ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРАВОЗАЩИТНИКОВ

Практический бюллетень №3

Бюллетень подготовлен Центром исследования правовой политики и ОО «ЭХО» в рамках проекта «Консолидация усилий гражданского общества с целью поощрения защиты правозащитников» финансируемого Европейским Союзом. Содержание данной публикации является предметом ответственности Центра исследования правовой политики и ОО «ЭХО» и необязательно отражает точку зрения Европейского Союза.

LPRC
ЦЕНТР ИССЛЕДОВАНИЯ ПРАВОВОЙ ПОЛИТИКИ

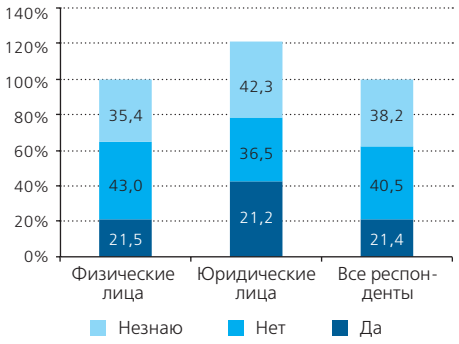
ЭО
общественное объединение

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРАВОЗАЩИТНИКОВ

Мониторинг по проекту **«Консолидация усилий гражданского общества с целью поощрения защиты правозащитников»** в целях сбора информации о ситуации с правозащитниками осуществил социологический опрос среди правозащитников во всех областях Казахстана, а также в гг. Астана и Алматы. Всего опросом было охвачено 131 правозащитников, из них 79 работающих самостоятельно, как физическое лицо, и 52 представителя НПО.

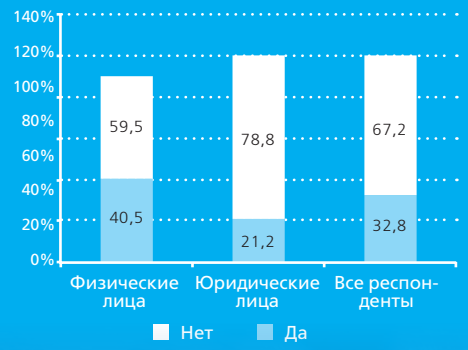
В ходе опроса правозащитникам было предложено ответить на вопрос: «Защищены ли Ваши информационные системы от нападений, потери информации?», значительная часть правозащитников **(40,5%)** ответили **«нет, не защищены»**. Так же значительная часть респондентов (38,2%) ответила «не знаю». В целом однозначно положительно о защищённости информационных систем ответили лишь 21,4% респондентов.

Распределение ответов респондентов на вопрос «Защищены ли Ваши информационные системы от нападений, потери информации?», n=131



Далее всем участникам опроса задавался вопрос: «Были ли в отношении Вас атаки: физические (телесные повреждения), информационные (вирусы, блокирование сайта и т.д.), технические (порча/кража профессионального оборудования и иных технических средств), репутационные (публичные обвинения против организации)?». Различным видам информационных атак правозащитники подвергались больше, чем всем другим видам атак: в целом 32,8% правозащитников отметили о таких случаях. Факты информационных атак чаще распространены среди физических лиц (40,5%), чем среди юридических лиц (21,2%). В среднем было 6 информационных атак на правозащитников, минимум – 1, максимум – 20.

Распределение ответов на вопрос о факте информационных атак, n=131



С целью оценить возможные угрозы правозащитникам, всем участникам было предложено оценить вероятность возникновения различных атак. Второй по вероятности возникновения респондентами была указана атака – информационная, 62,6% респондентов отметили возможность данной атаки. Высокую степень вероятности возникновения данной атаки чаще отмечали правозащитники из числа физических лиц (22,8%), чем представители юридических лиц (13,5%).

Наш третий практический бюллетень предлагает рассмотреть возможность работы с инструментом под названием «Detekt», который поможет вам найти возможные угрозы на своем компьютере.

Статистический опрос продемонстрировал неосведомленность правозащитников о современных технологиях информационной безопасности (38,2%). Существует несколько методов защиты вашего компьютера от вредоносного программного обеспечения (ПО):

- **Антивирусные программы.** Рекомендуется использовать антивирусные программы на компьютерах, а также мобильных устройствах. Антивирусные программы могут быть весьма эффективными при борьбе с «дешевой, нецелевой атакой», которая может быть использована преступниками против сотен целей. Однако антивирусные программы могут быть весьма неэффективными при целенаправленной атаке *(https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware)*.

- **Индикаторы риска – улики, которые свидетельствуют о взломе вашего устройства или его подделке.** Если невозможно определить возможную атаку при помощи антивируса, можно попробовать воспользоваться индикаторами риска. Например, Google иногда предупреждает пользователей почтового ящика Gmail о том, что возможно их почта стала целью спонсируемых государством взломщиков. Дополнительно, вы можете заметить, что ваша веб камера включена, хотя вы ее сами не активировали (хотя вредоносное ПО может ее отключить) – это также может служить индикатором риска. Также существуют менее заметные индикаторы: вы можете заметить, что вход на ваш почтовый аккаунт был сделан с незнакомого IP адреса или ваши настройки, были сделаны таким образом, что позволяют отправлять копии ваших переписок на незнакомый электронный ящик. Вы также можете заметить, что ваш компьютер подключен к командному и контрольному серверу - к компьютеру, который посылает команды зараженным вирусами машинам или которые получают данные от зараженных машин. *(https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware)*

- **Программы, сканирующие компьютер на наличие шпионских программ.** В настоящее время существует множество вредоносных программ, которые не считаются вирусами, т.к. они не обладают способностью к размножению. Программой-шпионом принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет. Кроме того, ряд программ нацелены на перехват сообщений и электронной почты, прослушивание и несанкционированную запись с видеокамер компьютера.

Что такое Detekt?

«Detekt» – это бесплатный инструмент, который сканирует компьютер с операционной системой Windows на наличие следов FinFisher и Hacking Team RCS, коммерческих шпионских программ наблюдения, которые также используются для выявления и мониторинга правозащитников и журналистов по всему миру.

Необходимо отметить, что, если программа не обнаружила шпионских программ на вашем устройстве, это не означает, что таковых нет. Некоторые шпионские программы могут специально обновляться по причине выпуска Detekt, из-за чего они могут быть оснащены специальными функциями для защиты от обнаружения.

Detekt не удаляет инфекцию или любой файл, который он считает подозрительным. Если программа указывает на признаки заражения, следует предположить, что ваш компьютер был взломан, и больше не является безопасным для использования. Злоумышленники, скорее всего, имеют доступ удаленного управления вашего компьютера, то есть они могут просматривать не только ваши файлы и сообщения электронной почты, но все, что вы печатаете на клавиатуре, и даже может переключиться на веб-камеры и микрофон удаленно.

Detekt выпущен в партнерстве с Amnesty International, Digitale Gesellschaft, Electronic Frontier Foundation и Privacy International.

Этот инструмент был размещен публично для того, чтобы обеспечить исследователей, правозащитников, журналистов и других лиц, которые подозревают, что они являются целью незаконного наблюдения программой, с помощью которой легко проверить свои компьютеры на наличие известных шпионских программ.

Инструмент является свободным и открытым исходным кодом и предоставляется как есть, без каких-либо гарантий.

Как это работает?

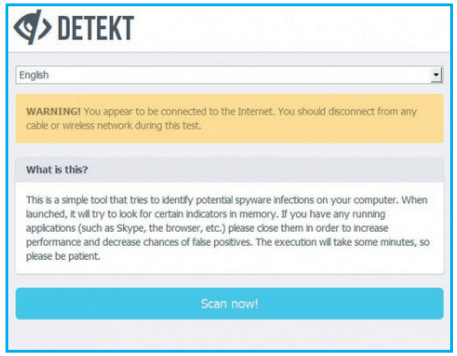
Для установки программы необходимо предпринять несколько подготовительных шагов. Для начала необходимо закрыть все приложения и отключить компьютер от сети Интернет. При обнаружении шпионских программ нужно оставить компьютер без подключения к Интернету до полного удаления подобных программ. Разработчики также рекомендуют отключить антивирусные программы для предотвращения возможных помех.

ШАГ 1

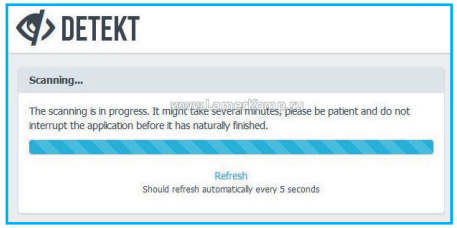
Для использования программы Detekt вам необходимо запустить ее на правах Администратора: для этого необходимо нажать правой кнопкой мыши на иконку и выбрать “Запустить от Администратора”. В операционной системе Windows XP двойного щелчка будет достаточно.

ШАГ 2

Программа Detekt доступна на амхарском, арабском, английском, немецком, итальянском и испанском языках. Вы можете выбрать нужный язык из выпадающего меню.



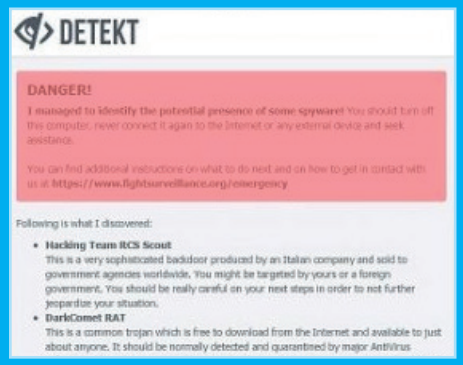
После запуска программы откроется графический интерфейс, и после команды «Сканировать» начнет анализ памяти компьютера на наличие следов от шпионских программ.



Процесс сканирования может занять до 30 минут, в зависимости от характеристик компьютера.

ШАГ 3

После окончания действия программа выдаст результат сканирования и укажет, были ли обнаружены какие-либо инфекции.



Программа также создает файл журнала с дополнительными данными, которые могут быть полезны для технических экспертов для дальнейшего изучения. Разработчики программы рекомендуют распечатать или копировать данные журнала для хранения вне зараженного компьютера и предоставить его техническим экспертам при поиске помощи.

Если программа обнаружит шпионские программы необходимо:

№ 1: перестать пользоваться зараженным компьютером и отключить его от сети Интернет, других сетей и съемных устройств, если это необходимо. Каждая кнопка, на которую вы нажимаете, каждая страница, на которую вы заходите и каждое электронное письмо, которое вы открываете, может находиться под наблюдением;

№ 2: решить, следует ли утилизировать компьютер или сохранить его и запросить дополнительную помощь, чтобы расследовать атаку и помочь вам безопасно восстановить работоспособность компьютера. Разработчики рекомендуют поговорить с экспертом для помощи в принятии решения.

В некоторых случаях, программа Detekt может ошибаться, поэтому важно обратиться к эксперту, который смог бы проверить компьютер. Вы также можете обратиться к разработчикам программы для проверки результатов сканирования. При обращении за помощью разработчики рекомендуют использовать другой компьютер, а также рассмотреть возможность подключения к Интернету из другого места, чем вы обычно используете, например, из интернет-кафе или с помощью Wi-Fi в общественных местах.

Полезные ресурсы:

О программе: *https://resistsurveillance.org/index.html*
Скачать программу Detekt можно тут: *https://github.com/botherder/detekt/releases/tag/2.0*
Написать техническим экспертам для помощи можно на этот электронный адрес: *nex@nex.sx*

Республика Казахстан, г. Алматы,
050009, пр. Абая д. 157, офис 44
+7 727 394 36 60/ 94
info@lprc.kz, www.lprc.kz