Бойтесь «троянцев», дары приносящих

Опасная программа для кражи паролей распространяется через спам в корпоративной почте

Эксперты Kaspersky обнаружили вредоносную спам-кампанию. Ее цели – организации по всему миру, в том числе и в Беларуси. Атакующие пытаются украсть учетные данные с помощью программы-стилера Agent Tesla. Они распространяют зловред через письма якобы от поставщиков или контрагентов. Всего с апреля по август 2022 года решения «Лаборатории Касперского» обнаружили около 740 тысяч писем в рамках этой кампании. Украденные данные злоумышленники могут продавать на форумах в даркнете или использовать в дальнейших целевых атаках на те же организации.

Agent Tesla – троянец-шпион, который умеет красть логины и пароли из браузеров и других приложений, делать скриншоты, а также собирать данные с веб-камер и клавиатур. Зловред распространяется в виде архива в электронном письме.

Судя по данным Kaspersky, злоумышленники все тщательнее готовят массовые спам-атаки. Обычно такие письма довольно примитивны и не отличаются разнообразием, но в последнее время в массовых рассылках стали прослеживаться приемы, характерные для целевых атак. В частности, атакующие рассылают письма от имени существующих компаний, копируют стиль письма и подпись отправителя. Например, в этой вредоносной кампании деловые письма подделаны очень хорошо. Единственное, что выдает злоумышленников, – это странные адреса отправки. Так, одна из рассылок шла с адреса newsletter@trade***.com, а содержала поддельную информацию о закупках. Слово же «newsletter» обычно используется в новостных рассылках, а не для переписки по закупкам. Кроме того, доменное имя отправителя отличалось от официального названия компании на логотипе.

Одно из писем на белорусском языке якобы от представителя некоего завода содержало предложение оформить заказ на его продукцию. С условиями можно было ознакомиться в документе из прикрепленного к письму архива. Адрес отправителя не соответствовал адресу в автоподписи.

Объединяет эти письма не только схожий сценарий рассылки и то, что они не похожи

Рисунок 1 – Пример вредоносного письма с подозрительного адреса newsletter@trade***.com

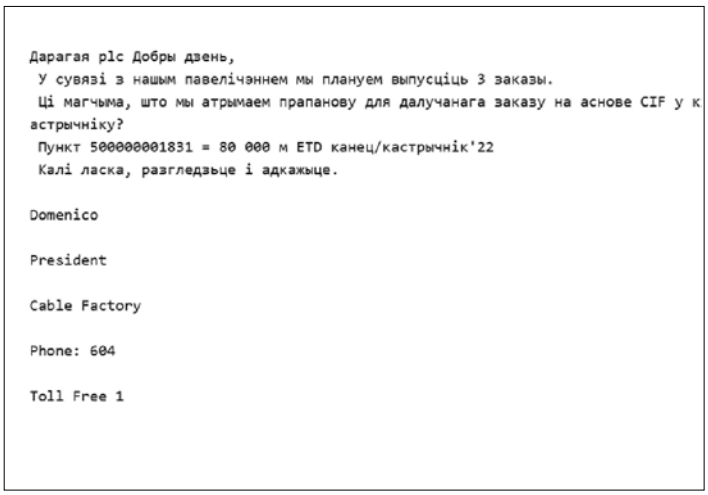

Рисунок 2 – Пример вредоносного письма на белорусском языке

на автоматически сгенерированные. Заголовки писем также имеют одну и ту же структуру. Кроме того, сообщения приходят с ограниченного набора IP-адресов. Это означает, что они являются частью одной большой вредоносной почтовой кампании.

«Agent Tesla –популярный стилер, который мошенники используют еще с 2014 года для кражи паролей и других учетных данных. Но в последнее время эксперты фиксируют переход злоумышленников от массовых вредоносных рассылок к целевым почтовым атакам на организации. Их письма выглядят все более правдоподобно, и компаниям необходимо уделить особое внимание защите почтового сегмента, как с точки зрения применения защитных технологий, так и в плане обучения сотрудников основам киберграмотности», – комментирует Дмитрий Кудревич, представитель Kaspersky в Республике Беларусь.

Продукты Kaspersky детектируют стилер Agent Tesla как Trojan-PSW.MSIL.Agensla.

Узнать больше об Agent Tesla можно в полном отчете на Securelist: https://securelist.ru/agent-tesla-malicious-spam-campaign/105932/.

Чтобы защититься от подобных рассылок, «Лаборатория Касперского» рекомендует организациям следующие меры безопасности:

– обучать сотрудников правилам информационной безопасности, регулярно проводить тренинги, в том числе посвященные безопасному обращению с электронной почтой;

– установить специализированную защиту для почтовых серверов, в которую входят функции борьбы с фишингом, спамом и детектирования вредоносного ПО.

Лаборатория Касперского
специально для журнала «Веснік сувязі»

7,8 % белорусских компаний ничего не делают для обеспечения кибербезопасности

К такому выводу пришли эксперты компании hoster.by по результатам недавнего исследования кибербезопасности белорусского бизнеса. Всего в нем приняло участие 477 респондентов. Больше половины участников опроса – представители трех отраслей: оптовой и розничной торговли (28 %), информационных технологий (15,5 %) и промышленности (15,5 %). Отвечали на вопросы в основном руководители компаний или ИТ-подразделений – на их долю приходится 68 % ответов.

Как бизнес воспринимает киберугрозы?

Первая вероятная цель кибератаки – сайт компании. Он есть практически у всех (98 %) участников опроса. Из них 46 % отметили, что на сайте компании есть личный кабинет. Это значит, что компания собирает данные о пользователях, которые могут стать потенциальной целью кибератаки.

Более половины участников опроса (54 %) считают, что хакерская атака на них возможна, но вероятность не очень высокая. Еще 35 % воспринимают эту вероятность как крайне низкую. Возможно, это связано с особенностями ИТ-инфраструктуры респондентов: среди тех, кто отметил низкую вероятность хакерской атаки, у 62 % нет личного кабинета на сайте, а значит, они не самая привлекательная цель для взлома. Только 11 % участников опроса считают, что вероятность хакерской атаки на их компанию очень высокая.

В отличие от сотрудников малых предприятий и индивидуальных предпринимателей сотрудники средних и крупных компаний более настороженно относятся к кибератакам. Хакерскую атаку назвали маловероятной 39 % представителей малого бизнеса и 45 % индивидуальных предпринимателей, принимавших участие в опросе.

Еще одна потенциальная точка уязвимости – электронная почта. Этот инструмент используется для бизнес-переписки, и поэтому может быть объектом хакерских атак. Наибольший риск представляет использование личной почты для бизнес-задач. Результаты опроса показали, что только четверть опрошенных не пользуется специальной корпоративной почтой. Еще 5 % участников опроса сознались, что корпоративная почта в ходу у них на работе, но они все равно используют личную.

С какими угрозами информационной безопасности бизнес сталкивался в этом году?

«Белтелеком» напоминает

Чтобы не стать жертвой киберпреступника, рекомендуется придерживаться простых правил безопасного пользования интернетом.

1. Создавайте надежные пароли. Используйте сложные для подбора пароли к разным сервисам: минимум 10 символов, одновременно цифры, строчные и прописные символы и др. Доверяйте только проверенным менеджерам паролей. Не используйте одинаковые пароли для разных аккаунтов.
2. Будьте внимательны к соединениям Wi-Fi. Отключайте общий доступ к своей точке Wi-Fi, даже если у вас безлимитный интернет. Используйте надежный пароль для доступа к вашей сети. Деактивируйте автоматическое подключение своих устройств к открытым точкам Wi-Fi.
3. Используйте проверенные браузеры и сайты. Подключите специальное ПО (расширение для браузера), чтобы избежать посещения сомнительных сайтов. Не скачивайте контент с ненадежных сайтов: он может содержать вредоносный код.
4. Защитите электронную почту. Подключите двухфакторную аутентификацию и используйте спам-фильтры.
5. Будьте осторожны с приложениями, соцсетями и мессенджерами. Устанавливайте приложения только из PlayMarket, AppStore или проверенных источников. Обращайте внимание, к каким функциям гаджета приложение запрашивает доступ. Обменивайтесь сообщениями в соцсетях и мессенджерах, только полностью убедившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.
6. Установите антивирусные программы. Применяйте и регулярно обновляйте антивирусное ПО, которое сможет обнаруживать потенциальные угрозы.

В основном респонденты воспринимают ситуацию спокойно: больше половины опрошенных (67 %) отметили, что не сталкивались с угрозами информационной безопасности за прошедшие 12 месяцев. Однако это не означает, что компании действительно не сталкивались с такими угрозами: зачастую последствия взлома дают знать о себе далеко не сразу. В частности, трояны и бэкдоры могут годами работать незаметно, чтобы активизироваться в самый удобный для злоумышленника момент.

Среди наиболее распространенных угроз, которые все же были зафиксированы, заражение рабочих компьютеров вирусами (16,1 %), атаки на сайт (15,9 %) и поломка оборудования с остановкой работы сайта (9,2 %).

Реже всего участники опроса сталкивались с утечками корпоративных данных из-за ошибок сотрудников (2,7 %), интернет-мошенничества (2,3 %) и взлома хранилищ корпоративных данных (1,4 %).

Как бизнес защищается от угроз инфобезопасности?

Наиболее распространенные способы защиты от киберугроз – установка антивирусов (66 %) и резервное копирование данных (62,8 %). Наименее популярные меры – оценка рисков и угроз (9 %) и регулярный аудит инфобезопасности (5,8 %).

Довольно много опрошенных (17,8%) отметили, что в их компаниях не предпринимается никаких мер для обеспечения информационной безопасности. 85% из них работают в качестве индивидуальных предпринимателей или в компаниях со штатом до 15 человек.

А что с личной кибербезопасностью?

Самые популярные тактики личной защиты – это использование антивирусных программ (71 %), применение сложных паролей из цифр, букв и спецсимволов (68,3 %) и создание разных паролей для всех ресурсов (64,5 %). Реже всего участники опроса прибегают к закупке лицензионного программного обеспечения (16,5 %). То ли санкции не позволяют, то ли еще силен пиратский дух. Совсем ничего для своей кибербезопасности не предпринимает всего 5,4 % респондентов.

https://www.kv.by
High-Tech Club