ШИФРОВАЛЬЩИКИ КАК МАСШТАБНАЯ УГРОЗА

Использование современных программ класса Ransomware (шифровальщики) является один из самых популярных способов заработка киберпреступников. Согласно данным Group-IB, в 2020 году стало известно о более чем 500 успешных атак шифровальщиков на организации в более чем 45 странах, что на 40% больше чем за предыдущий год. Большинство из них направлены на корпоративную инфраструктуру организаций, что обусловлено значительной выгодой по отношению ко взлому обычных пользователей.

По данной причине, опасность вредоносного ПО типа Ransomware неумолимо растет, так как у киберпреступников появляются новые эффективные инструменты для проникновения, закрепления и последующего распространения шифровальщиков в организациях.

Обнаружение. За частую ряд сотрудников организаций не представляют, что необходимо делать при обнаружении на служебном компьютере или сервере шифровальщика. В этой связи специалистами РУП «Белтелеком» предлагаются к использованию подробные инструкции при обнаружении шифровальщика на служебных ПЭВМ.

1. Не выключая ПЭВМ, отключить его от сетевой инфраструктуры. Чаще всего для этого достаточно достать кабель из сетевой розетки или отключить сетевую карту Wi-Fi.

2. Зафиксировать события (предупреждения) ПО шифровальщика и информацию по зашифрованным файлам. Если есть возможность - сфотографировать экран ПЭВМ.

3. Зафиксировать все действия, которые могли привести к заражению ПЭВМ, в частности, было ли замечено странное поведение ПЭВМ в последнее время, последние действия перед обнаружением заражения и другие.

4. Связаться со службой технической поддержки, проинформировать о случившимся и передать зафиксированные события.

Сдерживание. Для технической поддержки, системного администратора и специалиста по защите информации сообщение о появлении в корпоративной инфраструктура шифровальщика должно обрабатываться в режиме

максимальной приоритизации. При этом, основным механизмом защиты корпоративной инфраструктуры является изоляция зараженных ПЭВМ и информационных систем от основной части инфраструктуры. Для определения границы заражения, необходимо определить тип шифровальщика, технические признаки компрометации и вектор заражения.

Тип шифровальщика можно определить на основе информации, предоставленной пользователем. Дополнительно, техническая поддержка может уточнить у пользователя: всплывающее сообщение при попытке открыть зашифрованный файл, адрес, по которому предлагается перевести оплату за разблокирование зашифрованной информации, схему переименования файлов (.cry, .crypt, .locked и другие), язык и так далее.

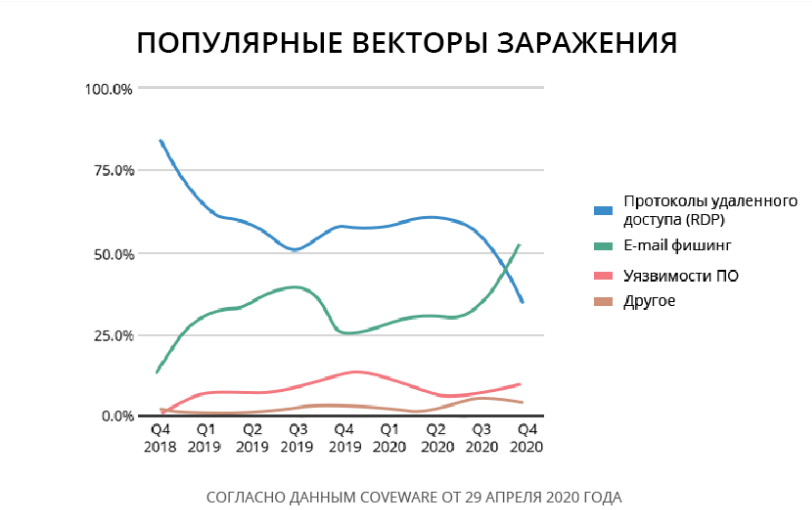
Определив тип шифровальщика, системный администратор или специалист по информационной безопасности должен собрать следующие технические признаки компрометации из открытых источников в сети Интернет:

- имя процесса;
- устанавливаемые сетевые соединения;
- названия и хеши вредоносных файлов;
- типы необходимых учетных записей;
- адреса почты, с которых проводится рассылка писем (в случае фишинга) и т.п.

Тем не менее, все собранные значения для конкретного шифровальщика могу быть изменены злоумышленником. В этой связи самым наилучшим способом получить достоверную информацию о шифровальщике является анализ сетевой активности зараженного узла и образца вредоносного ПО. При этом желательно отправить образец шифровальщика в бесплатные онлайн сервисы анализа подозрительных файлов (например, VirusTotal) и национальный центр реагирования на компьютерные инциденты Республики Беларусь (CERT) для последующего реагирования других организаций.

Далее системный администратор и специалист по информационной безопасности должны начать процедуру выявления и изоляции зараженных ПЭВМ и информационных систем от основной части инфраструктуры на основе технических признаков компрометации. Для этого могут использоваться сетевые средства защиты информации, антивирусные средства или средства мониторинга серверов и ПЭВМ. На межсетевых экранах, DNS-серверах или прокси-серверах можно проверить устанавливаемые с сетью Интернет соединения. Для комплексного выявления зараженных узлов удобно использовать SIEM.

В это же время, специалист по информационной безопасности должен провести детальный анализ образца вредоносного ПО для подтверждения и расширения списка возможных технических признаков компрометации, а также определить вектор заражения внутри корпоративной сети.



После определения вектора заражения специалист обязан провести сканирование корпоративной инфраструктуры на предмет наличия уязвимых к атаке шифровальщика информационных систем и ПЭВМ. Все уязвимые узлы в срочном порядке должны быть изолированы системным администратором.

Восстановление. Перед проведением мероприятий по восстановлению информационных систем и ПЭВМ владельцы бизнеса должны определить степень влияния заражения на бизнес-процессы, репутацию организации и пользовательские данные, а системные администраторы - возможность восстановления данных из резервных копий.

В случае, когда восстановление данных из резервных копий невозможно, можно попробовать восстановить работу другими способами:

- провести поиск специализированных утилит;
- провести анализ вредоносного ПО в антивирусной лаборатории;
- в исключительных случаях (по договоренности с правоохранительными органами) заплатить вымогателям за важные данные.

Однако стоит понимать, что последний пункт сопряжен с огромными рисками как со стороны злоумышленника (отказ от восстановления или повышение стоимости), так и со стороны самого шифровальщика (невозможность восстановить данных).

Предотвращение. В целях снижения рисков заражения и повышения шансов восстановления информации после заражения специалисты РУП «Белтелеком» рекомендуют:

1. Сегментировать корпоративную сеть организации (в частности, с помощью технологии VLAN);
2. Проводить регулярное резервное копирование критических данных на изолированном от корпоративной инфраструктуры сервере или СХД;
3. Провести обучение пользователей и технической поддержки по вопросам информационной безопасности;
4. Регулярно устанавливать критические обновления и обновления безопасности на информационные системы и ПЭВМ;
5. Использовать лицензионное антивирусное ПО;
6. Разработать и внедрить инструкции по обнаружению, идентификации и предотвращению распространения вредоносного ПО.