Babr24.com

Автор: Алиса Беглова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 5088 19.09.2020, 19:12
0

Главные киберугрозы-2020: фишинг, шпионы, трояны и бэкдоры

Специалисты международной компании Group-IB, специализирующейся на предотвращении кибератак, назвали самые распространённые киберугрозы первого полугодия 2020 года — то есть как в тот отрезок времени, когда в России и по всему миру бушевала пандемия.

На первом месте — **фишинг,** на который пришлось 46% от общего числа фейковых веб-страниц.

Фишинг дословно переводится с английского как «ловля рыбы» и обозначает вид мошенничества, в котором используется сайт-ловушка. Например, злоумышленники создают сайт, имитирующий официальный сайт банка (с разницей в доменном имени в одну или пару букв). Невнимательный пользователь переходит на сайт (думая, что это официальный сайт кредитного учреждения) и вводит на нём свои банковские данные. Заманить жертву на поддельную страницу можно с помощью email-писем якобы от банка.

Способ защиты от фишинга один — внимательно читайте адреса сайтов в адресной строке браузера. У безопасных сайтов там стоит значок замочка (это значит, что сайт поддерживает защищённое соединение).

На **вложения с программами-шпионами** или ссылки, ведущие на их скачивание, пришлось 43% проанализированных Group-IB вредоносных писем, ещё 17% содержали загрузчики.

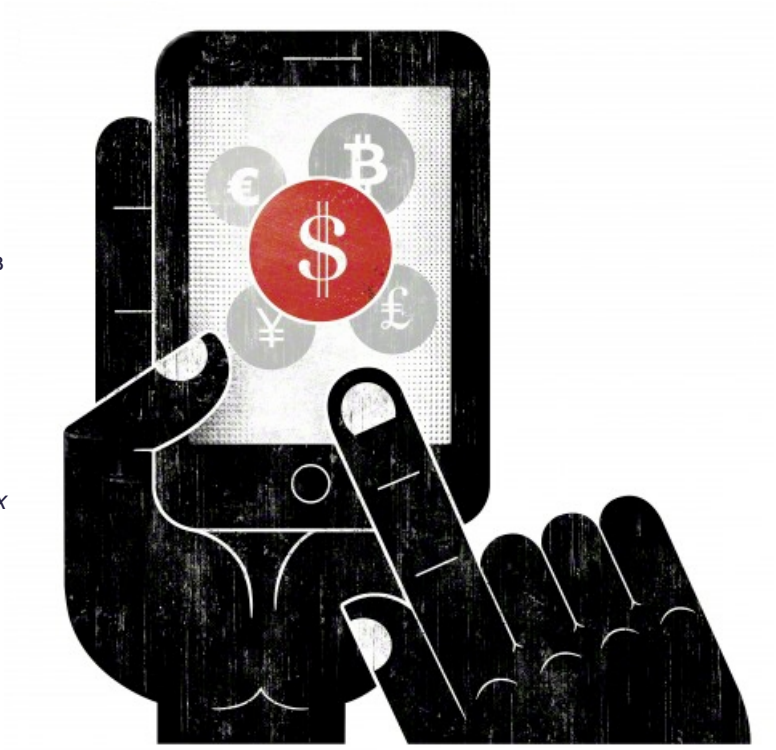
Программа-шпион скрыто устанавливается на компьютер или смартфон с целью сбора информации с устройства.

Третье место в числе киберугроз разделили **бэкдоры и банковские трояны** — они скрывались в 16% и 15% вредоносных рассылок соответственно.

Банковский троян — это вредоносная программа, которую злоумышленники устанавливают на смартфон жертвы для кражи банковских данных под видом лицензионной программы. Банковские трояны могут: мимикрировать под мобильные приложения банков; действовать в автоматическом режиме, время от времени отправляя относительно небольшие суммы на счета преступников; скрывать от пользователя банковские SMS с паролями и тут же перенаправлять их злоумышленнику.

Бэкдор (дословно — «тайный вход») — вредоносная программа, которая открывает для злоумышленников удаленный доступ к компьютерам жертв для осуществления несанкционированных действий. Бэкдоры могут воровать персональные данные пользователя, скачивать и отправлять файлы, открывать доступ для вирусов и червей, подключаться к удаленным хостам, делать компьютер частью ботнета — всё это осуществляется незаметно для владельца.

Почти 70% вредоносных файлов попадали на компьютер жертвы с помощью архивов, около 18% были замаскированы под офисные документы с расширениями .doc, .xls и .pdf, ещё 14% скрывались под исполняемыми файлами и скриптами.



Специалисты по кибербезопасности отмечают, что практически полностью исчезли **программы-шифровальщики,** которые в прошлом полугодии были в каждой второй вредоносной рассылке. Шифровальщик — вредоносное программное обеспечение, предназначенное для вымогательства после шифрования файлов в системе.

«Операторы шифровальщиков сфокусировались на целевых атаках, выбирая себе крупные жертвы, и требуя от них значительно большие суммы. Точечная проработка таких атак снизила их объем в антирейтинге угроз, а на их место пришли программы-шпионы и бэкдоры, с помощью которых злоумышленники сначала похищают чувствительную информацию, а затем шантажируют жертву, требуя выкуп, и, в случае отказа, продают ее на хакерских форумах или выставляют в паблик. Вероятнее всего, стремление операторов шифровальщиков сорвать большой куш постепенно приведет к росту таргетированных атак, при этом почта по-прежнему будет главным источником их распространения, что повышает требования к обеспечению ее кибербезопасности», — рассказал замруководителя CERT-GIB Ярослав Каргалев.

Отметим, за время пандемии широта мысли злоумышленников и мошенников вышла на качественно новый уровень. В ход пошли новые способы отъёма денег, лежащие в том числе в киберсфере. Подробнее об этом:

«Коронавирусное» мошенничество: способы отъёма денег

Автор текста: **Алиса Беглова**,
обозреватель.

На сайте опубликовано **257**
текстов этого автора.

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