

Взломаны крупнейшие cybercrime-форумы в РФ

Самый известный на сегодняшний день закрытый форум киберпреступников "MAZA.la" (или как его еще называют, "MAZAFKA"), администраторами которого являются Afx (предположительно Алексей), Render, 4x4 и Fiesta, подвергся 18 февраля массовой хакерской атаке, в результате чего база данных форума, состоящая из более чем двух тысяч пользователей, была похищена и стала доступна общественности.

Второй волной был атакован не менее приватный форум "Direct Connection", администратором которого является некий "k0pa", выходец группировки "CyberLords Team" — той же команды, членом которой являлся скандальный хакер из Новосибирска Евгений Аникин. Аналитики предполагают, между российскими кардерами началась своя "Интернет-война" за передел влияния в мире киберпреступности, предпосылки которой известны лишь только им.

MAZA.la

Данный форум являлся приватным и абсолютно закрытым, доступ туда был открыт только по наличию нескольких проверенных и авторитетных поручителей, уже имеющих учетную запись на форуме. Безопасность проекта обеспечивалась с учетом последних тенденций в области ИБ: применение цифровых сертификатов безопасности, встроенный антифишинговый фильтр и т.д. Кроме того, сервера проекта располагались в отвлеченной от всех возможных cybercrime-законов области — на Тайване.

Спектр допущенных к участию лиц постоянно сужался и проверялся специальным ответственным лицом — "MF_SUPPORT", выходцем Украины, работа которого финансировалась со стороны Администраторов. Во многом, именно качество работы "MF_SUPPORT" определяло, каким будет контингент форума. Кроме того, им же проверялись все сделки участников форума.

"Киберпреступники пользуются самыми хитроумными схемами, а их места общения обладают высокой анонимностью, поэтому противостоять им может лишь схожий по мышлению контингент, разделяющий легальную сторону вопроса с правоохранительными органами", — сообщил Джозеф Бланк, представитель Анти-фродового командного центра RSA.

Структурно деятельность злоумышленников делилась на несколько категорий:

- изготовление поддельных документов (паспорта, водительские права, ценные бумаги и поручения);
- торговля учетными записями известных Интернет-казино, лотерейных агентств, букмекерских организаций;
- организация несанкционированных массовых рассылок;
- разработка и создание вредоносного кода;
- организация сервисов по выводу незаконно полученных денежных средств.

Среди участников форума "MAZA.la" фигурировали такие нагнетавшие "ники", как BadB (Хорохорин Владислав, 27 лет, арестован во Франции), Severa (известный спамер Петр Лавашов, продолжающий криминальную деятельность), zo0mer (Сергей Козерев, в отношении него АНБ США проводилось отдельное расследование по выявлению линий сбыта дампов кредитных карт, продолжает криминальную деятельность), My0 (торговец кредитными картами Роман Кхода, 26 лет), многих из которых постигла весьма суровая участь. Все они, так или иначе, попали, под взгляд Интерпола и международных силовых структур, которые выискивали мошенников годами.

Сами участники признавались, что форум стал доступен не только их "сфере", но и людям в погонах. Впервые один из официальных скриншотов закрытого форума оказался доступен зарубежному Интернет-изданию

"Krebssecurity" 24 октября 2010 года, опубликовавшему скриншот темы форума, в котором обсуждалось появление нового, на тот момент, банковского трояна "SpyEye".

Direct Connection

DC – более закрытый форум, хотя лица там фигурируют абсолютно те же.

Например, Петр Севера (SEVERA), всемирно известный российский спамер, дает рекламу своих услуг на двух площадках, только на DC – делает это в лице модератора.

Неизвестные хакеры взломали оба форума, украв оттуда всю базу пользователей и их переписку. В настоящее время база попала в руки самым известным компаниям по предупреждению киберпреступности и фрода – RSA, Anti Money Laundering Alliance и IISFA.

Комментарии специалистов

Кислицин Никита, главный редактор журнала Хакер:

Случившаяся утечка — чрезвычайно занимательная иллюстрация того, как эффективно можно противостоять электронной преступности с помощью методов, которые традиционно являлись визитной карточкой самих киберпреступников: эксплуатация уязвимостей нулевого дня, применение специального вредоносного софта и т.д. Утекшие данные в очередной раз свидетельствуют о высочайшем уровне организации электронной преступности и о масштабе существующих угроз в области защиты персональных данных и предотвращения хищений из электронных финансовых систем. Получение доступа к столь объемным и ценным базам данных обязательно даст новые вектора для борьбы с киберпреступностью.

Lars van Mulligen, Europol:

Безусловно, борьба с незаконной деятельностью в Интернет является одним из первостепенных вопросов в формировании безопасных условий работы простых пользователей, которые сталкиваются с мошенничеством практически на каждом третьем сайте в Сети. Форумы злоумышленников – один из взаимосвязанных элементов, в отношении которых специалисты правоохранительных органов всех стран должны проявлять совместные усилия.

Никита Семшов, ОАО "Банк "ВТБ":

Каждый банк сталкивается с фактами проявления мошеннической активности, в том числе через каналы Интернет и доверенных пользователей Интернет-банкингов. При всем при этом, реальные организаторы данных правонарушений остаются за кадром, присутствуя на подобных форумах.

www.xakep.ru

Автор: Артур Скальский © Babr24.com ИНТЕРНЕТ И ИТ, МИР 👁 7283 28.02.2011, 23:51 📌 541

URL: <https://babr24.com/?ADE=92017> Bytes: 5454 / 5405 Версия для печати Скачать PDF

👍 Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com

Автор текста: **Артур
Скальский.**

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)