Оригинал: http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf

Монетизация инсайдера

Растущий симбиоз инсайдеров и Dark Web

Идо Вулкан (IntSights)
Тим Конделло (RedOwl)
Дэвид Погемиллер (RedOwl)

Содержание

Резюме

Организации сталкиваются с беспрецедентными рисками со стороны инсайдеров — сотрудников и подрядчиков, имеющих доступ к корпоративным сетям. Риск со стороны инсайдеров возрастает частично из-за растущего влияния Dark Web — той части интернета, которая позволяет сохранить анонимность. Dark Web все чаще используется киберпреступниками для вербовки инсайдеров, чтобы помочь украсть данные, совершить незаконные сделки или получить прибыль.

Компании RedOwl и IntSights объединили свои усилия, чтобы лучше понять, как Dark Web способствует увеличению риска со стороны инсайдеров. Изучив темные форумы, посвященные вопросам найма и сотрудничества с инсайдерами, мы обнаружили:

- Вербовка инсайдеров в Dark Web ведется активно и продолжает расти в объемах. Мы увидели, что число обсуждений этой темы на форумах удвоилось за период с 2015 по 2016 год.
- Dark Web создала рынок для сотрудников с целью более легкой монетизации доступа к инсайдерской информации. В настоящее время Dark Web служит средством, которое используют инсайдеры для «обналичивания денег», полученных за инсайдерскую торговлю и в качестве оплаты украденных кредитных карт.
- Источники угрозы используют Dark Web, чтобы находить и привлекать инсайдеров с целью загрузки вредоносного ПО в обход методов защиты, применяемых организацией. В

результате любой инсайдер, имеющий доступ ко внутренней сети, независимо от технических возможностей или трудового стажа, представляет риск для своей компании.

Чтобы решить эту проблему, компании по управлению рисками должны присоединиться к растущему числу организаций, активно занимающихся разработкой программ по защите от внутренних угроз. Как ни странно, 80% предложений по обеспечению безопасности сосредоточены на защите периметра, в то время как лишь менее половины организаций финансируют программы защиты от внутренних угроз.

Об авторах

Идо Улькан. Идо обладает десятилетним опытом в области разработки и оценки, фокусируясь особенно глубоко на Dark Web. Идо служил в одном из ведущих разведывательных подразделений Армии Обороны Израиля (Цахал) в качестве аналитика кибербразведки, где получил глубокие познания относительно различных субъектов угрозы и их методов. После службы Идо работал в нескольких компаниях в как аналитик и руководитель, где смог расширить свои познания о киберпреступных экосистемах. Теперь Идо возглавляет команду аналитиков кибербразведки IntSights.

Тим Конделло. Тим работал в сфере кибербезопасности в частном секторе, а также в вооруженных силах США. В настоящее время Тим является техническим менеджером компании RedOwl, помогая заказчикам создавать и развертывать программы для снижения риска со стороны инсайдеров. Тим работал аналитиком по киберугрозам в банке BNY Mellon. В его обязанности входило проведение расследований в Dark Web и осуществление работы с Национальным Альянсом киберкриминалистики и обучения (NCFTA).

Дэвид Погемюллер. В качестве вице-президента по стратегии, Дэвид провел последние два года, возглавляя разработку, анализ и реализацию программ по выявлению внутренних угроз для клиентов компании RedOwl. До этого Дэвид был менеджером в Bridgewater Associates, хедж-фонде. Перед этим Дэвид возглавлял небольшую консалтинговую фирму, приобретенную Moody.

Мотивы инсайдеров и влияние Dark Web

Ежегодный отчет Verizon о нарушениях в работе выявил, что на протяжении многих лет инсайдеры были одним из постоянных источников цифровых атак. В докладе приводятся два основных фактора: обещание финансовой выгоды и простота осуществления атаки. Как Dark Web влияет на эти мотивы? Мы полагаем, что темная сеть усиливает три психологических фактора, которые побуждают инсайдера делать расчеты:

- Значимость. Dark Web создала рынок с готовыми покупателями и сотрудниками, что позволяет монетизировать инсайдерские действия. А именно, Dark Web катализирует злонамеренную инсайдерскую деятельность, облегчая возможность получить прибыль, снижая при этом риск обнаружения.
- Стоимость мероприятия. Серьезные преступники в Dark Web могут вооружить менее искушенных инсайдеров знаниями и инструментами, необходимыми им для действий. Хуже того, менее искушенные инсайдеры могут вступать в сговор с более опытными преступниками для выполнения сложных атак.
- Риск обнаружения. Анонимность Dark Web серьезно снижает вероятность быть обнаруженным. Кроме того, сговор с преступниками помогает обеспечить инсайдеров

техническими инструментами для более эффективного сокрытия преступной деятельности.

Отслеживание действий инсайдеров в Dark Web

Используя сочетание скрытых методов и поиска, исследователи контролировали инсайдерскую деятельность в Dark Web и отслеживали объем ссылок на инсайдеров на киберпреступных форумах за последние два года. Каждый отдельный пост, ссылающийся на инсайдеров, учитывался как уникальный. Кроме того, каждый пост был проанализирован аналитиком, чтобы подтвердить, что ссылки на инсайдеров были сделаны в правильном контексте. В течение двух лет мы отметили около 1000 ссылок, пик роста наблюдался в последние месяцы 2016 года.

Диаграмма 1: Упоминание об инсайдерах на форумах в Dark Web, 2015-2016гг.

Взгляд внутрь Dark Web

Наше исследование выявило некоторые области Dark Web, в которых задействованы инсайдеры:

- инсайдерская торговля (т. е. торговля информацией, недоступной широкой публике);
- продажа номеров кредитных карт, полученных от сотрудников сектора розничной торговли;
- вооружение инсайдеров.

Инсайдерская торговля

Инициаторы угроз используют форумы Dark Web для привлечения инсайдеров и сговора. Получив информацию от инсайдера, киберпреступник пытается получить более высокую прибыль. Инсайдер получает комиссионные. Dark Web облегчает незаконную торговую деятельность, предоставляя анонимность, затрудняя идентификацию кибепреступников.

Исследуемые нами форумы по инсайдерской торговле были уникальными. Хотя некоторые действия могут происходить на «черных рынках», кажется, что самые информированные и опытные участники пребывают в закрытых небольших группах. От тех, кто подает заявку на участие, эти сообщества требуют доказательства возможностей или доступа к знаниям посредством обмена реальной внутренней информацией, которая затем тщательно проверяется и подтверждается. Один из форумов — это KickAss marketplace (см. рис. 2). Этот конкретный подфорум по инсайдерской торговле был создан в феврале 2016 года, и его цели были таковы:

- торговля на фондовом рынке;
- торговля на «Форекс»;

- товары;
- агрессивное бизнес-ремоделирование;
- технология «Знай, что происходит перед отдыхом».

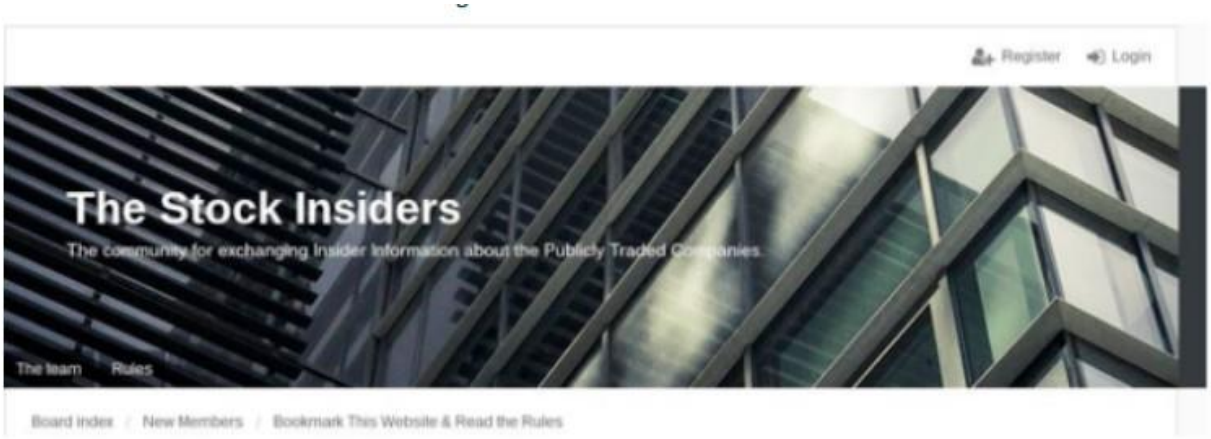
Рисунок 2: Инсайдерская торговля на форуме KickAss marketplace

Менеджеры форума утверждают, что соблюдают высокие стандарты. Например, форум утверждает, что перед публикацией проверяет каждый пост на предмет актуальности. В обмен на высокие стандарты форум требует значительный членский взнос в размере 1 Биткойна.

Форум выглядит относительно активным, размещая примерно пять публикаций в неделю и осуществляя в общей сложности 40 транзакций BTC (приблизительно 35 800 долл. США, см. Комиссионные по сделкам в Приложении 1). По словам менеджера группы, есть члены, которые зарабатывают более 5000 долларов США в месяц, используя украденную информацию.

Этот форум не единственный. Другой форум (см. рис. 3), называемый The Stock Insiders, также посвящен исключительно инсайдерской торговле. Он был открыт в апреле 2016 года. Его цель заключалась в том, чтобы «... создать долгосрочное и хорошо отобранное сообщество джентльменов, которые уверенно обмениваются инсайдерской информацией о компаниях открытого типа». Администратор утверждает, что он «успешный (изначально выходец из Европы) ИТ-предприниматель, проживающий в настоящее время в США [...], также является активным трейдером и имеет доступ к нескольким компаниям открытого типа».

Рис. 3. Форум The Stock Insiders



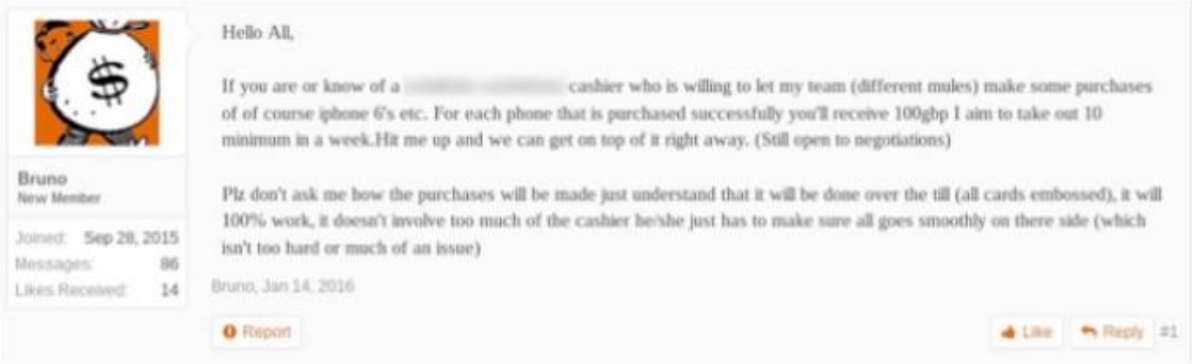
Вербовка инсайдеров

Наши исследования также выявили непрерывную вербовку работников сфере розничной торговли, которые имеют доступ к кредитным картам потребителей. Опытные киберпреступники

затем будут заниматься кардингом, процессом по снятию денег с украденных кредитных карт для личной выгоды. Как правило, рекрутеры нацелены на работников низшего звена, таких как кассиры, чья помощь необходима для использования украденных кредитных карт.

На рис. 4 участник веб-форума разместил объявление о получении услуг со стороны кассира в известном магазине розничной сети с целью приобретения iPhone.

Рис. 4. Участник Dark Web просит помощи инсайдера



На рис. 5. Рекрутер ищет кассиров, которые будут готовы украсть данные кредитных карт:

<u>Вооружая инсайдеров</u>

Помимо других действий, опытные хакеры в Dark Web могут вооружать инсайдеров инструментами и знаниями, необходимыми для кражи данных и совершения мошенничества, а также для сокрытия любых своих действий.

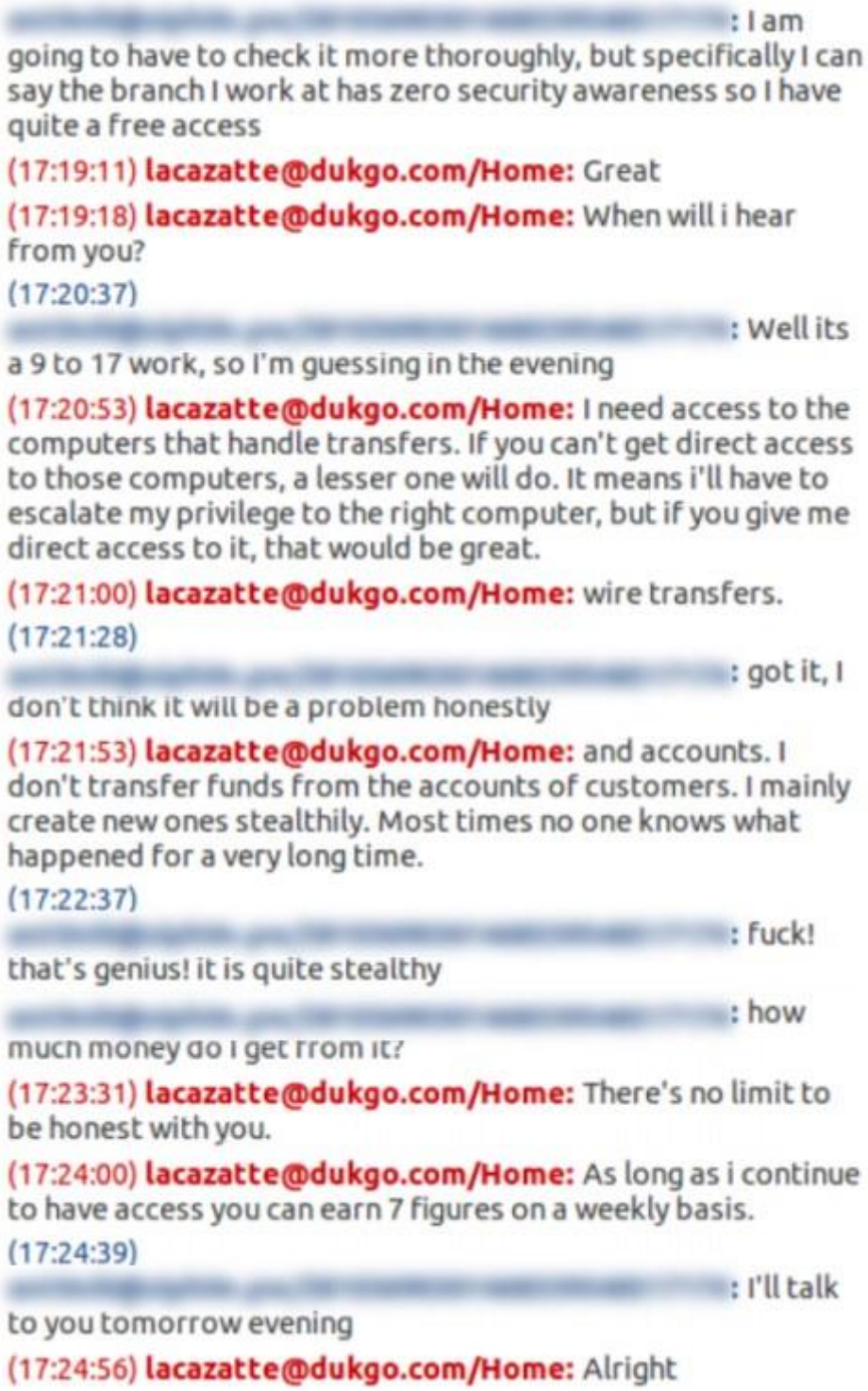
В одном случае хакер потребовал, чтобы инсайдеры банка разместили вредоносное ПО непосредственно в сети банка. Такой подход значительно снижает стоимость атаки, поскольку хакеру не нужно осуществлять фишинг, а также повышает шанс на успех, давая миновать многие технические методы защиты организации (например, антивирус или «песочницу»).

Чтобы проиллюстрировать это действие, на рис. 6 показано рекламное объявление по поиску банковских работников. Оно дает понять, что должность сотрудника в банке не имеет значения, если у него есть доступ к компьютеру.

Рис. 6. Вербовка инсайдера для обмана банка

На рис.7 злоумышленник объясняет потенциальному сотруднику подход, указывая, что ему нужен прямой доступ к компьютерам, через который осуществляется доступ к учетным записям и на котором обрабатывают банковские переводы, и что он готов платить «7 цифр еженедельно» за продолжительный доступ к такому компьютеру.

Рис. 7. Инсайдер, сотрудничающий с киберпреступником, на форуме в Dark Web



Заключение: Dark Web все чаще делает выбор с пользу инсайдеров

Dark Web имеет внутри себя активное сообщество искушенных покупателей и сотрудников, которые содействуют монетизации и вооружению вредоносной инсайдерской деятельности. Легкость, с которой сотрудники могут получить доступ к Dark Web, означает, что ее влияние в ближайшие годы будет продолжать расти.

Что могут сделать группы по обеспечению безопасности и снижению риска? Для борьбы с этой проблемой группы по управлению рисками должны присоединяться к растущему числу

организаций, которые активно создают программы по снижению инсайдерской угрозы. По иронии судьбы, почти 80% инициатив в области безопасности сосредоточены на защите периметра, в то время как лишь менее половины бюджета организаций используется на финансирование программ по снижению инсайдерской угрозы. Это означает, что многие события, представляющие угрозу, не обнаружены до конца. Согласно опросу Gartner, проведенному в 2016 году и представленному на Саммите по безопасности Gartner, только 18% предприятий имеют официальную программу по обнаружению инсайдерской угрозы.

Предприятия, надеющиеся создать программу по снижению инсайдерской угрозы, должны учитывать следующее:

Воздействие на культуру поведения

Эффективным рычагом, которым располагают организации для снижения инсайдерской угрозы, является культура поведения. Предприятиям следует создавать, обучать и настаивать на соблюдении последовательной корпоративной политики безопасности, одновременно защищая конфиденциальность сотрудников. Понимание сотрудниками и поставщиками правил — и наличие штрафов за их нарушение — оказывает огромное влияние.

Бдительность в отношении сотрудников

В недавнем отчете Forrester об инсайдерских угрозах отмечается: «Рассмотрение инсайдеров как технологической проблемы игнорирует человеческие аспекты мотивации и поведения». Группы по обеспечению безопасности должны следить за поведением сотрудников, оценивая его в соответствии с широким спектром параметров, которые идентифицируют подозрительную активность, но также помогают понять негативный настрой работников.

Правильная технология

Создание эффективной программы защиты от инсайдеров требует наличия надежной экосистемы безопасности, основанной на основополагающих возможностях для просмотра всей деятельности сотрудников и нежелательного поведения, не нарушая при этом права сотрудников на конфиденциальность.

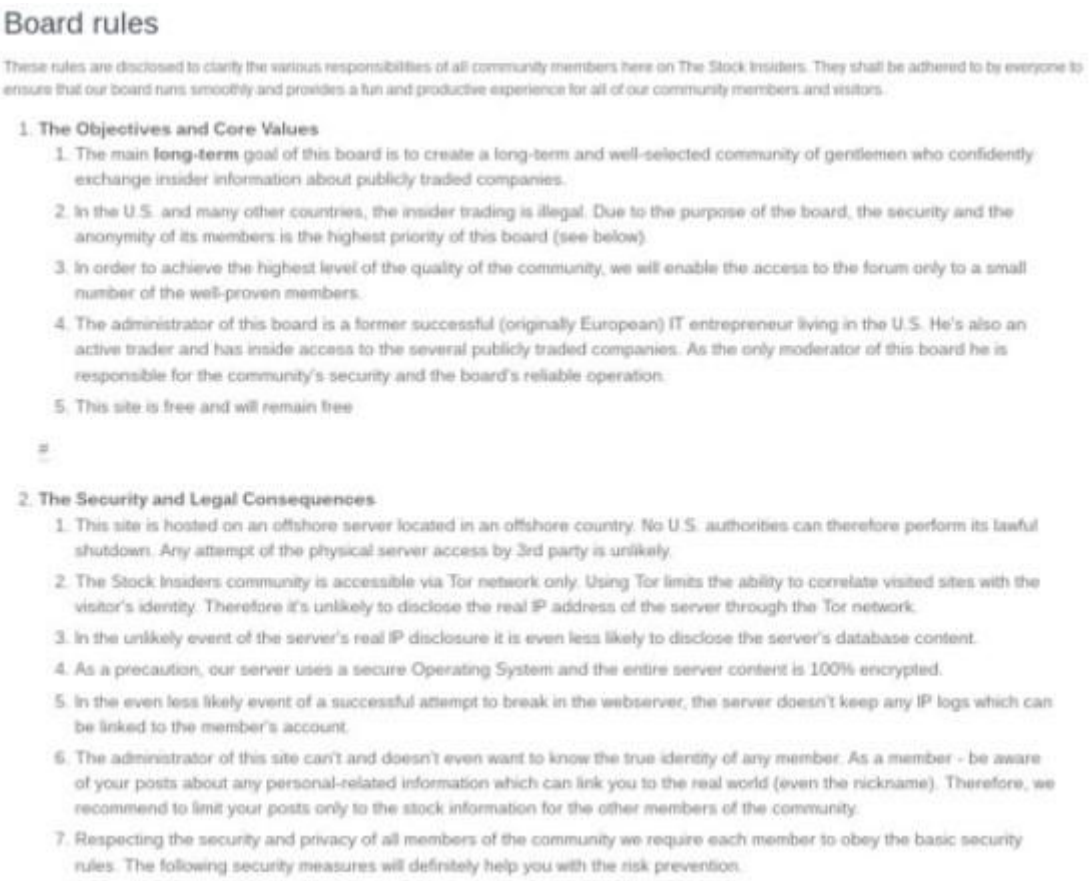
Приложение I: Денежные переводы на инсайдерском форуме

Ниже приведен список счетов BTC, которые используются форумом «Kick Ass marketplace».

Address	Total Received	Final Balance	# of Transactions
19JTncP1EwBvpsTpfmMpg7weJFJCQsoqUL [5]	0-BTC/$0.00	0-BTC/$0.00	0
17oUCfkt3kQqstbsSpujYyQwH5Hk5D9Q3b [6]	8-BTC/$7,160.00	0-BTC/$0.00	34
178GrbdgyXUNSrUpsDhDeXADba4PcFAZbF [7]	92.1-BTC/$82,429.50	$0.43	184

Приложение II: Денежные переводы на инсайдерском форуме

Ниже приведен список счетов BTC, которые используются форумом Kick Ass marketplace.



Board rules

These rules are disclosed to clarify the various responsibilities of all community members here on The Stock Insiders. They shall be adhered to by everyone to ensure that our board runs smoothly and provides a fun and productive experience for all of our community members and visitors.

1. **The Objectives and Core Values**
   1. The main **long-term** goal of this board is to create a long-term and well-selected community of gentlemen who confidently exchange insider information about publicly traded companies.
   2. In the U.S. and many other countries, the insider trading is illegal. Due to the purpose of the board, the security and the anonymity of its members is the highest priority of this board (see below).
   3. In order to achieve the highest level of the quality of the community, we will enable the access to the forum only to a small number of the well-proven members.
   4. The administrator of this board is a former successful (originally European) IT entrepreneur living in the U.S. He's also an active trader and has inside access to the several publicly traded companies. As the only moderator of this board he is responsible for the community's security and the board's reliable operation.
   5. This site is free and will remain free.

   #

2. **The Security and Legal Consequences**
   1. This site is hosted on an offshore server located in an offshore country. No U.S. authorities can therefore perform its lawful shutdown. Any attempt of the physical server access by 3rd party is unlikely.
   2. The Stock Insiders community is accessible via Tor network only. Using Tor limits the ability to correlate visited sites with the visitor's identity. Therefore it's unlikely to disclose the real IP address of the server through the Tor network.
   3. In the unlikely event of the server's real IP disclosure it is even less likely to disclose the server's database content.
   4. As a precaution, our server uses a secure Operating System and the entire server content is 100% encrypted.
   5. In the even less likely event of a successful attempt to break in the webserver, the server doesn't keep any IP logs which can be linked to the member's account.
   6. The administrator of this site can't and doesn't even want to know the true identity of any member. As a member - be aware of your posts about any personal-related information which can link you to the real world (even the nickname). Therefore, we recommend to limit your posts only to the stock information for the other members of the community.
   7. Respecting the security and privacy of all members of the community we require each member to obey the basic security rules. The following security measures will definitely help you with the risk prevention.

О компании RedOwl

Компания RedOwl предоставляет платформу управления рисками со стороны инсайдеров. Только компания RedOwl способна использовать существующие корпоративные данные для выявления и смягчения нежелательного поведения путем использования структурированных, неструктурированных и бизнес-данных для анализа взаимодействия между сотрудниками, поставщиками, устройствами, файлами и приложениями. Используя сочетание статистических сопоставлений образцов, машинного обучения и контент-аналитики для профилирования поведение пользователя, компания RedOwl предоставляет профессионалам по управлению рисками подробные описания, необходимые для эффективного выявления небрежных, скомпрометированных и вредоносных сотрудников. www.redowl.com

О компании IntSights

Компания IntSights исследует угрозы, исходящие от Dark Web. Компания IntSights проникает в Dark Web для обнаружения и анализа запланированных или потенциальных атак. Компания IntSights предлагает заказчикам единое решение, сочетающее быструю и действенную разведку с методами смягчения угрозы и устранением последствий.

https://intsights.com/