Автор: Роман Предеин ИНТЕРНЕТ И ИТ, МИР 2746 05.02.2012, 13:48 326

«РыБАБЛОвы» в сети

Фишинг стал более изощренным.

Система заработка на платных смс приглянулась мошенникам уже очень давно, однако заставить жертву отправить заветное сообщение на короткий номер, благодаря глобальной предостерегающей пропаганде, стало сложнее. В помощь жуликам пришел не устаревающий метод фишинга.

Фишинг был известен еще в начале девяностых, когда фишеры занимались в основном кражей логинов и паролей различных аккаунтов, пинкодов кредиток, обманывая жертв на огромные суммы денег. Классический фишинг, безусловно, существует и сейчас, но многие фишеры отложили «удочки» и взяли в руки Сеть – так «рыбка» меньше, да «улов» больше.

Google Files и другие «файлообменники»

Основой любого фишинга является грамотная «приманка». Но большинство пользователей сети Интернет уже не доверяют баннерам типа «Заработай миллион за 5 минут», да и вообще каким-либо незнакомым виртуальным сервисам, связанным с деньгами. Но люди доверяют проверенным источникам, а конкретно - Гуглу. Этим и воспользовались мошенники, создав фишинговый сайт G00gle Files.

Безупречный дизайн не оставляет никаких сомнений в том, что подобный портал вполне могли создать в Google. Смущает только адрес, в котором вместо двух «о» стоят нули, но адресную строку, к сожалению, обычный неопытный серфер проверяет редко, да и у портала есть зеркало: www.googleload1.com. У тех, кто слабо понимает что такое доменное имя, адрес вообще не вызывает никаких подозрений.

Что примечательно, поисковик G00gle Files находит все файлы, которые жертва так долго искала. Точнее, он находит все, что угодно (Например файл с именем: заштопанныйносокотбабушкитерминатора.rar) и предлагает скачать это с завидной скоростью.

Есть только одно условие – подтвердить, что вы человек, указав свой номер телефона, на который робот вышлет код для авторизации – практика популярная у многих крупных компаний типа Вконтакте, так что жертва вряд ли сильно насторожится и на этом этапе.

В чем же подвох? Мошенники не смогут получить наши деньги, зная только номер телефона. Мы обязательно должны что-то отправить сами...

Указываем номер телефона, появляется поле «введите полученный код», и тут нам приходит смс: «Вы заказывали код авторизации для Google Files? Ответьте ДА, чтобы получить код». – Вот и «крючок», осталось «клюнуть».

По той же схеме работают бесчисленное множество фишинговых файлообменников. Например: www.fileer0om.f7n.ru, www.googleload1.com, www.myyload9b.f7n.ru, google-fii1e.g8i.ru. Благо, что многие из них уже в «черном списке» самых популярных браузеров.

Узнай сколько у тебя будет детей/мужей/лишних кг и т. д.

Если откровенно жульнические файлообменники еще можно как-то блокировать, то настоящий рассадник фишинга http://rutesters.com/ будет, вероятно, действовать долго и безнаказанно.

«Фишка» сервиса заключается в предоставлении всевозможных тестов, которые никак не выходят из моды со времен женских журналов, бесплатно. Да-да, тесты действительно бесплатны. А вот, чтобы результаты получить надо пройти уже привычную регистрацию, где, естественно, необходимо подтвердить, что вы человек. Каким образом, дума, уже ясно.

Rustesters – это виртуальная гадалка, которая разводит на реальные деньги.

Поиск по национальной базе данных

Как заверяют нас обманщики, на этом «секретном» сайте, ссылками на который забита вся Сеть можно найти всю информацию, зная паспортные данные или номер телефона любого человека.

Для получения этой информации в системе нужно, кто бы сомневался, авторизоваться уже известным нам способом.

Не менее примечательным является то, что мы увидим, проверив в каком домене находится «национальная база» – снова http://rutesters.com/

Не хотите отправлять смс? Мы сделаем это за вас!

Бум на мобильные операционные системы настоящий подарок судьбы для опытных фишеров. Требуется просто внедрить вредоносный код в коммуникатор жертвы, который сам отправит платную смс на заданный номер.

Раньше вирус внедрялся под видом полезной программы, но многие пользователи предпочитают не устанавливать программы неизвестных разработчиков. Благо, проверенных приложений хватает. Поэтому, схему пришлось усложнить.

Теперь скрипт запускается при нажатии кнопки на фишинговом сайте, замаскированном под официальный магазин той или иной ОС или системную ошибку типа «база данных вашего антивируса устарела», «Опера не может запустить содержимое сайта, обновите Оперу» и т. д.

Будьте осторожны.

Автор: Роман Предеин © Областная газета ИНТЕРНЕТ И ИТ, МИР 2746 05.02.2012, 13:48 326
URL: https://babr24.com/?ADE=102273 Bytes: 4429 / 4393 Версия для печати Скачать PDF

Автор текста: **Роман Предеин**.

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