RED Systems Management & NotPetya (Petna) Ransomeware

Крис Стонефф

Произошла новая вспышка вредоносного ПО, названная такими именами, как NotPetya и Petna (и все же Petya, даже если это не Petya :). Вредонос, по-видимому, является эволюцией WannaCry ransomware. После доступа вредоносная программа заражает системы, которые уязвимы для MS17-010 и распространяется по инфраструктуре Windows.

Более подробную информацию о бюллетене по безопасности Microsoft MS17-010 можно найти здесь: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

Процесс заражения

NotPetya начинает свой процесс, создавая/изменяя файл в каталоге% windir% под названием «perfc» без расширения файла. Затем он пытается загрузить и впоследствии использовать встроенный инструмент SysInternals под названием PSEXEC.EXE. Этот файл встроен в другой файл с именем «DLLHOST.DAT», который также записывается в каталог% windir%.

Если PSEXEC не может быть использован, он также использует инструмент инструмента командной строки WMI (WMIC.exe), доступный на всех современных системах Windows, после Windows NT 4.

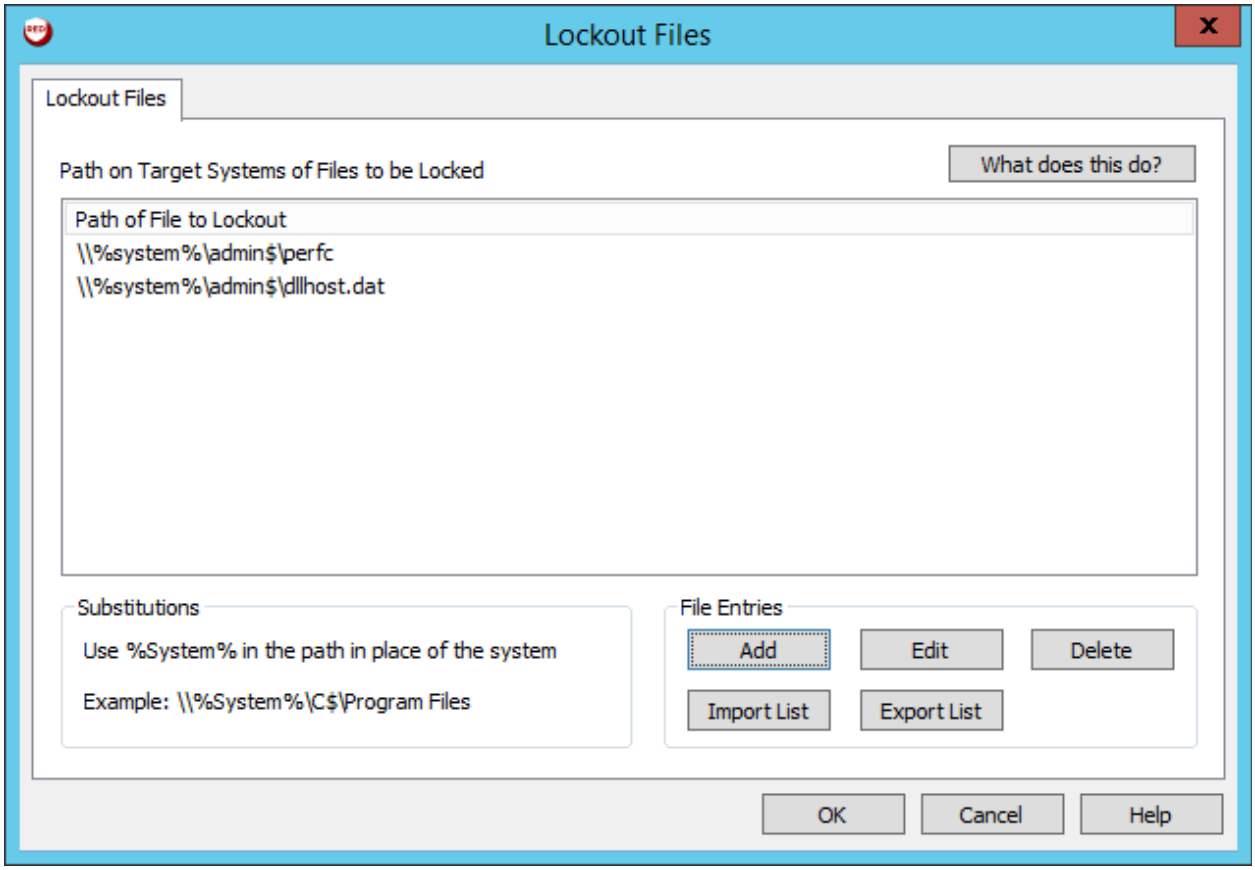
Затем этот процесс использует измененную версию mimikats для извлечения сетевых учетных данных, кэшированных в запущенной системе, чтобы начать процесс заражения последующих систем. Короче говоря, в нем используется тот факт, что многие организации используют плоские, физически связанные сети, в которых администратор с любой машины может управлять другими машинами или воровать из памяти учетные данные администратора домена памяти, до тех пор, пока сеть полностью не будет контролироваться,

Надо сказать, что само присутствие работающего в сети RED Lieberman значительно затрудняет захват контроля сети за счет частой смены паролей, и, соответственно обесценивания воровства кэшей паролей из памяти машин.

Как остановить заражение до того, как оно начнется:

Используйте RED Systems Management, доступный сам по себе или как часть пакета (RED), чтобы быстро блокировать доступ к файлам, которые NotPetya использует для заражения.

1. Открыть RED Systems Management.
2. Откройте свой набор управления со всеми вашими системами Windows.
3. Нажмите «Управление» | Операции с файлами | Блокировка файлов (Cratering).
4. Нажмите «Добавить».
5. В Путь к файлу на удаленной машине введите: \\% system% \ admin $ \ perfc
6. Нажмите «ОК».
7. Нажмите «Добавить» еще раз.
8. В Путь к файлу на удаленной машине введите: \\% system% \ admin $ \ dllhost.dat
9. Нажмите «ОК», чтобы закрыть диалог с файлами.
10. Нажмите «ОК», чтобы заблокировать файлы.



Когда вы нажмете OK, RED Systems Management будет подключаться ко всем целевым машинам. Если файлов нет, вместо них будут созданы пустые файлы. Затем ACL в файле будет изменен на DENY EVERYONE FULL CONTROL.

Дополнительно:

Вы должны не только защитить свои компьютеры, чтобы остановить эксплойты SMB с исправлениями, описанными в MS17-01, Вам нужно поработать с устаревшими проблемами SMB

Вы должны отключить SMBv1 (Надеемся, Вы уже избавились от всех своих 2003, XP и более ранних систем сразу, как они перестали поддерживаться).

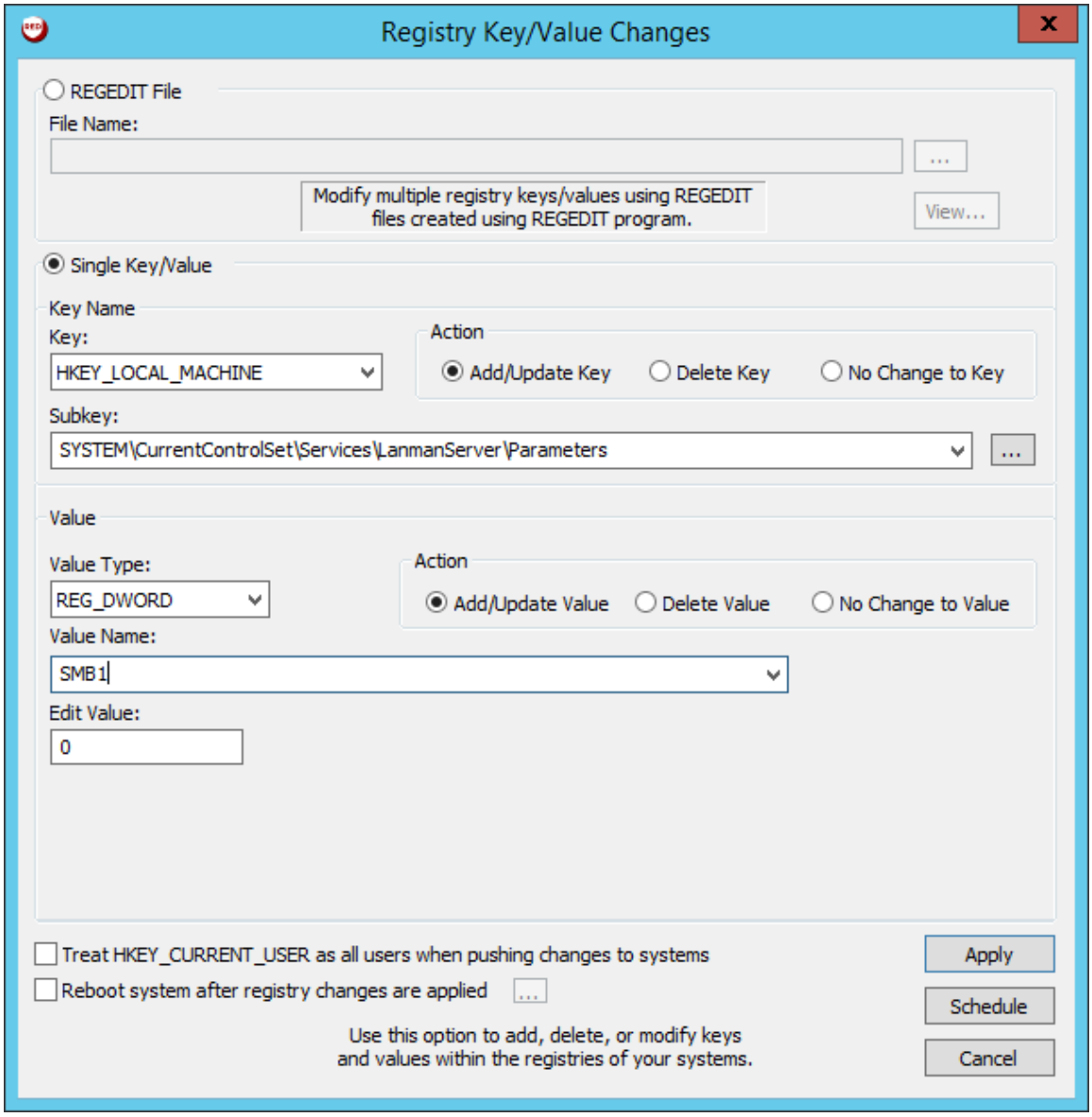
Управление версиями SMB контролируется записями реестра, которые могут быть заданы в настройках групповой политики Active Directory. Для получения дополнительной информации см. Https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/

К сожалению, средство групповых политик не дает отзывов об успешности или неудаче применения политики и может пройти несколько часов до вступления политики в силу. RED Systems Management может проактивно и немедленно обрабатывать изменения с помощью функции REGEDIT. Это обеспечивает немедленную обратную связь об успехе или отказе, а также может подтвердить успешность изменений верификацией реестром.

Чтобы использовать RED Systems Management для отключения серверных компонентов SMBv1 (будьте осторожны, поскольку устаревшие системы, такие как Server 2003 и XP и более ранние, не могут работать без него!), выполните следующие действия:

1. Откройте RED Systems Management.
2. Откройте свой набор управления со всеми вашими системами Windows.
3. Выберите целевые системы (не забудьте включить XP / 2003 и более ранние системы!)

4. Нажмите кнопку REGEDIT в левом нижнем углу диалогового окна.
5. Установите тип: Single Key / Value
6. Задайте имя ключа: HKEY_LOCAL_MACHINE
7. Установите действие: Добавить / Обновить ключ
8. Установите подраздел: SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters
9. Задайте тип значения: REG_DWORD
10. Задайте имя значения: SMB1
11. Установите для поля «Изменить значение» значение: 0
12. Нажмите «Применить».



Удалите постоянный привилегированный доступ администратора

RED Systems Management может использоваться для активного управления членством в локальных и доменных привилегированных группах. Этот процесс помогает остановить повторное использование учетных данных с высокими привилегиями. Эти элементы управляются множеством способов с использованием функций «Локальное членство» и «Глобальное членство» в RED Systems Management.

Если позднее требуется доступ с повышенными привилегиями - используйте RED Identity Management (RED IM: https://liebsoft.com/red-identity-management/), чтобы временно предоставить учетной записи членство в группе с минимальными привилегиями, а затем удалить эту привилегию, автоматически лишив членства в группе по истечении установленного времени или окончания работы. Этот процесс может быть полностью самообслуживаемым или быть привязанным к процессу документооборота, а также контролироваться аудиторами, подтверждающими заявки на повышение привилегий.

Используйте RED Identity Management для рандомизации паролей неперсонифицированных служебных и сервисныз учетных записей. RED IM также может помочь вам избежать предоставления постоянного доступа к учетным записям с наивысшими привилегиями (например, входящим в группу администраторов домена), который позволяет распространяться вредоносному ПО, извлекающим учетные данные из активных сеансов или сохранённых хешей, предоставляя доступ только к выбранной учетной записи или предоставляю доступ к уже запущенному приложению, с испозованием выбранной УЗ.