АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Деятельность кибергруппы Sednit под микроскопом

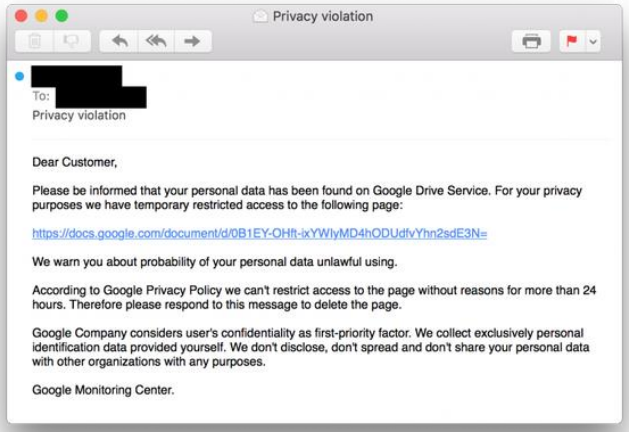
20 октября 2016 года

Мы уже несколько раз писали о деятельности кибергруппировки Sednit (APT28, Fancy Bear, Pawn Storm, Sofacy) в предыдущих постах нашего корпоративного блога. Эта группировка пыталась скомпрометировать более 1000 пользователей в различных организациях с использованием фишинговых атак, а также эксплойтов нулевого дня. Атакующие заинтересованы в краже конфиденциальной информации с компьютеров скомпрометированных пользователей.

Sednit осуществляла кибератаки на пользователей как минимум с 2004 г., при этом для их реализации использовались изощренные методы с обходом настроек сетевой безопасности. Исследователи ESET отслеживали деятельность группировки Sednit на протяжении последних двух лет. Sednit уличали в кибератаках на Комитет по выборам в Конгресс Демократической партии, немецкий парламент, серверы французского телеканала TV5Monde, а также антидопинговое агенство WADA.

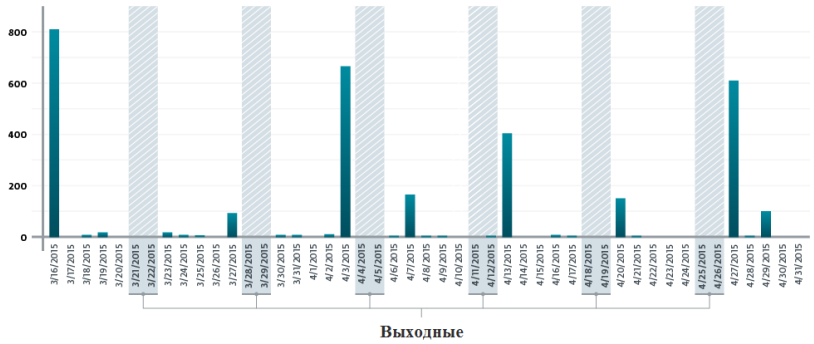
Кража конфиденциальной информации учетных данных почтовых сервисов

Для кражи учетных данных почтовых сервисов пользователей группировка использует довольно распространенный метод. Он заключается в рассылке направленных фишинговых сообщений, где расположены URL-ссылки, ведущие на фальшивые веб-страницы входа в учетную запись, где нужно ввести логин и пароль.



Фишинговые электронные письма используют методы социальной инженерии для обмана пользователей. Пользователю пытаются внушить, что ему нужно перейти по указанной ссылке как можно скорее, при этом он может забыть о возможных последствиях такого шага.

В результате анализа наши специалисты обнаружили 1,888 уникальных адресов электронной почты, на которые рассылались фишинговые сообщения между 16 марта и 14 сентября 2015 г. При этом видно, что наибольшее количество атак приходится на понедельник или пятницу.



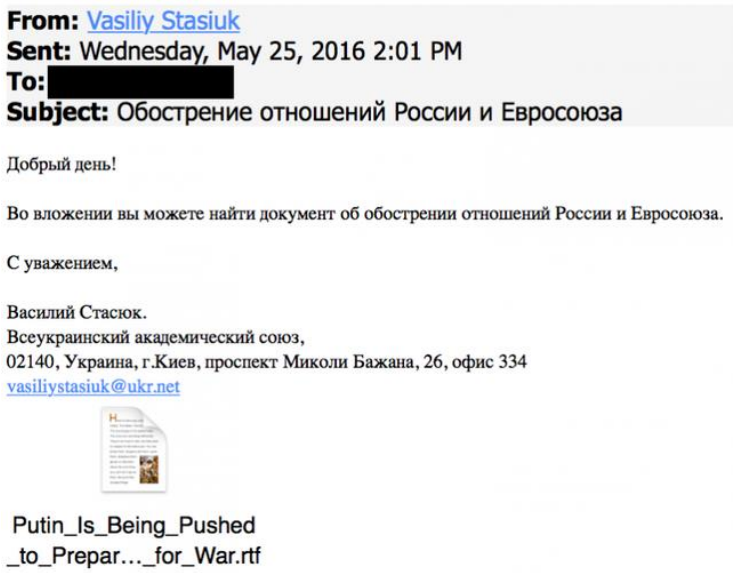
Наши специалисты предполагают, что регулярные всплески активности соответствуют времени запуска новых фишинговых кампаний.

Вредоносные сообщения электронной почты

Группировка Sednit использует сообщения электронной почты для заражения пользователей, отправляя им либо вредоносное вложение, либо вредоносную ссылку на набор эксплойтов

внутри письма. В случае с вложениями, Sednit прибегает к эксплойтам для таких распространенных продуктов как Microsoft Word, Microsoft Excel, Adobe Flash и Adobe Reader.

На скриншоте ниже можно увидеть используемое группировкой фишинговое сообщение, якобы от Всеукраинского экономического союза, к которому приложен документ с информацией об обострении отношений между Россией и ЕС.


From: Vasiliy Stasiuk
Sent: Wednesday, May 25, 2016 2:01 PM
To: [redacted]
Subject: Обострение отношений России и Евросоюза

Добрый день!

Во вложении вы можете найти документ об обострении отношений России и Евросоюза.

С уважением,

Василий Стасюк.
Всеукраинский академический союз,
02140, Украина, г.Киев, проспект Миколи Бажана, 26, офис 334
vasiliystasiuk@ukr.net

Putin_Is_Being_Pushed
_to_Prepar…_for_War.rtf

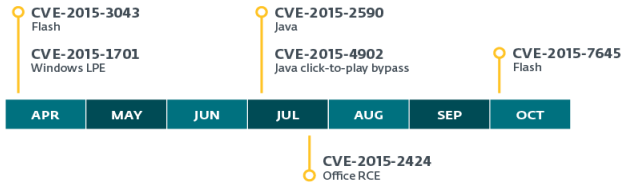
В данном конкретном случае, прикрепленный файл в формате RTF эксплуатирует уязвимость в Office для сбрасывания на диск жертвы другого вредоносного компонента. В случае других кибератак, группировка использовала темы актуальных новостных лент для заманивания пользователя на вредоносный ресурс для загрузки файла. Примеры таких тем новостей приведены ниже.

- «West’s military advantage is being eroded, report warns»
- «Despite ISIS Attacks, North Korea Remains the `Varsity` of Global Threats»
- «Taking War Seriously: a Russia-NATO Showdown Is No Longer Just Fiction»
- «Russia warns Turkey over Aegean warship incident»
- «Iraq warns of attacks before Paris assault»

Использование уязвимостей нулевого дня

Использование 0day эксплойтов позволяет группировке решить две задачи, во-первых, увеличить свои шансы на успешную компрометацию системы, а во-вторых установить вредоносное ПО в автоматическим режиме с минимальным вмешательством пользователя.

Специалисты ESET обнаружили, что только в 2015 г. группировка использовала эксплуатировала не менее шести 0day уязвимостей для Windows, Adobe Flash и Java.



Кроме этого, как будет описано в последующих постах, группировка разработала десятки своих вредоносных программ, включая, бэкдоры с различными модулями, буткиты, и руткиты для успешного выполнения поставленных задач.

Полную версию анализа деятельности группировки Sednit можно найти по этой ссылке.