

Прогнозы и предсказания: что станет объектом хакерских атак в 2018 году?

Несмотря на все старания служб по кибербезопасности, хакеры совершенствуются и придумывают все новые и новые способы залезть в чужой компьютер и что-то там украсть. Порой за их совершенством не успевают самые продвинутые «защитники». Несмотря на широкий спектр хакерских интересов, эксперты выделили основные направления, на которых в 2018 году следует ожидать усиления хакерской активности.

Криптовалюта всем нужна

Не так давно эксперты стали предрекать биткоином и прочим криптовалютам крах и судьбы мыльного пузыря. Вот только со временем «лопая» они никак не могут определиться – то ли сейчас, то ли через год, то ли через 20 лет. Во всяком случае, большая стоимость биткоинов привлекает киберпреступников, и в 2018 году данное направление будет пользоваться усиленным вниманием хакеров.



Компания High-Tech Bridge провела исследование и показала, что 94% приложений в Google Play, так или иначе связанных с криптовалютами, имеют по три уязвимости минимум. Этим и будут пользоваться хакеры.

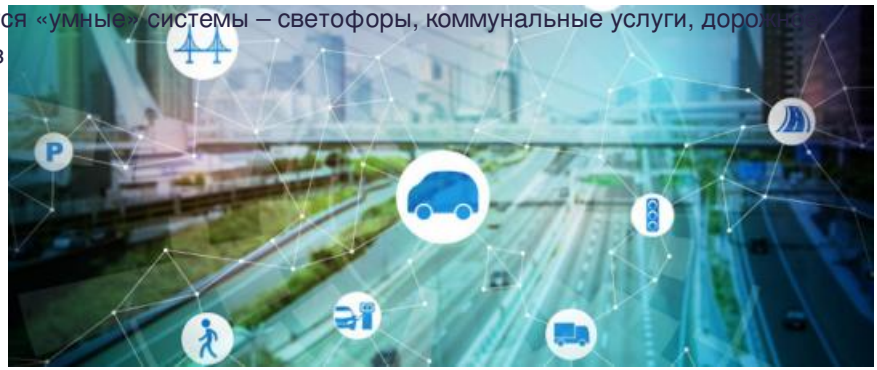
Второе направление – это вредоносные программы и приложения, которые проникают в компьютеры и смартфоны и используют ваши гаджеты для скрытого майнинга криптовалют. Такие процессы резко замедляют производительность системы, но владелец гаджета не связывает это со скрытым майнингом, а пробует запускать меньше приложений или перезагружать систему.

Также усиленным вниманием киберпреступников будут пользоваться криптоплатформы, с которых будут красть не саму криптовалюту, а токены. Их стоимость исчисляется миллионами, и они будут даже популярнее, чем отдельные биткоины.

Владельцы криптокошельков зачастую не запоминают имя своих виртуальных портмоне, поэтому начинающие хакеры часто «развлекаются» тем, что меняют несколько символов и получают переводы, осуществляемые владельцем реального кошелька, на свои счета.

«Умные» вещи

В городскую жизнь активно включаются «умные» системы – светофоры, коммунальные услуги, дорожное движение. Все это управляется через мобильные сети, и их уязвимости могут привести к тому, что «умные» городские системы «сойдут с ума». Что при этом будет твориться в городе – нетрудно себе представить.

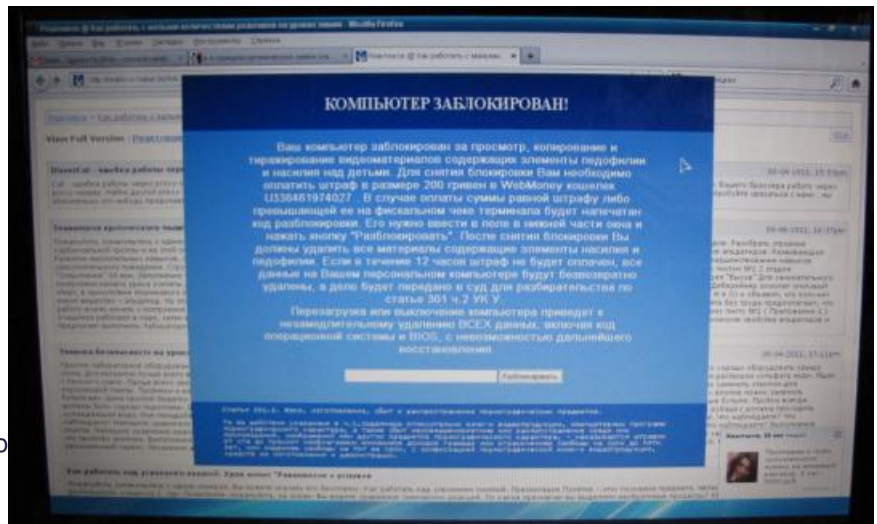


Даже в масштабах одного дома количество «умных» вещей постоянно растет. IoT-устройства проникают в производство, добывающую промышленность и энергетику. Машины общаются друг с другом без участия человека, и решения принимаются также между машинами. К сожалению, мир «умных» вещей не синхронизирован в плане кибербезопасности, и среди них есть такие, которые позволяют следить за вашей жизнью даже самому неопытному хакеру.

Так, эксперты обещают увеличение уровня атак на Smart TV. Также в 2018 году предполагается большое количество программ-вымогателей, которые будут блокировать «умные» устройства и требовать от владельцев выкуп за восстановление доступа.

Число вирусов-вымогателей вырастет

Успех, который имели зловреды WannaCry и Petya, повернул мысли хакеров в сторону совершенствования вирусов-вымогателей, число которых в 2-18 году будет только расти. Эксперты прогнозируют, что киберпреступники будут использовать уязвимости удаленного выполнения кода. Тогда для распространения программ-вымогателей не нужно будет взаимодействовать с самим пользователем. Также ожидается, что хакеры будут более избирательно подходить к выбору жертв и устройств. Такие атаки будет очень сложно отследить.



В сегменте приложений для смартфонов будет все больше и больше подделок, замаскированных под легальное ПО, которые будут выманивать у пользователей данные аккаунтов и банковских карт. Также эксперты ожидают рост числа программ-шифровальщиков, которые будут шифровать данные на смартфонах. Подчас на мобильных устройствах хранится больше важных данных, нежели на ПК, и большинство пользователей будут больше готовы заплатить, нежели потерять информацию.

Хакер и банкомат


Атаки киберпреступников на банкоматы стали еще одним печальным трендом 2017 года. При этом хакеры научились контролировать целые сети банкоматов через локальную сеть банка. Тенденция сохранится и преумножится в 2018 году, тем более что технология отработана, растратирована, а инструкции и инструмент доступны всем желающим. За несколько тысяч долларов можно подобрать комплект ПО для взлома банкомата, опустошить устройство и браться за следующее. Затраты окупаются за несколько атак, говорят эксперты, и поэтому тенденция взломов банкоматов сохранится до тех пор, пока банки не объединятся и не начнут массово внедрять эффективные технологии защиты.



Киберпреступники не стоят на месте. Будем надеяться, что их оппоненты не станут отставать, а еще лучше – наконец-то обгонят мошенников, и сделают нашу жизнь легче и безопаснее.

Автор: Алина Саратова © SmartBabr



НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР  2893 22.01.2018, 13:58  18

URL: <https://babr24.com/?IDE=272706> Bytes: 5510 / 4675 [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: **Алина
Саратова.**

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: equatoria@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](#)