ООО «Акстел-Безопасность»

630084, г. Новосибирск, ул. Авиастроителей 39 Б
Телефон: +7 (383) 255-3-255
Факс: +7 (383) 311-05-30

ИНН: 5410779213, КПП: 541001001
ОКПО: 44067005,
ОГРН: 1135476117391
БИК 045004850

Приложение №1

1. Краткое описание угрозы

Отличительными особенностями вредоносного программного обеспечения являются:

- Использование уязвимости протоколов SMB v.1, SMB v.2 «EternalBlue» (из архива Shadowbrokers). SMB v.3 по предварительным данным не подвержена указанной уязвимости (данная версия используется, начиная с ОС Windows 8 / Windows Server 2012);
- Функционал сетевого червя: производится поиск соседних устройств в той же локальной сети или смежных сетях, куда имеет доступ зараженное устройство и заражает, в свою очередь, их. Этим объясняется лавинообразное распространение заражений.

При заражении шифруются файлы баз данных, документы и прочие «чувствительные» файлы. Файл для шифрования выбирается по его расширению.

Средства расшифровки на данный момент отсутствуют.

2. Меры противодействия

1. На серверах / пользовательских АРМ: организовать резервирование всех важных файлов с **использованием сторонних средств резервирования** (отличных от «теневых копий» документов Windows и средства восстановления Windows, т.к. данные резервные копии могут быть уничтожены в процессе работы ВПО), обязательно включив в список файлы со следующими расширениями: .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; также рекомендуется включить все файлы баз данных и иные критичные для организации файлы, не перечисленные выше;
2. Установить обновление безопасности для Windows KB4013389 от 14 марта 2017 года (см. Microsoft Security Bulletin MS17-010);

3. В случае невозможности установки патча – следует отключить протокол SMB v1 (v2 и v3 также можно отключить при целесообразности, негативные последствия отключения приведены в таблице ниже). Ниже приведены сведения, как это сделать:
    - На стороне сервера через Power Shell: Set-SmbServerConfiguration -EnableSMB1Protocol $false –Force проверить результат выполнения можно командой Power Shell: Get-SmbServerConfiguration (в строке EnableSmb1Protocol значение будет False). Для полного удаления драйвера протокола SMB v1, следует выполнить команду в Power Shell: Disable-WindowsOptionalFeature –Online –FeatureName SMB1Protocol –Remove и после перезагрузки системы поддержка протокола SMB v.1 будет полностью отключена. Остальные протоколы (SMB v.2, SMB v.3 отключаются аналогично);
    - На стороне клиента:
        - Вариант через Power Shell / CMD: выполнить команду sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi и sc.exe config mrxsmb10 start= disabled.
        - Вариант через GUI: удаление «Клиент для сетей Microsoft» и «Служба доступа к файлам и принтерам сетей Microsoft», а также «Совместный доступ к файлам и принтерам сетей Microsoft» в настройках сетевого подключения.

4. Рекомендуется отслеживать запросы по следующим DNS-именам:
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- Rphjmrpwmfv6v2e.onion
- Gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

Обращение по одному из этих имен означает, что в сети есть инфицированное WannaCry устройство. Вместе с тем, обращение к доменному имени iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com и получение от него ответа о существовании такого доменного имени является для текущей версии ВПО ключевым словом остановки инфицирования (отключения функции сетевого червя), поэтому целесообразно, при наличии технической возможности, организовать положительный отклик о существовании данного домена. По состоянию на 15.05.2017, указанный домен зарегистрирован в Великобритании;

5. Контролировать соединения по портам 139 и 445, блокирование входящего трафика по указанным портам;

6. Общие варианты сигнатур для средств обнаружения вторжения (попытка эксплуатации EnterealBlue):

1	alert smb any any -> $HOME_NET any (msg:”ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)”; flow:to_server,established; content:”|00 00 00 31 ff|SMB|2b 00 00 00 00 18 07 c0|”; depth:16; fast_pattern; content:”|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|”; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity; sid:2024220; rev:1;)
2	alert tcp $HOME_NET 445 -> any any (msg:”ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response”; flow:from_server,established; content:”|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|”; depth:16; fast_pattern; content:”|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|”; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;).

3. При выявлении заражения

В случае, если выявлено заражение, необходимо:

1. Отключить от локальной сети зараженное устройство (устройства) с целью недопущения распространения вируса;

2. Если начат процесс шифрования, то рекомендуется физическое отключение (обесточивание) устройства «грубым» методом – т.е. без попыток корректного завершения работы, после чего изъятие жесткого диска устройства с последующим подключением вторичным (не системным) носителем к компьютеру, не имеющему сетевого доступа с последующим восстановлением (копированием) незашифрованных файлов; пострадавший носитель рекомендуется переформатировать;

3. В случае, если процесс шифрования завершен, можно попытаться восстановить резервные копии файлов, сделанных Windows. Следует иметь ввиду, что данный процесс с большой долей вероятности может завершиться неудачно, поскольку ВПО пытается уничтожить резервные копии, созданные с помощью штатных средств восстановления ОС Windows.

Обращаем внимание, что в случае наличия хотя бы одного зараженного устройства может вызвать лавинообразное распространение по локальной сети данного ВПО и привести к полной неработоспособности всех элементов локальной сети, работающих под управлением ОС Windows.

Рекомендуется не выполнять требования злоумышленников и не производить им никаких выплат. Получение ключа восстановления для дешифровки файлов не гарантируется.