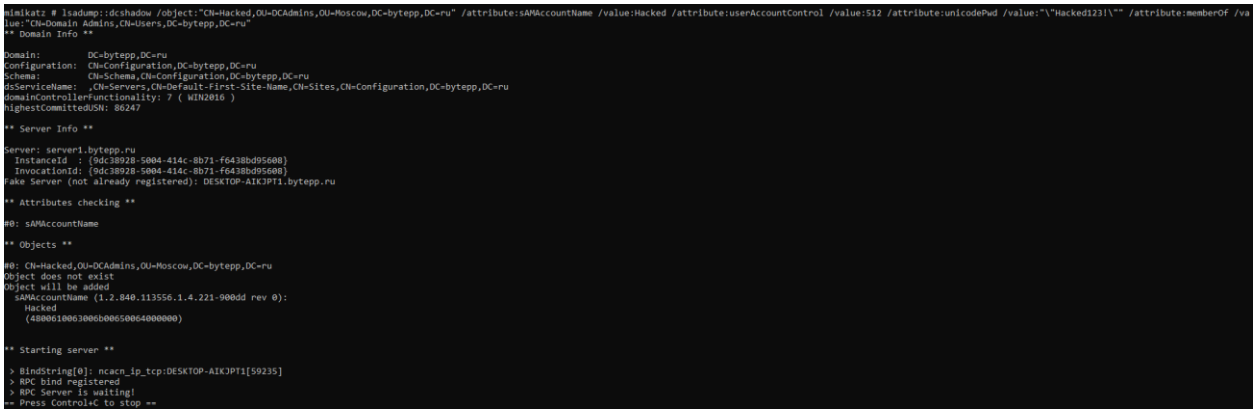

Рисунок 1 – Первый этап исполнения «DCshadow»

В отдельном окне запускается команда lsadump::dcshadow /push, после чего контроллер принимает изменения, считая атакующую машину легитимным источником репликации. На рисунке 2 отображён вывод команды push.

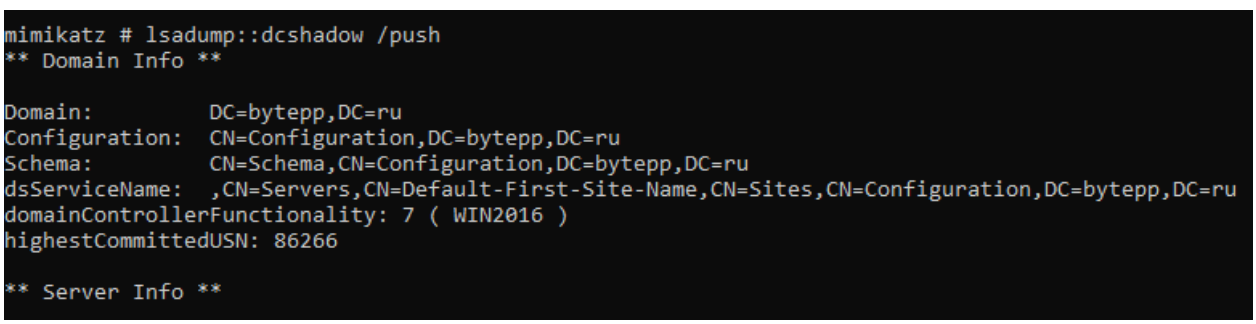

Рисунок 2 – Второй этап исполнения «DCshadow»

В результате атаки в AD появляется новый объект «CN=Hacked», обладающий административными правами. Этот объект можно проверить через Active Directory Users and Computers или с помощью PowerShell (Get-ADUser). На рисунке 3 можно заметить, что новый пользователь был создан.

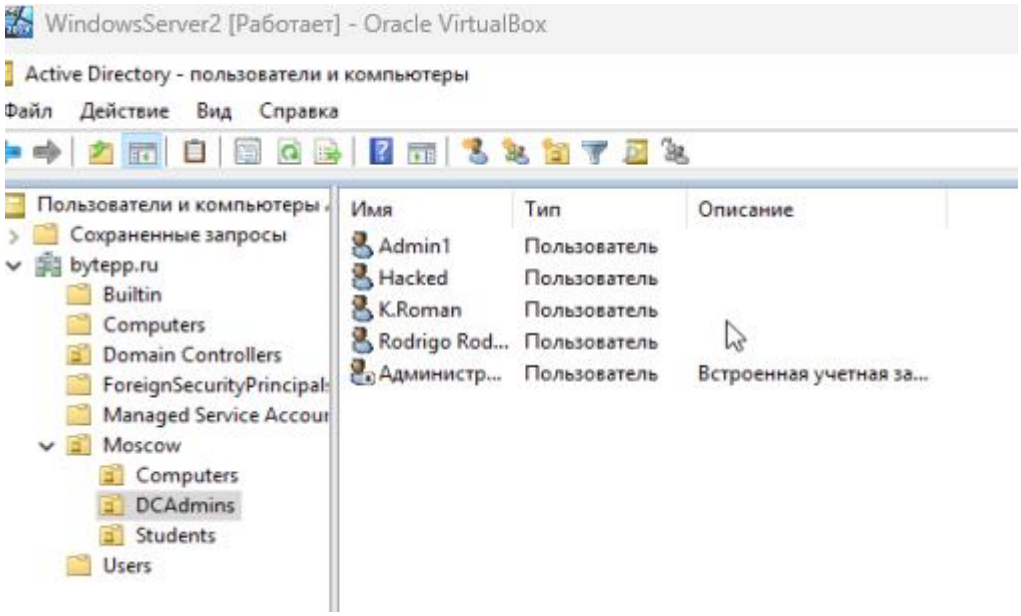

Рисунок 3 – Новый пользователь был создан

Теперь потенциальный злоумышленник может залогиниться под учёткой доменного админа в целевом домене и совершать вредоносные действия.

На рисунке 4 приведён скриншот из дампа сетевого трафика, который был записан во время исполнения атаки «DCshadow».

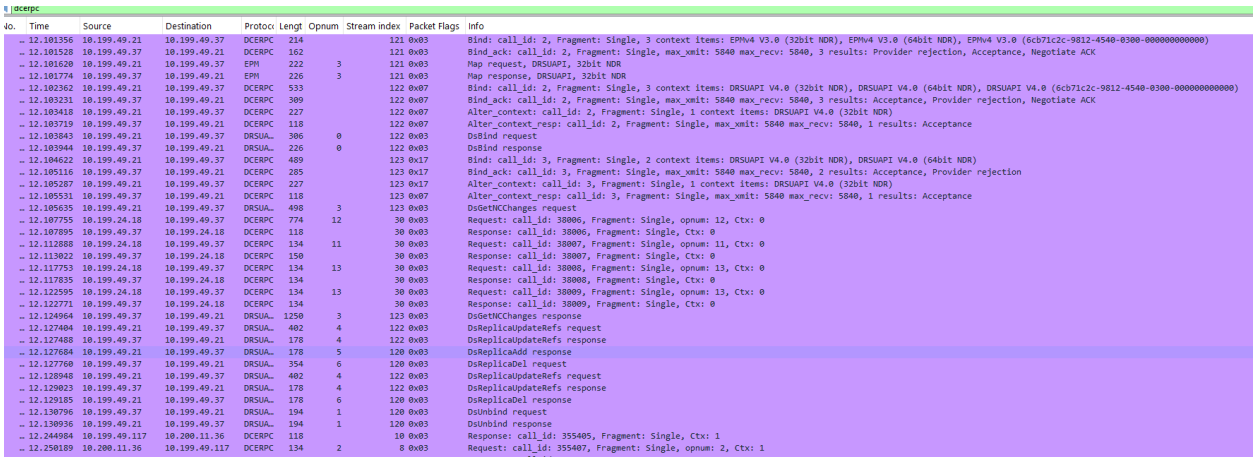

Рисунок 4 – Запись сетевого трафика при атаке «DCshadow»

В ходе атаки «DCShadow» поддельный контроллер домена инициирует соединение со службой репликации по протоколу «DRSUAPI» с легитимным

«КД», начиная с «DsBind», чтобы установить RPC-соединение. Далее через «DsAddEntry» в каталог «Active Directory» внедряется новый объект (В нашей случае – Администратор домена), после чего используется функция «DsReplicaAdd» для добавления сведений о поддельном «КД» в repsFrom легитимного «КД».

После получения запроса о добавлении нового объекта целевой «КД» отправляет запрос поддельному «КД» для запуска репликации с помощью функции «DsGetNCChanges». Параллельно с этим легитимный «КД» совершает обновление списка «repsFrom» и как бы сообщает поддельному «КД»: мы устанавливаем доверительные отношения для репликации.

По трафику видно, что репликация была успешно завершена («DsReplicaAdd response»). Затем поддельный «КД» инициирует зачистку следов своего присутствия через функцию «DsReplicaDel» и разрывает соединение.

По журналам безопасности Windows достаточно сложно задетектировать данную атаку. Попытки атаки «DCShadow» могут быть детектированы по журналу событий контроллера домена, особенно в случае ошибок при передаче некорректных данных. Характерные признаки включают события 1168 («Active Directory Domain Services error») с кодами ошибок 8442 (0x20FA) или 1726 (0x6BE), а также 1481 («Attribute Error») с указанием атрибута «nTSecurityDescriptor» и проблемой «CONSTRAINT_ATT_TYPE». Такие ошибки возникают, например, при передаче некорректного «DACL» без владельца объекта и указывают на попытку низкоуровневого изменения реплицируемых объектов, что не характерно для стандартной административной активности.

Событие 1168 (рисунок 5) – это общее сообщение об внутренней ошибке AD DS, которое говорит о том, что служба каталогов столкнулась с фатальной или некорректно обработанной ситуацией. Появляется, если попытка внедрить объект через поддельный DC завершается с ошибкой – например, при передаче

недопустимого значения атрибута, нарушении логики схемы или ошибке RPC при имитации push-репликации.

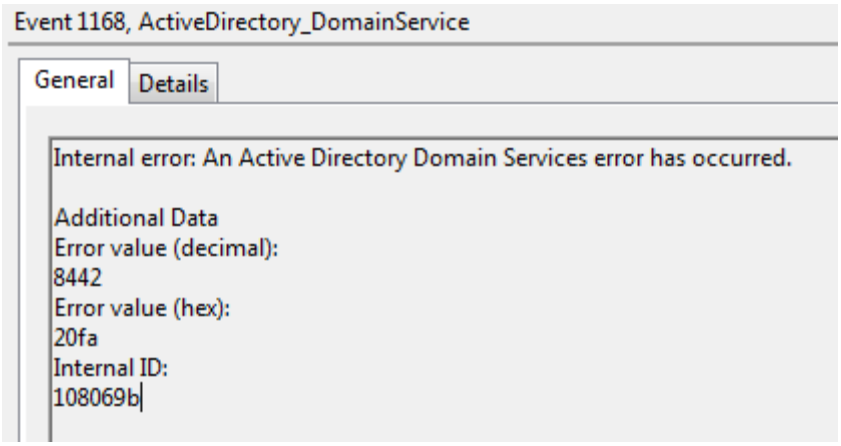

Рисунок 5 – Событие 1168

Event ID 1481 – это сообщение говорит о сбое при модификации атрибутов объекта «AD», вызванном нарушением ограничений схемы или формата данных. В случае «DCshadow» – это, как правило, атрибут nTSecurityDescriptor, отвечающий за права доступа (DACL, SACL, владелец и т.п.). Ошибка problem 1005 («CONSTRAINT_ATT_TYPE») говорит о том, что атрибут нарушает ограничения по типу или структуре, установленные в схеме «AD». В контексте «DCshadow» это часто происходит, если злоумышленник пушит объект с пустым или некорректным владельцем или «DACL» нарушает заданный формат (рисунок 6).

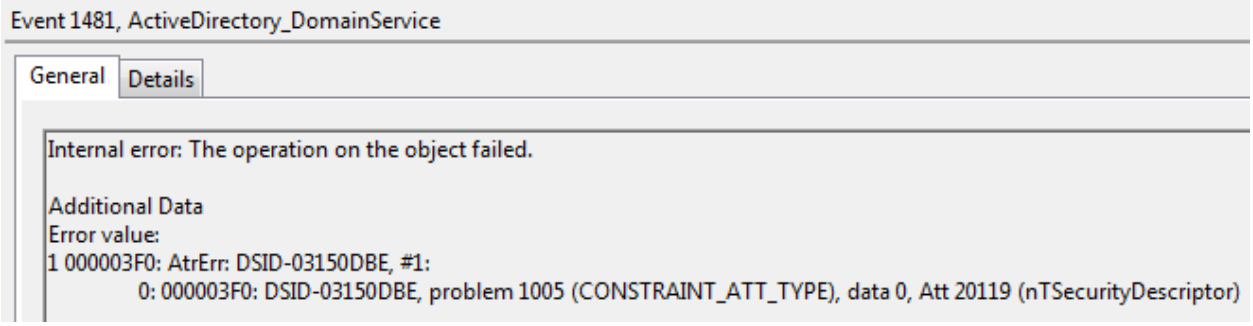

Рисунок 6 – Событие 1481

Наиболее лучшим решением для детектирования и предотвращения атаки будет детектирование на уровне сети. Ниже приведены правила для IDS «Suricata»:

alert tcp any any -> any any (msg: " [Rodrigo] RPC Bind detected"; content: "|05 00 0B|"; depth: 3; content: "|35 42 51 E3 06 4B D1 11 AB 04 00 C0 4F C2 DC D2|"; distance: 0; flowbits: set, DCshadowfirst; flowbits: noalert; sid: 1337; rev: 1;)

alert tcp any any -> any any (msg: "[Rodrigo] DCShadow Replication detected"; content: "|05 00 00 03|"; depth: 4; content: "|05 00|"; distance: 18; within: 2; flowbits: isset, DCshadowfirst; sid: 1338; rev: 1;)

Первое правило детектирует установку RPC-соединения по интерфейсу «DRSUAPI «(репликация «AD») через сигнатуру Bind-запроса, и помечает поток с помощью flowbits; второе срабатывает только если соединение уже помечено первым правилом, и фиксирует попытку вызова функции «DsReplicaAdd», характерную для атаки «DCShadow».