KASPERSKY lab

Информация по ВПО WannaCry и инструкции по борьбе с ним

Оглавление

1. Информация по ВПО WannaCry

Специалисты «Лаборатории Касперского» проанализировали информацию о заражениях программой-шифровальщиком, получившей название “WannaCry”, с которыми 12 мая столкнулись компании по всему миру. Как показал анализ, атака происходила через известную сетевую уязвимость Microsoft Security Bulletin MS17-010. Затем на зараженную систему устанавливался руткит, используя который злоумышленники запускали программу-шифровальщик.

Все решения «Лаборатории Касперского» детектируют данный руткит как MEM:Trojan.Win64.EquationDrug.gen. Решения Лаборатории Касперского также детектируют программы-шифровальщики, которые использовались в этой атаке следующими вердиктами:

- Trojan-Ransom.Win32.Scatter.uf
- Trojan-Ransom.Win32.Scatter.tr
- Trojan-Ransom.Win32.Fury.fr
- Trojan-Ransom.Win32.Gen.djd
- Trojan-Ransom.Win32.Wanna.b
- Trojan-Ransom.Win32.Wanna.c
- Trojan-Ransom.Win32.Wanna.d
- Trojan-Ransom.Win32.Wanna.f
- Trojan-Ransom.Win32.Zapchast.i
- Trojan.Win64.EquationDrug.gen
- PDM:Trojan.Win32.Generic (для детектирования данного зловреда компонент «Мониторинг системы» должен быть включен)

Мы рекомендуем компаниям предпринять ряд мер для снижения рисков заражения:

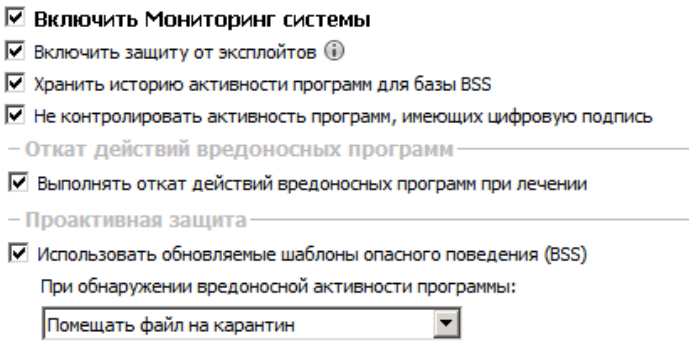
- **Установить официальный патч от Microsoft, который закрывает используемую в атаке уязвимость**
- Убедиться, что включены защитные решения на всех узлах сети
- Обновить базы всех используемых продуктов «Лаборатории Касперского»

Эксперты «Лаборатории Касперского» анализируют образцы вредоносного ПО для установления возможности расшифровки данных.

Более подробную информацию об атаках “WannaCry” можно найти в отчете «Лаборатории Касперского» https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

2. Что делать, если произошло заражение?

1. Отключить зараженный хост от корпоративной сети
2. Установить официальный патч от Microsoft:
    - Для поддерживаемых ОС: https:/technet.microsoft.com/en-us/library/security/ms17-010.aspx
    - Для устаревших ОС: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
3. Если используется защитное решение «Лаборатории Касперского», убедиться, что компонент «Мониторинг Системы» и все его модули включены:

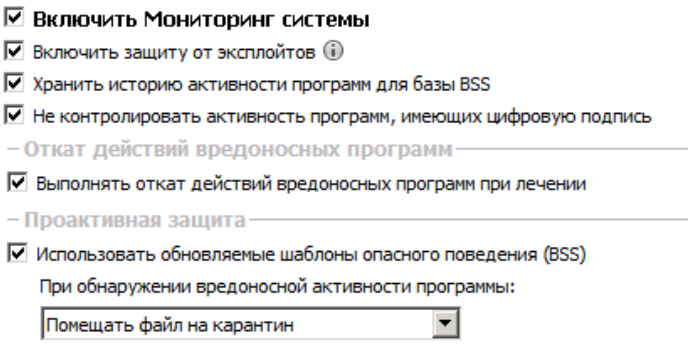


4. Убедиться, что включен компонент «Защита от сетевых атак»
5. Запустить задачу сканирования критических областей в защитном решении «Лаборатории Касперского», чтобы обнаружить возможное заражение как можно раньше
6. После детектирования MEM:Trojan.Win64.EquationDrug.gen, произвести перезагрузку системы
7. Выполнить полную проверку на вирусы, чтобы удалить ВПО
8. Подключить хост к сети

Если используется стороннее Антивирусное решение, для проверки можно воспользоваться [Kaspersky Rescue Disk]

3. Что делать, чтобы не допустить заражения?

1. Установить официальный патч от Microsoft:
    - Для поддерживаемых ОС: https:/technet.microsoft.com/en-us/library/security/ms17-010.aspx
    - Для устаревших ОС: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
2. Если используется защитное решение «Лаборатории Касперского», убедиться, что компонент «Мониторинг Системы» и все его модули включены:



3. Убедиться, что включен компонент «Защита от сетевых атак»

4. Централизованное распространение обновления от Microsoft с помощью Kaspersky Security Center

Основной метод:

1. Загрузить необходимые обновления с ресурсов Microsoft:
    - Для поддерживаемых ОС: https:/technet.microsoft.com/en-us/library/security/ms17-010.aspx
    - Для устаревших ОС: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

2. Создать на локальном диске временный каталог и поместить туда загруженные файлы (*.msu)
3. Во временном каталоге создать bat файл и прописать в нем команду вида:
   wusa.exe %updatename%.msu /quiet /warnrestart
   %updatename% - имя файла обновления

   Данная команда предписывает провести установку обновления, не показывая процесс пользователю, но потом выводит запрос на перезагрузку и дает около минуты на сохранение открытых файлов (отказаться от перезагрузки нельзя). Если прописать forcerestart вместо warnrestart - то ПК будет принудительно перегружен немедленно, а открытые приложения - закрыты с потерей данных.

   В итоге во временном каталоге должен быть bat файл и необходимые файлы msu

   Важно: если команду запустить на ПК, где уже стоит обновление или где оно не подходит - ничего страшного не произойдет.

4. В Kaspersky Security Center перейти в раздел "Удаленная установка\Инсталляционные пакеты", и там выбрать опцию "Создать инсталляционный пакет".

5. Создать инсталляционный пакет, который будет вызывать созданный bat файл, при этом обязательно включить опцию галочку "копировать всю папку в инсталляционный пакет" - это приведет к тому, что MSU файлы будут включены в пакет
   Дополнительно: В bat файле можно указать установку нескольких обновлений и поместить их все в во временный каталог, но в таком случае размер установочного пакета будет больше.
6. Созданный пакет установить на ПК. Это можно сделать из выборки ПК по типу ОС (выбрать любую группу ПК, в меню по правой кнопке "Установить программу"), можно создать задачу для группы ПК (в "Управляемые ПК" выбрать корень списка или определенную группу, там закладка "Задачи", создать задачу по установке, либо другим привычным Вам способом.
   Пакет так же можно установить локально.

Альтернативный метод:

Условия работы:

1. Наличие Расширенной лицензии на продукт
2. Использование задачи Поиска уязвимостей и обновлений для ПО Microsoft

Выполнение:

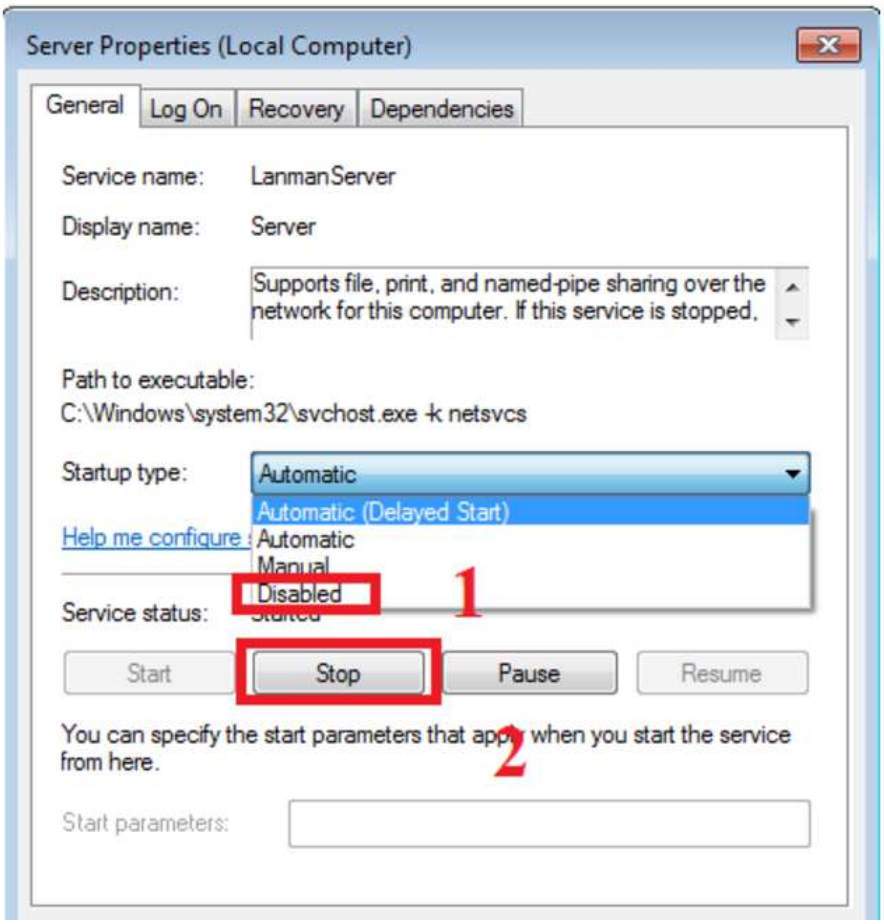
1. Перейти в раздел «Дополнительно-Управление программами-Обновление»
2. В строке поиска найти необходимое обновление Microsoft
3. Нажать правой кнопкой на обновление и выбрать пункт «Установить обновление»
4. Выполнить установку на необходимые хосты

5. Безопасное включение хостов без обновления Microsoft

Для безопасного включения компьютеров необходимо сделать следующее:

1. Отключить компьютер от сети организации (вытащить сетевой кабель)

2. В настройках сервисов отключить службу Server:



3. Подключить сетевой шнур и произвести обновление ОС со всеми перезагрузками (чтобы система не предлагала больше ничего поставить (!))
4. После этого службу Server можно включить
5. Убедиться, что в Kaspersky Endpoint Security включены компоненты:

- Мониторинг системы
- Защита от сетевых атак