Интерфейс преступников меняет профиль

По данным представителей органов правопорядка, в период пандемии в большинстве стран резко снизилась доля уличных преступлений. Но, к сожалению, не сбавляются темпы киберпреступности. Как противостоять сетевым мошенникам?

Эксперты отмечают, что с самого начала пандемии существенно изменился ландшафт киберугроз. Например, в марте текущего года число атакованных пользователей выросло на 6 %, а количество атак – на 35 % по сравнению с предыдущим месяцем. В текущих условиях злоумышленники не прекращают свою деятельность. Число атак программ-шифровальщиков также выросло по сравнению с февралем – на 5 %. Текущая новостная повестка активно используется злоумышленниками для фишинга, а также при проведении целевых атак.

Однако в целом количество атак вредоносного ПО уменьшается. По данным исследований российской компании «Лаборатория Касперского», в мире в 2019 году такие программы были зафиксированы на устройствах каждого пятого пользователя, что на 10 % меньше, чем в 2018 году. Также в два раза сократилось количество уникальных вредоносных ресурсов, где были заблокированы попытки заражения, и количество таких атак. Но одновременно с этим растет количество уникальных вредоносных программ.

По словам ведущего антивирусного эксперта компании Сергея Голованова, число угроз снижается, но они становятся более изощренными. Это приводит к тому, что растет уровень сложности задач, стоящих перед защитными решениями и сотрудниками отделов безопасности. Кроме того, злоумышленники расширяют географию успешных атак. Так, если какая-то угроза помогла атакующим достичь своих целей в одном регионе, то затем они реализуют ее и в другой точке мира. Для предотвращения атак и сокращения их числа эксперт рекомендует обучать навыкам кибербезопасности сотрудников всех уровней и отделов, а также регулярно проводить инвентаризацию сервисов и оборудования.

Чтобы проникнуть в корпоративные сети, в каждом третьем случае злоумышленники проводят атаки на инфраструктуру, ищут открытые порты или подбирают пароли. Так же часто заражение происходит через вредоносные файлы, либо загруженные через интернет, либо отправленные по электронной почте.

Нередко нежелательное и вредоносное ПО злоумышленники распространяют под видом треков, написанных известными диджеями. Самыми популярными у преступников в 2019 году оказались Дэвид Гетта, Алан Уокер, DJ Snake, Кельвин Харрис и Мартин Гаррикс – имена этих диджеев фигурировали чаще других. Например, под видом танцевальных треков распространялись установщики нежелательного софта, рекламное ПО (AdWare), а также различные семейства троянцев и майнеров. Так, примерно каждый пятый подобный файл (22 %) представлял собой образец одного из семейств класса not-a-virus:Downloader. Такие программы навязчиво предлагают пользователям установить сторонний нежелательный софт еще до того, как человек получает доступ к нужному ему файлу.

– Злоумышленники следят за всеми трендами, в том числе музыкальными, и используют их в своих интересах, – комментирует ситуацию антивирусный эксперт Антон Иванов.

Согласно новому опросу «Лаборатории Касперского» о влиянии COVID-19 на стиль работы, в период самоизоляции **31 %** сотрудников в мире стал тратить на профессиональную деятельность больше времени, чем раньше. Общепринятые меры по борьбе с пандемией коронавируса привели к тому, что работникам большинства компаний пришлось приспособиться к новой профессиональной среде. В таких условиях нередко размываются границы между личной жизнью и работой. В то же время у сотрудников высвободилось время, которое теперь не нужно теперь тратить, чтобы добраться до работы. И **46 %** опрошенных заявили, что им теперь удается чаще бывать с семьей и больше времени посвящать личным делам.

Кроме того, **55 %** респондентов отметили, что читали меньше новостей, до того как начали работать

из дома. Причем **60 %** из них сейчас читают новости онлайн на устройствах, которые используют и для работы. Подобная тенденция увеличивает шансы заражения вредоносным ПО, если сотрудники не уделяют должное внимание тому, какие веб-ресурсы они посещают.

Другая киберугроза в нынешних условиях – это теневые IT (не одобренные компанией сервисы, которые тем не менее применяются сотрудниками для работы). Например, **42 %** используют личную почту для решения рабочих вопросов, и половина из них признают, что подобное использование возросло при удаленной работе. Кроме того, **38 %** респондентов общаются по работе в мессенджерах, не одобренных IT-отделами компаний, и **60 %** из них делают это чаще именно в новых обстоятельствах.

– Организации просто не могут себе позволить удовлетворять все запросы сотрудников, например разрешать им пользоваться любыми сервисами по собственному усмотрению. В сложившихся обстоятельствах необходимо найти баланс между удобством пользователей, бизнес-необходимостью и безопасностью. Для этого компании должны обеспечить доступ к сервисам, которые предоставляют минимальные, только необходимые привилегии, использовать защищенные и одобренные корпоративные системы. Подобное ПО может иметь определенные ограничения, которые несколько снижают удобство его использования, при этом дают гораздо большие гарантии в соблюдении мер кибербезопасности, – комментирует Андрей Евдокимов, руководитель отдела информационной безопасности «Лаборатории Касперского».

В связи с этим эксперты рекомендуют организациям придерживаться следующих мер кибербезопасности:

• запланируйте обучение сотрудников основам информационной безопасности, в том числе онлайн. Это позволит научить их управлять учетными записями и паролями, обеспечивать безопасность электронной почты и конечных устройств;

• убедитесь, что устройства, программное обеспечение, приложения и сервисы регулярно обновляются;

• установите проверенное защитное ПО.

Самим сотрудникам и всем домашним пользователям рекомендуется использовать надежное решение для комплексной защиты от широкого спектра угроз, а также загружать образовательный и развлекательный контент только из надежных источников.

По данным исследований «Лаборатории Касперского»