Trend Micro представляет прогноз кибербезопасности на 2019 год

Обзор актуальных киберугроз для бизнеса и обычных пользователей

Компания Trend Micro Incorporated — мировой лидер в области решений для обеспечения кибербезопасности, опубликовала отчет MAPPING THE FUTURE, в котором представляет прогноз ключевых угроз и тенденций кибербезопасности в 2019 году: от мобильных устройств и IoT до облака.

В 2019 году прогресс в области искусственного интеллекта и машинного обучения, обусловленного постоянно растущим объемом данных, окажет колоссальное влияние на технологии и безопасность. Миграция предприятий в облако, распространение подключенных устройств/IoT/IIoT, полномасштабное внедрение сетей 5G создадут больше возможностей для проведения эффективных атак злоумышленниками, которые могут нанести многомиллиардный ущерб мировой экономике.

Фишинговые атаки по электронной почте станут самой распространенной угрозой как среди потребителей, так и бизнеса. На подъеме находятся все типы атак по электронной почте: будь то использование

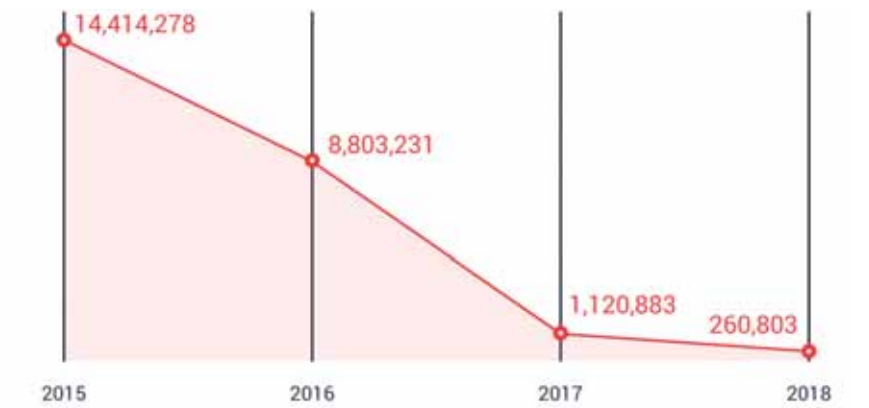

Figure 1. Exploit kit activity blocked decreased over the years, based on data from the Trend Micro™ Smart Protection Network™ infrastructure as of Q3 2018.

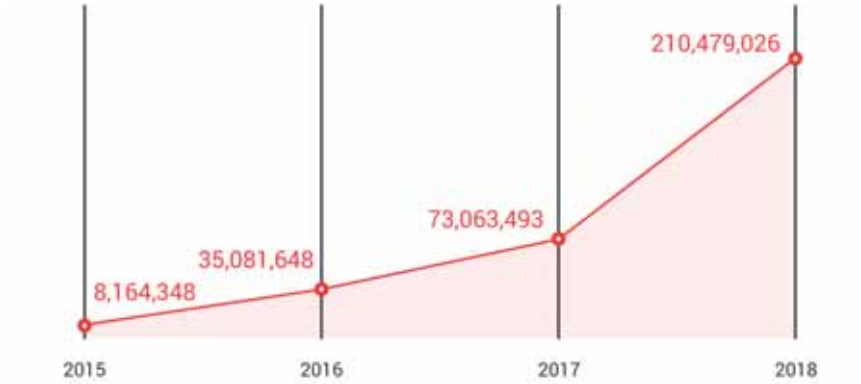

Figure 2. Phishing-related URLs blocked increased over the years, based on data from the Trend Micro Smart Protection Network infrastructure as of Q3 2018.

вредоносной ссылки, вложения или проведение целевых BEC-атак (компрометация деловой переписки), которые содержат определенные текстовые сообщения-ловушки. С 2015 года количество фишинговых URL-адресов, заблокированных Trend Micro, увеличилось почти на ***3800%***. В то же время обнаружение наборов эксплойтов за тот же период сократилось на 98%. Это подтверждает сдвиг в киберпреступной тактике от использования эксплойтов к практике использования социальной инженерии.

В следующем году в информационном пространстве появится больше неизвестных киберугроз, что усилит потребность в многоуровневом подходе к кибербезопасности. Корпоративные сети предприятий должны быть надежно защищены от новых и существующих видов атак.

Краткое резюме отчета Trend Micro по всем сегментам рынка, для которых существуют киберриски, представлено ниже.

Потребитель:

- Атаки при помощи социальной инженерии заменят распространение эксплойтов.
- Чат-боты будут скомпрометированы.
- Аккаунты знаменитостей будут

подвергаться атакам типа Watering Hole.
- Продолжится массовое использование украденных учетных данных.
- Будут изучены последствия от применения цифрового вымогательства с возможным увеличением смертности людей из-за «sextortion» (шантаж разоблачениями из чьей-либо личной жизни).

Бизнес:

- Предоставление возможности сотрудникам работать из дома может обернуться угрозой для безопасности предприятий, в частности, благодаря росту популярности концепции BYOD («принеси свое собственное устройство»).
- Регуляторы GDPR (общий регламент по защите данных) оштрафуют первого «громкого» нарушителя на полные 4% оборота.
  - Компаниям придется переосмыслить ценность операций по сбору и анализу данных пользователей, присущую текущим рекламным моделям, так как такое нарушение будет дорого стоить.
  - К 2020 году до 75% новых бизнес-приложений должны будут выбирать между удобством и безопасностью.
- Реальные события в мире (чемпионаты, концерты, выборы) будут использоваться в атаках социальной инженерии.
- Компрометация деловой переписки (BEC) опустится на два уровня ниже организационной структуры предприятия.
- Автоматизация станет новым препятствием в компрометации бизнес-процессов.

Государства:

- Борьба с фейковыми новостями будет разворачиваться под давлением различных предвыборных гонок.
  - События затронут Грецию, Польшу, Украину, Южную Африку, Нигерию, Индонезию и Индию.
- Невинные жертвы попадут под перекрестный огонь, так как страны будут наращивать собственное киберприсутствие.
- Усиление регулирующего надзора.
  - В центре внимания — конфиденциальность личной жизни и IoT.

Индустрия безопасности:

- Киберпреступники будут использовать больше скрытых методов атак.
- 99,99% атак на основе эксплойтов попрежнему не базируются на уязвимостях нулевого дня.
- Получат распространение целенаправленные атаки, в том числе с помощью искусственного интеллекта.

Промышленные системы управления:

- Реальные атаки на промышленные системы управления станут предметом

растущей озабоченности.
- Баги в HMI по-прежнему будут основным источником уязвимостей SCADA.

Облачная инфраструктура:
- Неправильная настройка параметров безопасности во время миграции в облако приведет к большему количеству утечек данных.
- Облако будет использоваться для майнинга криптовалют.
- Будут обнаружены дополнительные уязвимости облачного программного обеспечения.

Умные дома:
- Киберпреступники будут бороться за доминирование в «войне червей» для IoT-устройств.
- Появятся первые случаи, когда пожилые люди станут легкими жертвами атак через IoT/Умные девайсы для здоровья.

Для ознакомления с полной версией отчета MAPPING THE FUTURE, пожалуйста, посетите страницу ***https://www.trendmicro.com/vinfo/ru/security/research-and-analysis/predictions/2019***

О компании Trend Micro

Trend Micro Incorporated, мировой лидер в области решений для кибербезопасности, помогает сделать безопасным обмен цифровой информацией во всем мире. Наши инновационные решения для домашних пользователей, предприятий и госструктур обеспечивают многоуровневую безопасность центров обработки данных, облачных инфраструктур, сетей и конечных точек. Все наши продукты работают в тесной взаимосвязи друг с другом для беспрепятственного обмена данными об угрозах и обеспечения быстрой и качественной защиты с централизованным управлением. Более 6000 сотрудников из 50 различных стран и самая передовая система обнаружения и исследования угроз Trend Micro помогает организациям обеспечивать безопасность их сетевой инфраструктуры.

Для получения более подробной информации посетите сайт:
trendmicro.com.ru