Важная информация: шифровальщик WannaCry

12 мая вредоносное ПО - шифровальщик WannaCry нанесло ущерб сотням организаций в разных странах, в т.ч. в России. Вредоносное ПО зашифровывает персональные и критичные документы и файлы, и требует от жертвы выкуп размером ~ $300 USD в BitCoin для предоставления ключа расшифрования файлов.

Следует заметить, что решения Fortinet успешно блокируют эту атаку

1. FortiGate IPS блокирует эксплоит

2. FortiSandbox выявляет вредоносное поведение

3. Антивирус Fortinet выявляет Wannacry в различных вариантах

4. Веб-фильтр FortiGuard классифицирует веб-сайты, к которым обращается Wannacry, как вредоносные (за исключением домена "kill switch")

5. Межсегментный сетевой экран (ISFW) FortiGate может остановить распространение вредоносного ПО

Wannacry распространяется по принципу сетевого червя, за счёт активного опроса ПК в сети по протоколу SMBv1 и порту 445 с целью выявления ПК, подверженных уязвимости Backdoor.Double.Pulsar Если уязвимость присутствует на ПК-жертве, она используется для доставки и запуска образца вредоносного ПО. Если нет, используется менее результативный способ эксплуатации.

По этой причине, мы рекомендуем организациям временно (до обновления всех подверженных систем) заблокировать порт 445 от соединений извне, а также, при наличии технической возможности, использовать функциональность NGFW для полного блокирования протокола SMB

Вредоносное ПО является модульным Это значит, что оно позволяет злоумышленнику получить административные привилегии на ПК-жертве, что в свою очередь может быть использовано для загрузки дополнительных модулей вредоносного ПО. В одном из случаев, расследованных Fortinet, вредоносное ПО использовало уязвимость CVE-2017-0144 для получения доступа к системе. После этого, был запущен загрузчик (dropper) для загрузки и запуска ПО шифровальщика.

Причиной этой уязвимости является переполнение буфера при разборе некорректно сформированного запроса Trans2 сервисом SMBv1. Успешная эксплуатация приводит к запуску кода в контексте приложения. Для эксплуатации не требуется аутентификация по SMB, именно это явилось основной причиной столь массового распространения Wannacry в локальных сетях.

Backdoor.Double.Pulsar

Если вредоносное ПО определяет, что в системе присутствует Backdoor.Double.Pulsar, оно пытается использовать его для загрузки и выполнения ПО шифровальщика. Что интересно, в некоторых проанализированных образцах присутствовал флаг для отключения DoublePulsar.

Вредоносное ПО загружается на ПК-жертву в виде зашифрованного ключом AES DLL файла. После запуска, вредоносное ПО создаёт файл “t.wry." и использует встроенный ключ AES для расшифрования DLL в буфер оперативной памяти, после расшифровки DLL загружается в родительский процесс - таким образом, расшифрованный DLL файл не сохраняется на диск. Это позволяет избежать детектирования некоторыми антивирусными решениями.

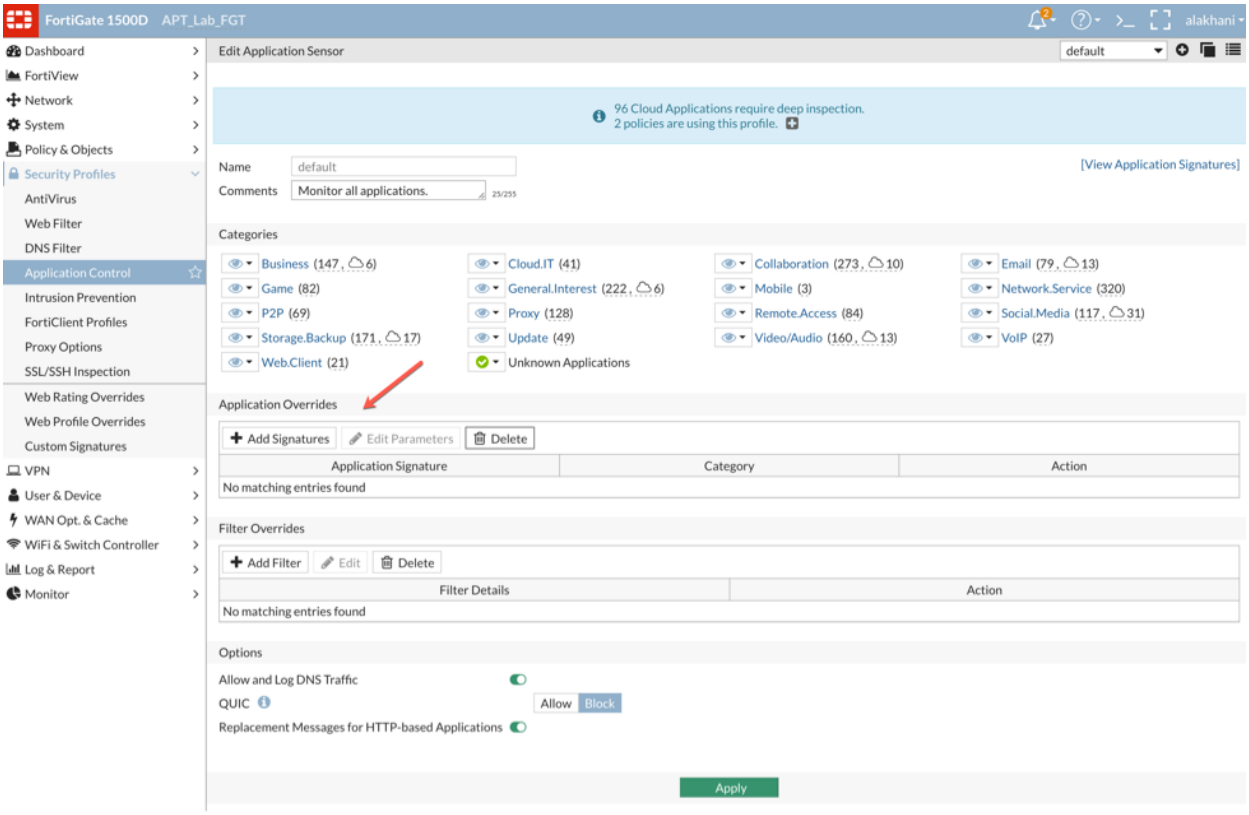
Шифровальщик ищет файлы 179 типов, для каждого файла генерируется ключ.

В субботу, 13 мая, исследователь в области ИБ обнаружил "kill switch" - способ дистанционно выключить вредоносное ПО. Это - DNS проверка и обращение к определенному домену, не зарегистрированному на тот момент. После регистрации, темп заражений сошел на нет, т.к. в большинстве новых случаем заражения вредоносное ПО детектировало доступность созданного домена.

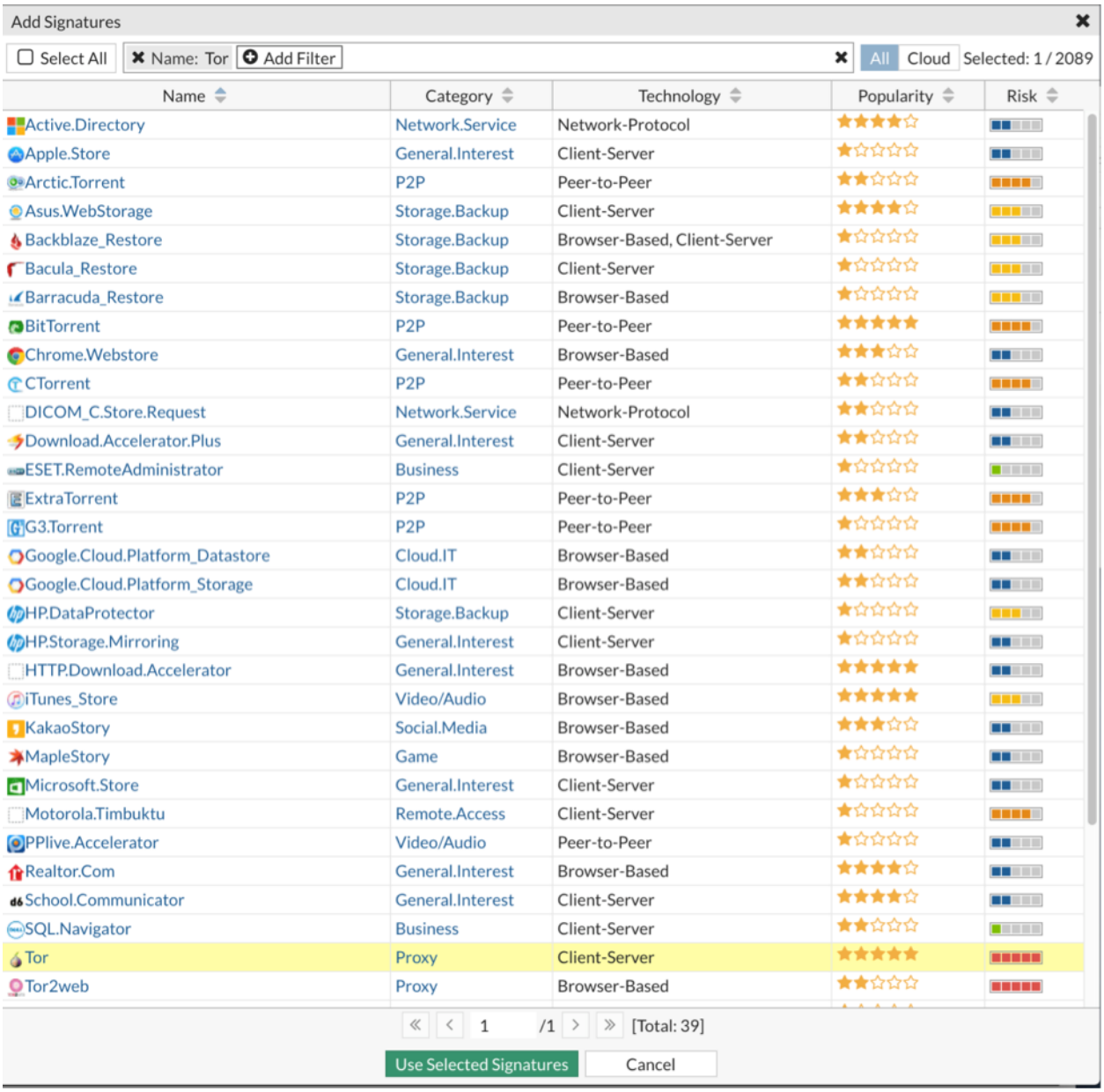
Исходящий TOR

Вредоносное ПО загружает клиент сети анонимизации TOR и использует его для анонимной, зашифрованной коммуникации с серверами управления. Мы рекомендуем блокировать исходящий трафик TOR. Это легко реализовать на FotiGate посредством сигнатур AppControl.

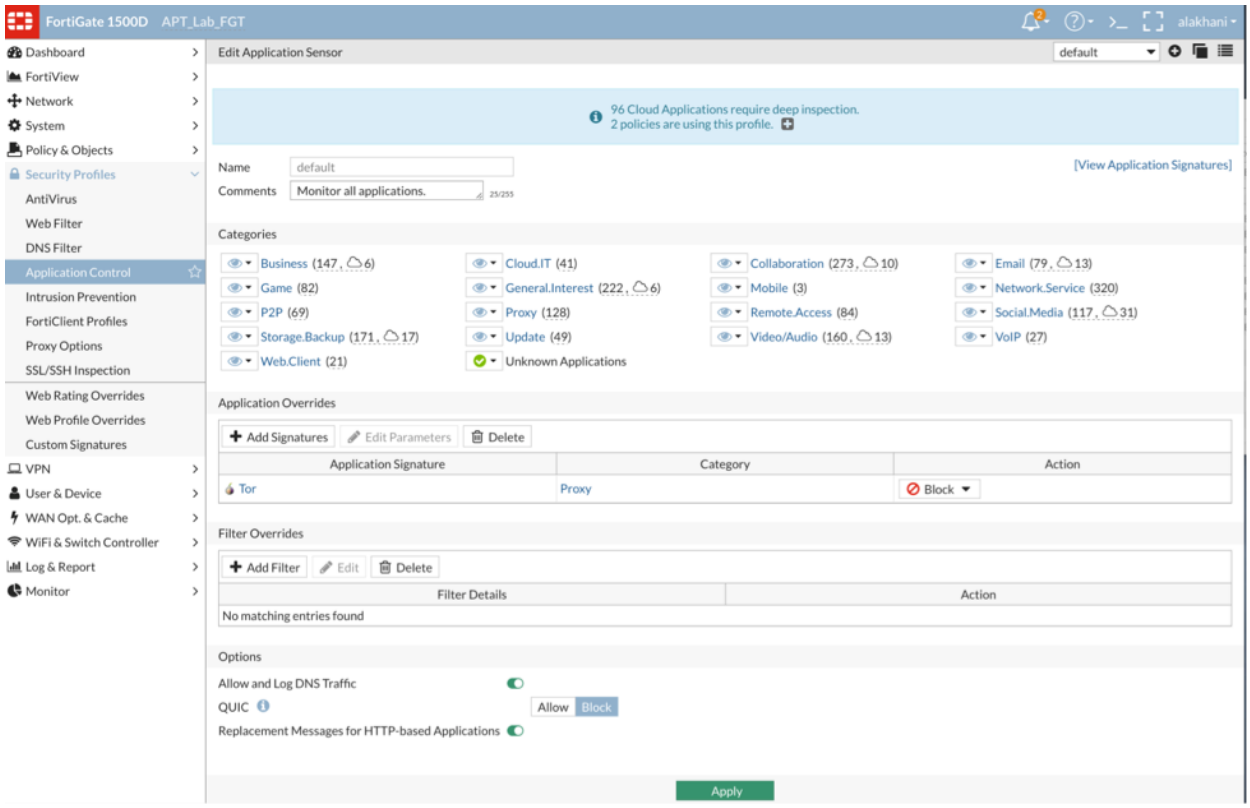
Для настройки перейдите в security profiles -> application control и нажмите add signature в секции Application Overrides.



Добавьте протокол Tor:



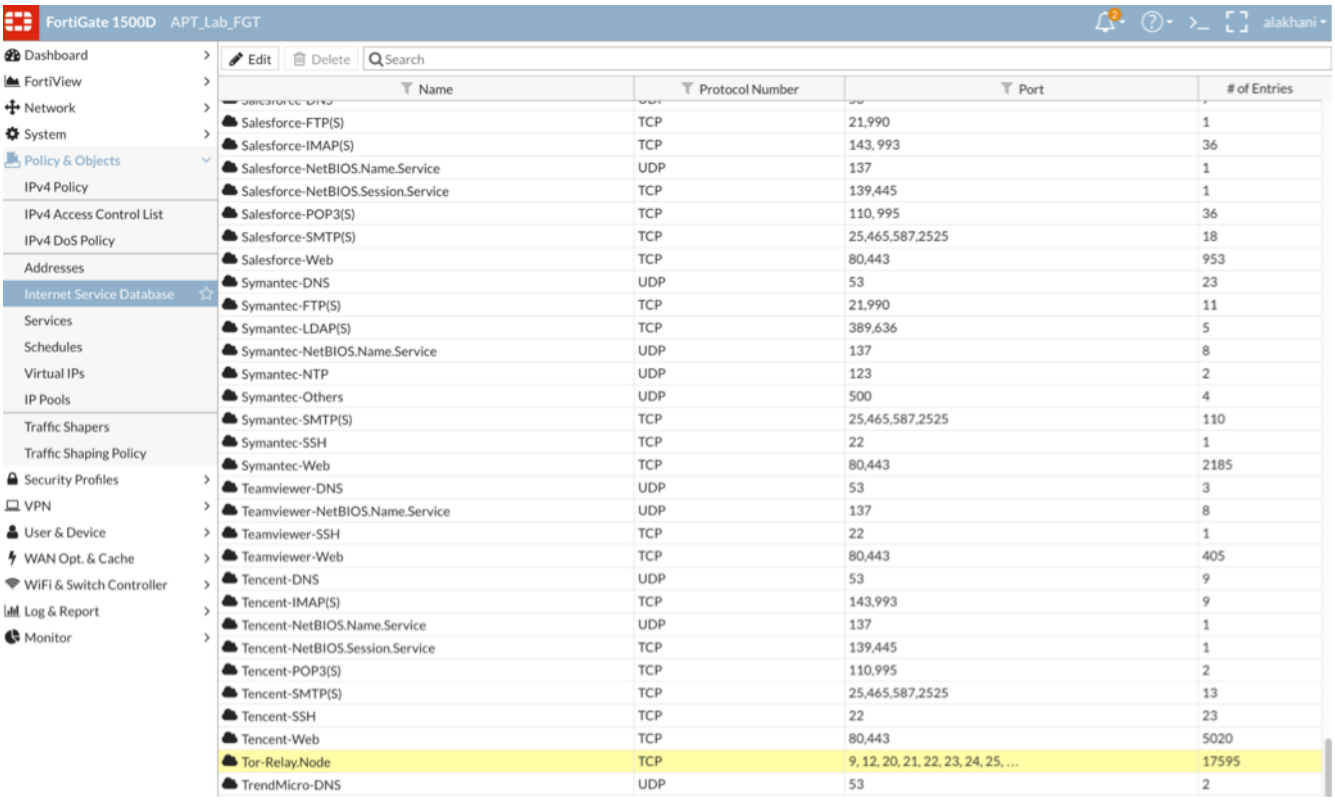
Теперь трафик Tor блокируется профилем.



Убедитесь, что профиль используется в релевантных правилах контроля доступа.

Входящий TOR

Несмотря на то что это не обязательно, также может быть предпринято блокирование трафика, исходящего из сети TOR. Входящий трафик из сети TOR не отличается от обычного Интернет трафика. Тем не менее, трафик исходит от "внешних" узлов TOR - exit nodes. Список известных exit nodes содержится и поддерживается в базе Fortinet Internet Service Database. Этот список может быть использован в правиле контроля доступа.



Если вредоносному ПО разрешен сетевой доступ, оно также попытается установить связь с несколькими доменами с плохой репутацией. Веб-фильтр FortiGuard определяет эти домены как вредоносные (malicious) и, при корректной настройке, должен блокировать коммуникацию с этими доменами в рамках правил контроля доступа.

Kill Switch

Вредоносное ПО останавливает свою активность, если удаётся установить связь с доменом “www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com”. Изначально в момент выявления этот домен не был зарегистрирован, теперь он зарегистрирован исследователем в области ИБ из Великобритании.

Примечание: *Организациям использующим прокси следует учесть, что вредоносное ПО выполняет обращение напрямую. Следовательно, в среде с прокси, вредоносное ПО может не иметь возможности установить связь с указанным доменом, и следовательно, не остановит вредоносную активность.*
Чтобы kill switch сработал, у вредоносного ПО должна быть возможность установить соединение с доменом kill switch. В интересах остановки вредоносного ПО, Fortinet не категоризует домен kill switch как malicious (чтобы предотвратить его блокировку). Следует заметить, что 14 мая появилась информация о новой версии вредоносного ПО, не использующей kill switch - поэтому эту меру не стоит считать панацеей.

По сути, kill switch следует считать временной и более не действующей мерой, т.к. распространение вредоносного ПО продолжается, и в новых образцах либо используются другие DNS-имена kill switch, либо kill switch отсутствует.

Меры защиты Fortinet, доступные на момент инцидента.

Лаборатория FortiGuard активно работает с партнерами по Cyber Threat Alliance в рамках обмена информацией threat intelligence и генерации актуальных обновлений мер защиты.

Fortinet предоставляет две IPS сигнатуры, применение которых позволяет выявить и заблокировать Wannacry и его варианты. Это - следующие сигнатуры:

MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
(добавлена 14 марта 2017, обновлена 10 мая 2017)
Backdoor.Double.Pulsar
(добавлена 27 февраля, обновлена 1 мая 2017)

Антивирус

Антивирус Fortinet содержит комплексные сигнатуры и модели поведения, позволяющие выявить и заблокировать существующие и новые образцы вредоносного ПО.

Это - следующие сигнатуры:

W32/Agent.AAPW!tr

W32/CVE_2017_0147.A!tr

W32/Farfli.ATVE!tr.bdr

W32/Filecoder_WannaCryptor.B!tr

W32/Filecoder_WannaCryptor.D!tr

W32/Gen.DKT!tr

W32/Gen.DLG!tr

W32/GenKryptik.1C25!tr

W32/Generic.AC.3EF991!tr

W32/Scatter.B!tr

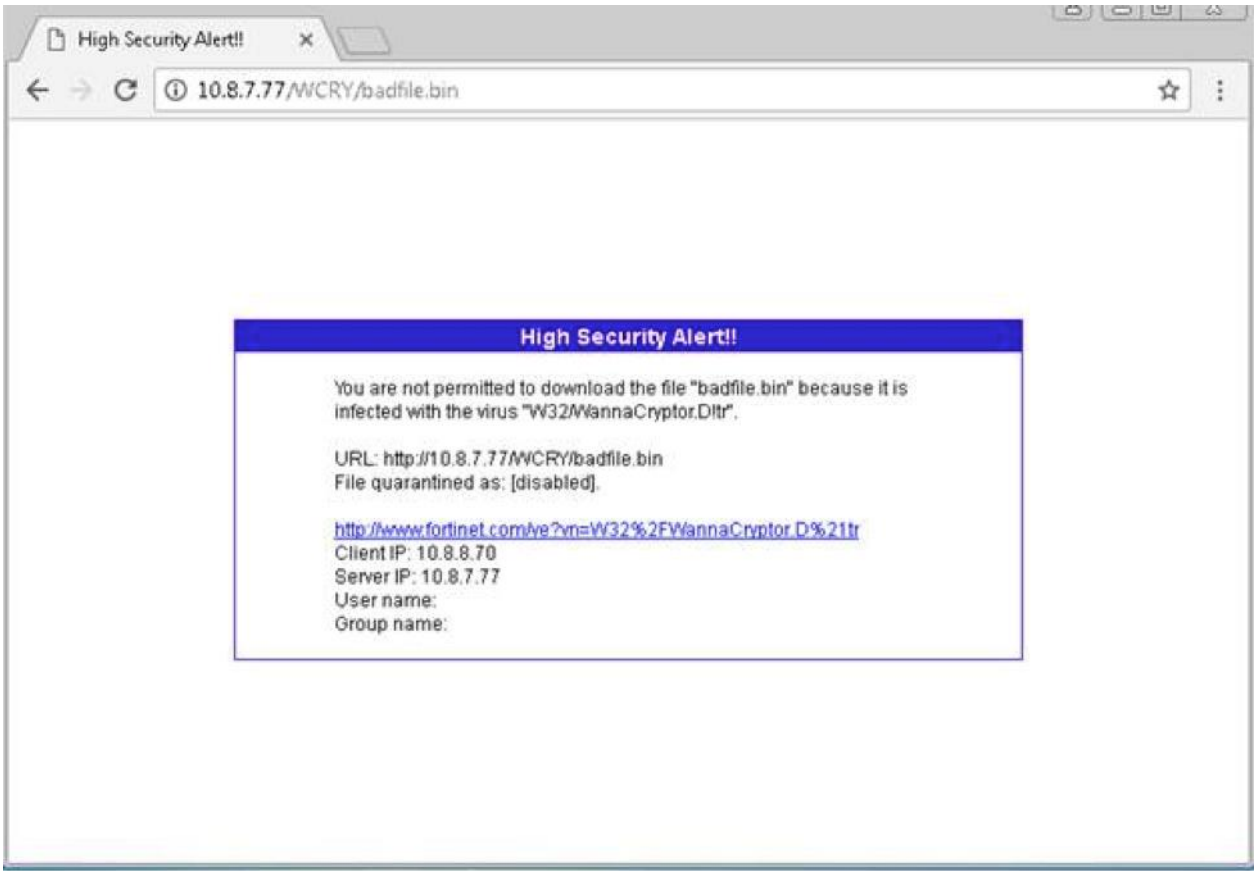
W32/Wanna.A!tr

W32/Wanna.D!tr

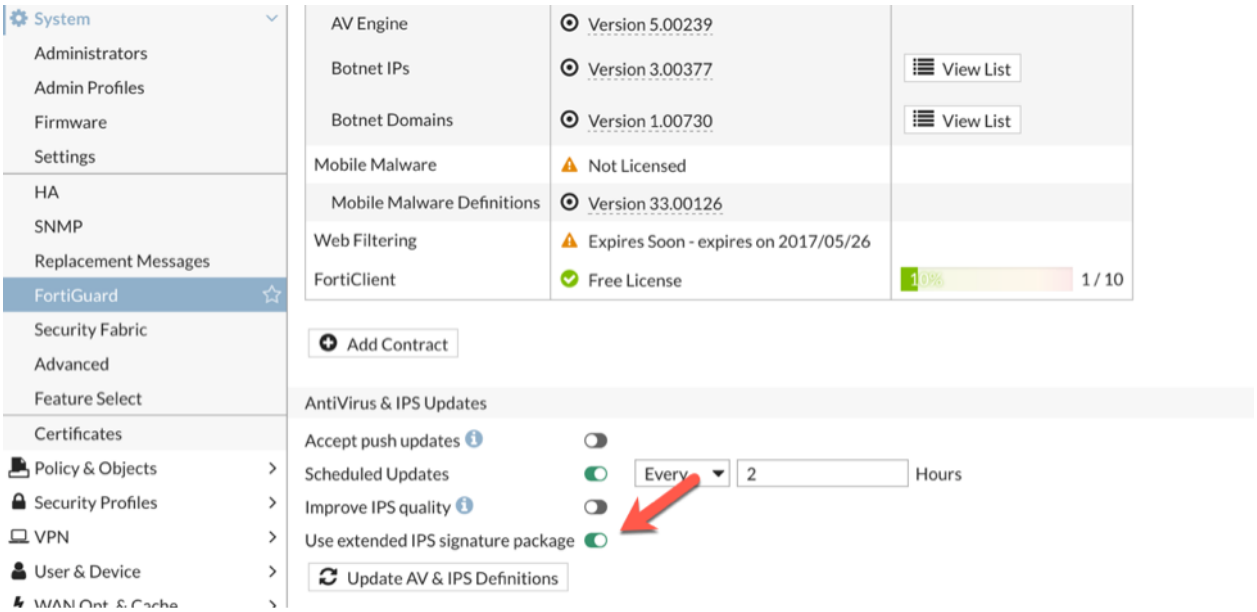
W32/WannaCryptor.B!tr

W32/WannaCryptor.D!tr

W32/Zapchast.D!tr



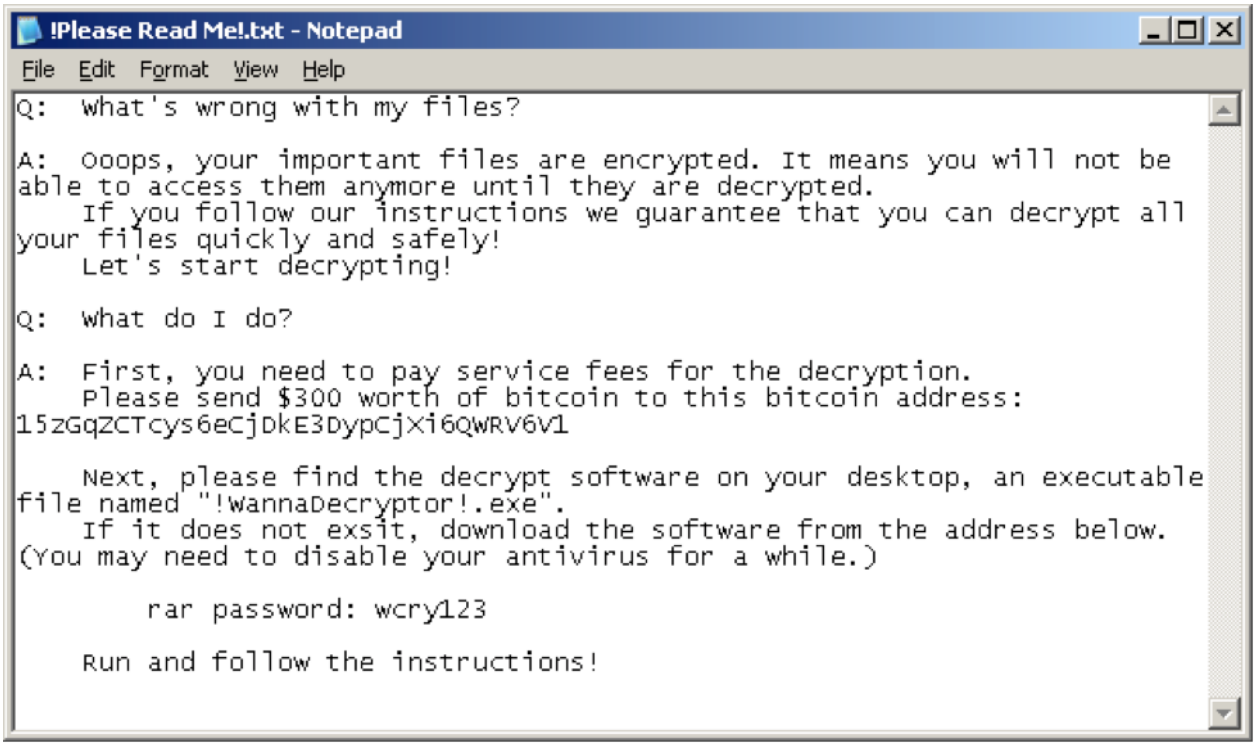
Следует убедиться, что на FortiGate включена расширенная база сигнатур антивируса (настройка по умолчанию). Для этого в интерфейсе управления FortiGate требуется перейти в меню system -> FortiGuard и выбрать "enable extended AV and Extended IPS" Не следует волноваться по этой причине. На большей части устройств это - настройка по умолчанию.



Если вредоносному ПО разрешен запуск, оно запустит команду icacls . /grant Everyone:F /T /C /Q , предоставляющую полный доступ ко всем файлам и папкам на ПК. Дополнительно, вредоносное ПО удаляет теневые копии Windows, отключает функцию восстановления при запуске и очищает историю Windows Server Backup.

После чего запускается и приступает к работешифровальщик. После выполнения шифрования, пользователи получают сообщение, похожее на указанное на скриншоте ниже.

Вредоносное ПО также оставляет файл *!Please Read Me!.txt* с дополнительными инструкциями. Имя файла может различаться в разных образцах вредоносного ПО.



Быстрый и легкий заработок, обеспечиваемый оплатой выкупа за расшифровку файлов, позволяет понять, почему этот вид вредоносного ПО столь распространён. Сколько пользователей уже заплатили выкуп? Сложно сказать, т.к. различные варианты вредоносного ПО используют разные кошельки Bitcoin для скрытия транзакций и постоянно перемещают средства между этими кошельками.

После заражения, жертвы могут попытаться восстановить файлы из резервных копий или другими методами (в настоящее время активно ведется поиск методов расшифровки), либо заплатить выкуп. Ниже представлено несколько ссылок, позволяющих понять, сколько средств уже перечислено в качестве выкупа. На момент написания статьи, стоимость 1 Bitcoin эквивалентна $1,784.90 USD.

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Всего получено: 9.41458497 BTC

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Всего получено: 5.17934856 BTC

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Всего получено: 7.1629281 BTC

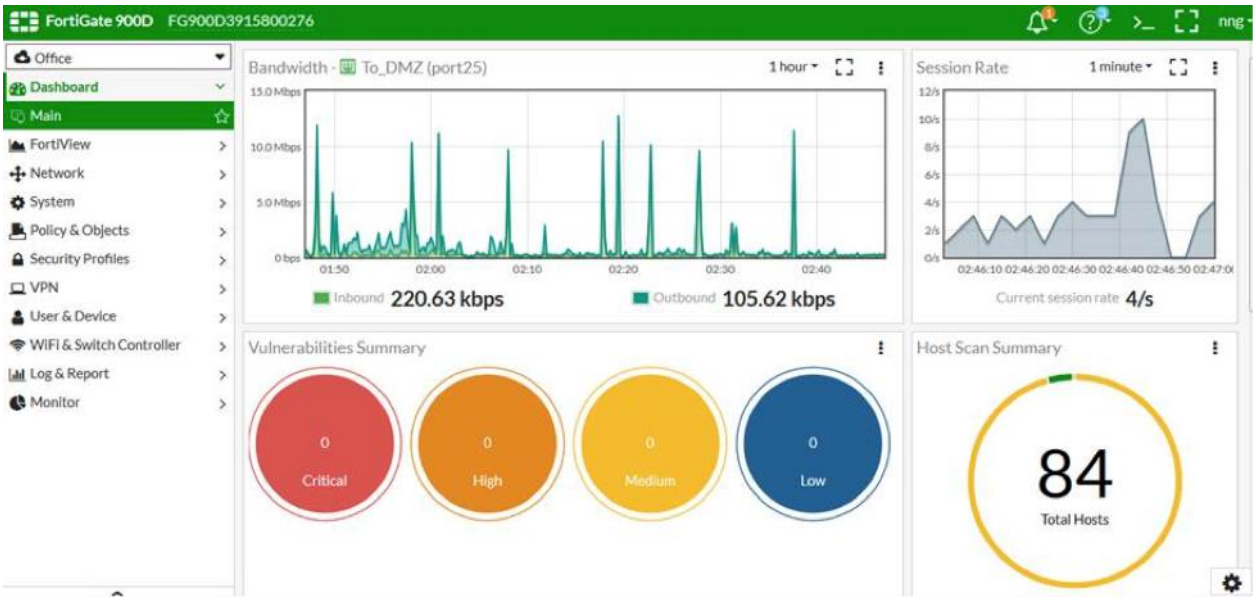
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Всего получено: 1.09469717 BTC

Это - всего лишь несколько кошельков, относящихся к Wannacry, на момент написания статьи в них перечислено более $38, 833.82 USD.

Выявление вредоносного ПО

Фабрика безопасности Fortinet может существенно облегчить выявление и блокирование этого и других вариантов вредоносного ПО, а также понять, на каких ПК функционирует Wannacry.



Индикаторы компрометации:

Зафиксированные IP-адреса центров управления (C&C):

```
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

Зафиксированные хеш-суммы образцов (SHA-256):

0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
7108d6793a003695ee8107401cfb17af305fa82ff6c16b7a5db45f15e5c9e12d
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
7e369022da51937781b3efe6c57f824f05cf43cbd66b4a24367a19488d2939e4
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740
aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494