Методические рекомендации по противодействию ВПО WanaCry

Рекомендации по противодействию в информационных системах, подключенных к сети общего пользования Интернет

1. Установить для открытых информационных систем, имеющих подключение к сети Интернет, обновление безопасности для Windows KB4013389 от 14 марта 2017 года.

2. Заблокировать входящий трафик на межсетевом экране, по портам SMB (139 и 445).

3. Внести в чёрный список на межсетевом экране используемые ВПО IP-адреса и домены:

- 188.166.23.127:443
- 188.166.23.127:443
- 193.23.244.244:443
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001
- 217.79.179.77
- 128.31.0.39
- 213.61.66.116
- 212.47.232.237
- 81.30.158.223
- 79.172.193.32
- 89.45.235.21
- 38.229.72.16
- 188.138.33.220
- 197.231.221.221:9001
- 128.31.0.39:9191
- 149.202.160.69:9001
- 46.101.166.19:9090
- 91.121.65.179:9001
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001
- 217.79.179.177:9001
- 213.61.66.116:9003

- 212.47.232.237:9001
- 81.30.158.223:9001
- 79.172.193.32:443
- 38.229.72.16:443
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- Rphjmrpwmfv6v2e.onion
- Gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

4. Установить актуальные обновления баз данных компьютерных вирусов к антивирусным средствам и осуществить полную проверку средства вычислительной техники.

5. Для минимизации ущерба (предотвращения шифрования в случае заражения), выполнить резервное копирование чувствительных файлов в форматах:

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg, .psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg, .pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot, .docm, .docx, .doc

Рекомендации при наличии подозрения на зараженность ВПО WanaCry

Перед началом работы на средстве вычислительной техники.

1. Загрузить средство вычислительной техники (далее – СВТ) с использованием загрузочного диска (Live-CD, Live-USB), размещенного на официальных сайтах производителей антивирусных средств (далее - АВС), например, АО «Лаборатория Касперского», ООО «Доктор Веб».

2. Обновить базы данных компьютерных вирусов (далее – БДКВ) АВС с использованием функциональных возможностей Live-CD (описание порядка действий приведено на диске).

3. Внести изменения в настройки АВС (установить режим – информирование о зараженных объектах).

4. Провести полную проверку жестких дисков.

5. При выявлении фактов заражения носителей информации ВПО таких как:

1) Trojan-Ransom.Win32.Scatter.uf

2) Trojan-Ransom.Win32.Fury.fr

3) PDM:Trojan.Win32.Generic

4) Trojan-Ransom.Win32.Zapchast.i

5) Trojan-Ransom.Win32.Wanna.c

6) Trojan-Ransom.Win32.Wanna.b

7) Trojan-Ransom.Win32.Agent.aapw

8) Troyan.Encoder.11432

необходимо скопировать на внешний носитель информации все зашифрованные файлы с расширением «.WCRY». (Для расшифровки информации в файлах, после возможного выхода утилиты дешифрования).

Все незашифрованные файлы (при их наличии) с пользовательской информацией следующих расширений:

.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg, .psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg, .pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot, .docm, .docx, .doc

с жесткого диска СВТ скопировать на другой внешний носитель информации.

6. В случае, если ВПО осуществило шифрование критически важной для пользователя информации, необходимо извлечь жесткий диск из СВТ, на случай выхода утилиты дешифрования, использующей в своей работе алгоритмы, применяемые в самом ВПО WanaCry, для последующего восстановления информации.

7. В случае выхода утилиты дешифрования, использующей в своей работе алгоритмы, применяемые в ВПО WanaCry, перед загрузкой зараженной операционной системы, необходимо в BIOSe установить дату и время, соответствующие (максимально приближенные) времени заражения.

8. Дешифровку файлов осуществлять в соответствии с инструкцией по использованию утилиты.

Примечание.

Исходя из принципов функционирования ВПО WanaCry (оригинальный файл удаляется после его шифрования), существует вероятность восстановления удаленных файлов специальным программным обеспечением типа R-Studio.