Статья Остановите серийного убийцу: Поймайте следующий удар

Когда мы смотрим на распространенное семейство вредоносных программ, мы отдаем должное его авторам за созданную вредоносную инфраструктуру. Новая вредоносная активность идет плавно, появляются командно-управляющие серверы, все работает как швейцарские часы. Есть ли у такой конструкции слабые места?

Чтобы ответить на этот вопрос, мы можем подумать о гоночной машине. Это шедевр, созданный для максимальной скорости, однако, чем больше у него скорости, тем меньше у него шансов сделать крутой поворот. Инфраструктура вредоносного ПО имеет такую же инерционную слабость. Когда каждый сустав работает нормально, у вас должна быть веская причина что-то в нем изменить.

Мы можем использовать это в своих интересах, как это делают кинодетективы. Возьмите карту города, отметьте места предыдущих преступлений — и вы, вероятно, поймете закономерность и даже получите вероятное место следующего преступления, оно, скорее всего, будет следовать установленному шаблону. В этом исследовании мы показываем, как преобразовать эти действия в мир вредоносных программ. Мы берем один из наиболее распространенных современных ботнетов под названием Dridex, отмечаем его предыдущие места преступлений, строим карту и делаем выводы, которые помогут нам поймать следующий удар. Мы показываем доказательства успеха такого подхода, выраженные точными цифрами, и объясняем, как использовать эту идею в других реальных случаях.

Введение

Банковский троян Dridex впервые появился в 2014 году и до сих пор остается одним из самых распространенных семейств вредоносных программ. В марте 2020 года Dridex возглавил список самых разыскиваемых вредоносных программ.

Dridex был создан киберпреступной группой под названием "Evil Corp", которая нанесла мировой банковской системе ущерб в размере 100 миллионов долларов. Было проведено много исследований, охватывающих различные аспекты деталей вредоносного ПО и того, как функционирует киберпреступная группа.

В этой статье мы приводим сводку основных деталей, известных на сегодняшний день о Dridex. Мы исследуем предысторию развития Dridex, дадим обзор и покажем его ключевые технические особенности и методы распространения. Мы объясняем, как

мы можем перехватить это вредоносное ПО на самых ранних этапах цепочки заражения. Мы также предоставляем графики, которые демонстрируют успех нашего подхода и то, как наши клиенты защищены от этого вредоносного ПО.

Происхождение

Дридекс имеет известное происхождение. Давайте сделаем шаг назад в историю, чтобы узнать больше о периоде времени, когда появилась его самая ранняя версия.

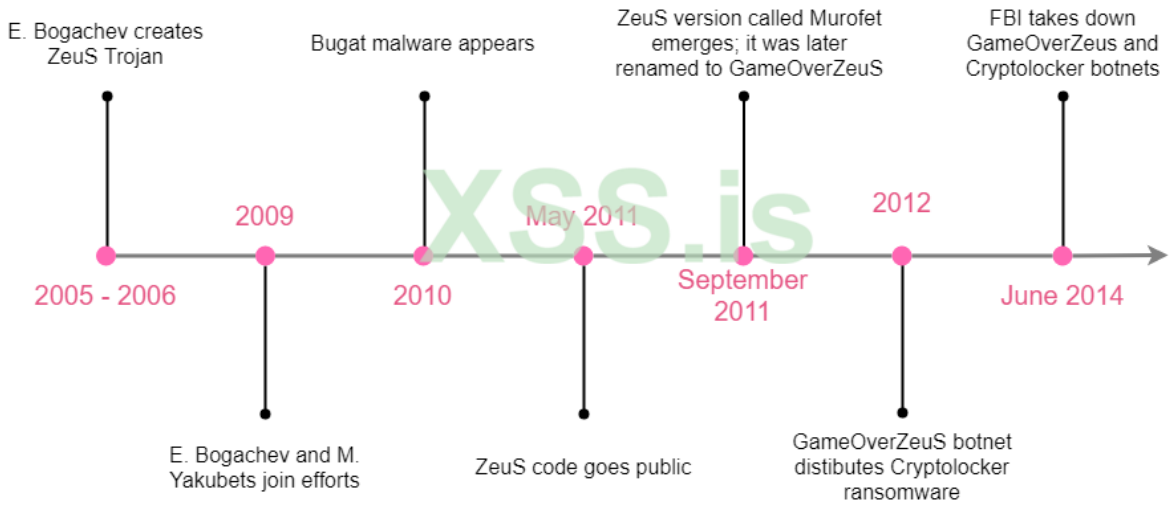
Ключевые имена в этой истории:

- Евгений Богачев — создатель печально известной вредоносной программы ZeuS.
- Максим Якубец — Предполагаемый лидер киберпреступной группировки Evil Corp, ответственной за деятельность Dridex.

Эра до Dridex - все начинается с ZeuS

Zeus - это вредоносный троянский конь. Его возможности включают превращение зараженной машины в узел ботнета, кражу банковских учетных данных, загрузку и выполнение отдельных вредоносных модулей. Согласно расследованию ФБР, члены киберпреступной группировки попытались украсть около 220 миллионов долларов США по всему миру, используя ZeuS.

На временной шкале ниже показаны ключевые моменты эволюции ZeuS:



Когда в 2011 году произошла утечка исходного кода ZeuS, начали появляться различные ответвления этого вредоносного ПО. Это было очень популярное вредоносное ПО, которое дало начало множеству различных ветвей вредоносного ПО. Версии ZeuS могут быть в онлайн-музее ZeuS. На момент написания этой статьи ZeuS был связан с 29 различными семействами вредоносных программ, насчитывающих в общей сложности около 490 версий.

В мае 2014 года ФБР выпустило бюллетень с описанием Евгения Богачева и обещанного вознаграждения в размере 3 миллионов долларов "за информацию, ведущую к аресту и/или осуждению".

WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

Эпоха Дридекс

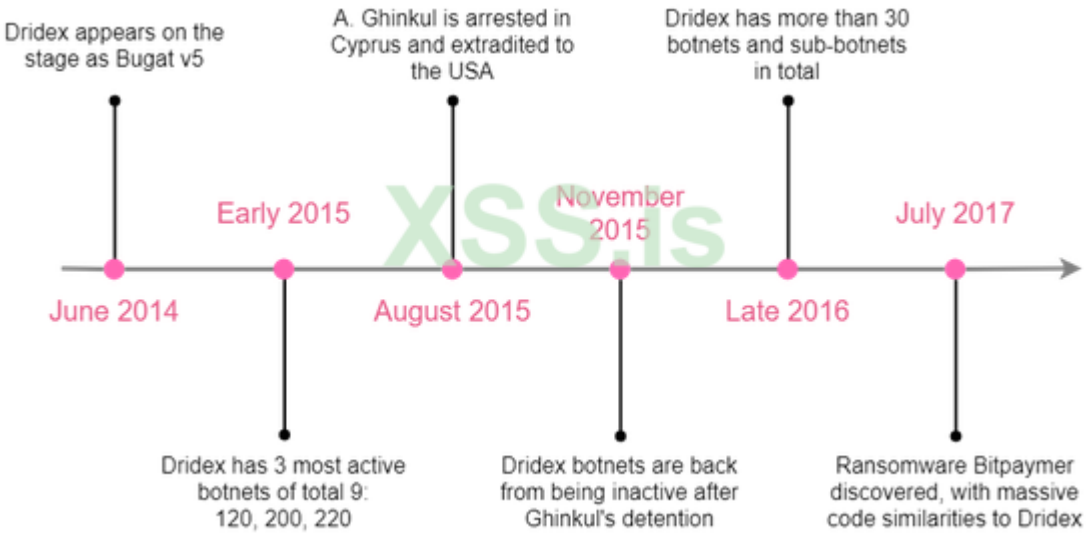
После того, как бот-сети прямых преемников ZeuS были отключены, пришло время Dridex. Эта вредоносная программа является результатом эволюции Bugat (появившейся в 2010 году). Bugat v5 был признан Dridex в 2014 году.

В это время на сцене появляется больше имен.

- Андрей Гинкул (из Молдовы) якобы был одним из администраторов ботнетов Dridex в 2015 году.
- Игорь Турашев якобы был одним из администраторов ботнета Dridex.
- Денис Гусев был одним из ключевых инвесторов EvilCorp.

Другие имена, связанные с Dridex, можно найти в заявлении о санкциях казначейства США.

На временной шкале ниже показаны некоторые вехи в развитии Dridex:



Dridex, в свою очередь, привел к появлению ряда программ-вымогателей, начиная с Bitpaymer в 2017 году. Эта ветка продолжилась с DoppelPaymer, который был разработан в 2019 году, и WastedLocker, который был разработан в 2020 году.

Недавнее прошлое

В 2019 году у Dridex было как минимум 14 активных ботнетов, некоторые из которых уже были замечены ранее, а другие были разработаны недавно. Ботнеты различаются по идентификатору. Это одни из самых активных на данный момент: 10111, 10222, 10444, 40200, 40300.

В конце 2019 года ФБР выпустило бюллетень с описанием автора Dridex и обещанным вознаграждением в размере 5 млн долларов США (по сравнению с 3 млн долларов США ранее для Е. Богачева).

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

Есть также свидетельства роскошного образа жизни Максима, несомненно, за счет доходов от его злонамеренных действий.

На сегодняшний день Максим Якубец не задержан правоохранительными органами.

Как упоминалось ранее, в 2020 году Dridex возглавил списки самых распространенных семейств вредоносных программ в мире.

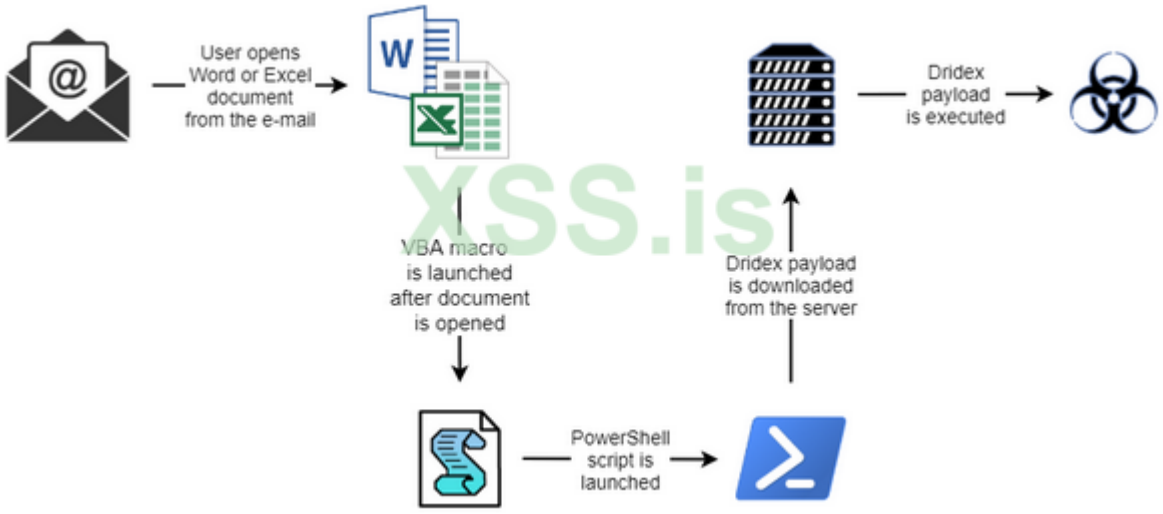
Цепочка заражения

Прежде чем мы начнем анализ самих образцов Dridex, мы хотим понять инфраструктуру, стоящую за вредоносным ПО. Как доставляется? Какие цели? Каков начальный уровень обнаружения вспомогательных файлов? Мы найдем ответы на все эти вопросы ниже.

Поток

Когда операторы хотят распространять Dridex, они используют спам-ботов от различных киберпреступных групп для рассылки вредоносных документов, прикрепленных к искусно созданным электронным письмам. В разные периоды жизненного цикла Dridex ботнеты Necurs, Cutwail и Andromeda участвовали в распространении Dridex.

Когда пользователь загружает и открывает такой документ (это может быть Word или Excel), запускаются встроенные макросы с целью загрузки и выполнения полезной нагрузки Dridex.



Цели

Dridex нацелен на различные известные организации из разных уголков мира:

- Банковские счета в США.
- Компании, выпускающие кредитные карты США.
- Финансовые инвестиционные корпорации США.
- Счета в европейских банках.
- Государственные агентства Саудовской Аравии, Катара, Омана.

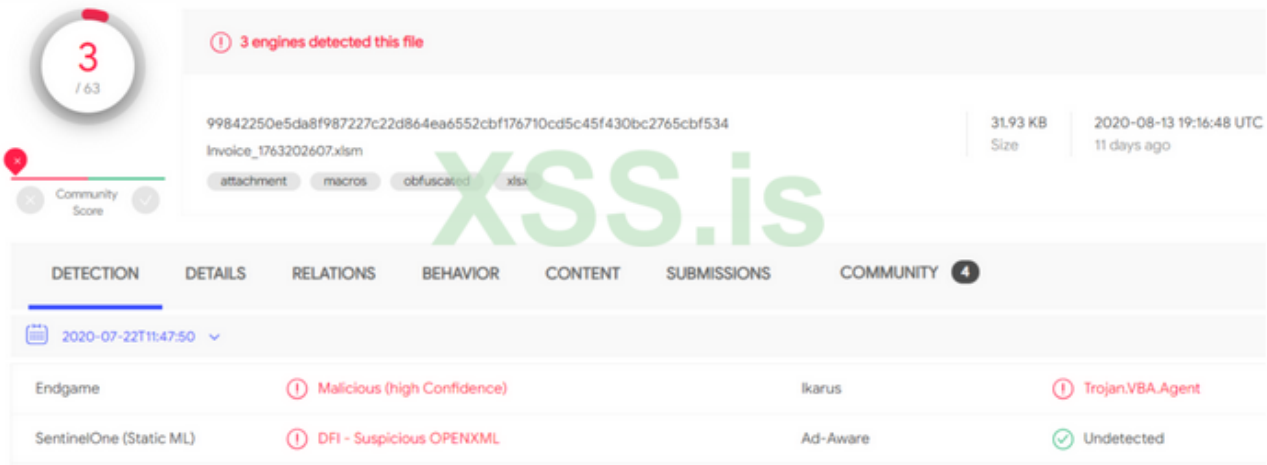
Приманки

Чтобы увеличить скорость распространения Dridex, злоумышленники маскируют свои спам-сообщения, чтобы они выглядели как законные. Мы можем назвать примеры UPS, FedEx и DHL как компаний, чьи логотипы и стиль рассылки используются в качестве приманки в таких электронных письмах.

При переходе по ссылке жертва открывает либо архив с вредоносным документом, либо сам вредоносный документ.

Начальная скорость обнаружения

При первом просмотре в дикой природе файлы доставки Dridex показывают очень низкий уровень обнаружения. На скриншоте ниже мы видим начальную скорость обнаружения документа Excel, который предоставляет Dridex:



То же самое и с другими файлами доставки.

Загрузчик и полезная нагрузка

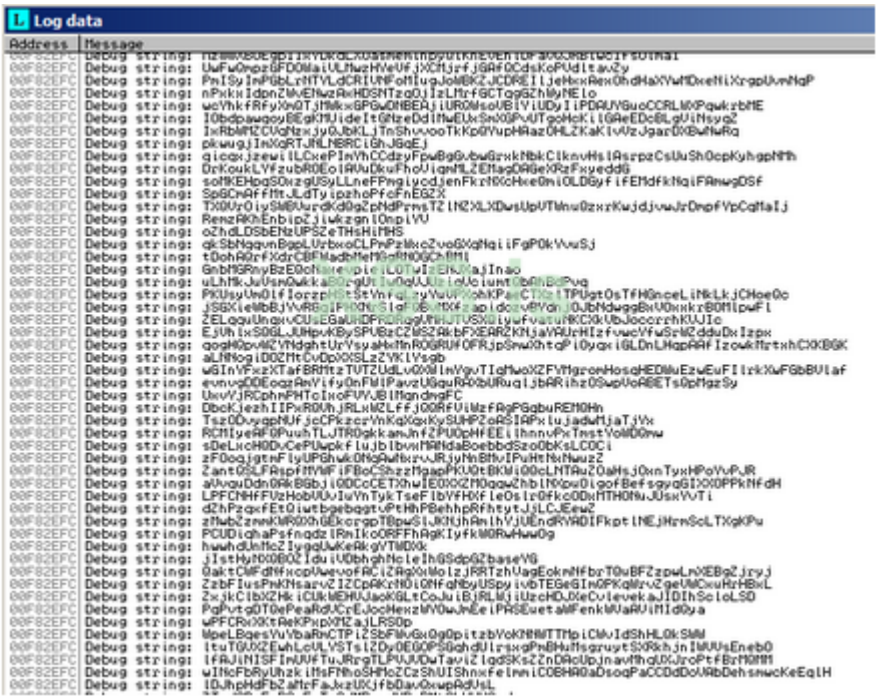
Пример Dridex состоит из загрузчика и полезной нагрузки. Ниже мы обсуждаем ключевые моменты каждой части.

Техника защиты от отладки

Загрузчик Dridex использует функцию OutputDebugStringW, чтобы затруднить анализ вредоносных программ. Разные загрузчики производят разные выходные данные (очень популярна строка "Установка..."), но идея везде одна и та же: создание длинного цикла, содержащего множество бессмысленных отладочных сообщений. На рисунке ниже мы видим пример такого цикла с итерацией около 200 миллионов:

```
00F82EE0    >  8BF7          mov esi,edi
00F82EE2    .  81FB 7B13000( cmp ebx,137B
00F82EE8    .- 7D 2B         jge short 00F82F15
00F82EEA    .  6A 50         push 50
00F82EEC    .  6A 14         push 14
00F82EEE    .  B2 03         mov dl,3
00F82EF0    .  8D4D F8       lea ecx,[ebp-8]
00F82EF3    .  E8 883E0100   call 00F96D80
00F82EF8    .  8B45 F8       mov eax,dword ptr ss:[ebp-8]
00F82EFB       50            push eax
00F82EFC       FF15 0010FA0( call dword ptr ds:[<&KERNEL32.OutputDebu
00F82F02       6A 0A         push 0A
00F82F04       FF15 0810FA0( call dword ptr ds:[<&KERNEL32.Sleep>]
00F82F0A    .  8D4D F8       lea ecx,[ebp-8]
00F82F0D    .  8D77 FF       lea esi,[edi-1]
00F82F10    .  E8 0B250100   call 00F95420
00F82F15    >  43            inc ebx
00F82F16    .  81FB 7CBEEB0( cmp ebx,0BEBBE7C
00F82F1C    .- 7C C2         jl short 00F82EE0
```

Результат в журнале выглядит так:



Обфускация

Полезная нагрузка сильно запутана; почти никакая функция не вызывается напрямую. Разрешение вызовов выполняется с помощью хэш-значений, идентифицирующих библиотеку и содержащуюся в ней функцию. Пример такого разрешения показан на скриншоте ниже:

```
01D061CA loc_1D061CA:
01D061CA mov     ecx, 302DE090h
01D061CF mov     edx, 0F4CD7A7Ch
01D061D4 mov     ebp, [esp+2Ch+var_1C]
01D061D8 call    resolve_func    ; CryptHashData
01D061D8
01D061DD test    eax, eax
01D061DF jz      loc_1D062C3
```

Так называются все функции, важные для ключевых задач Dridex.

```
      p  prepare_connection+97      call  resolve_func; InternetOpenA
D...  p  InternetCloseHandle+D      call  resolve_func; InternetCloseHandle
D...  p  connect_to_host+E8         call  resolve_func; InternetConnectW
D...  p  connect_to_host+19C        call  resolve_func; HttpOpenRequestW
D...  p  connect_to_host+27F        call  resolve_func; InternetSetOptionW
D...  p  connect_to_host+2A1        call  resolve_func; InternetSetOptionW
D...  p  connect_to_host+2C8        call  resolve_func; InternetQueryOptionW
D...  p  connect_to_host+2F7        call  resolve_func; InternetSetOptionW
```

Мы использовали инструмент Labeless для устранения запутанных вызовов функций.

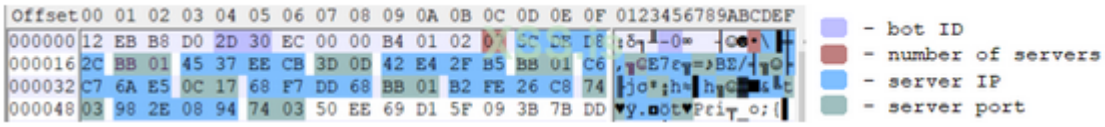
Строки в вредоносной программе запутываются с помощью алгоритма RC4 и ключа дешифрования, хранящегося внутри образца.

Конфигурация

Главный интерес внутри полезной нагрузки - это ее конфигурация. Он содержит следующие важные детали:

- ID бота.
- Количество C&C серверов.
- Список самих C&C серверов.

Пример конфигурации:

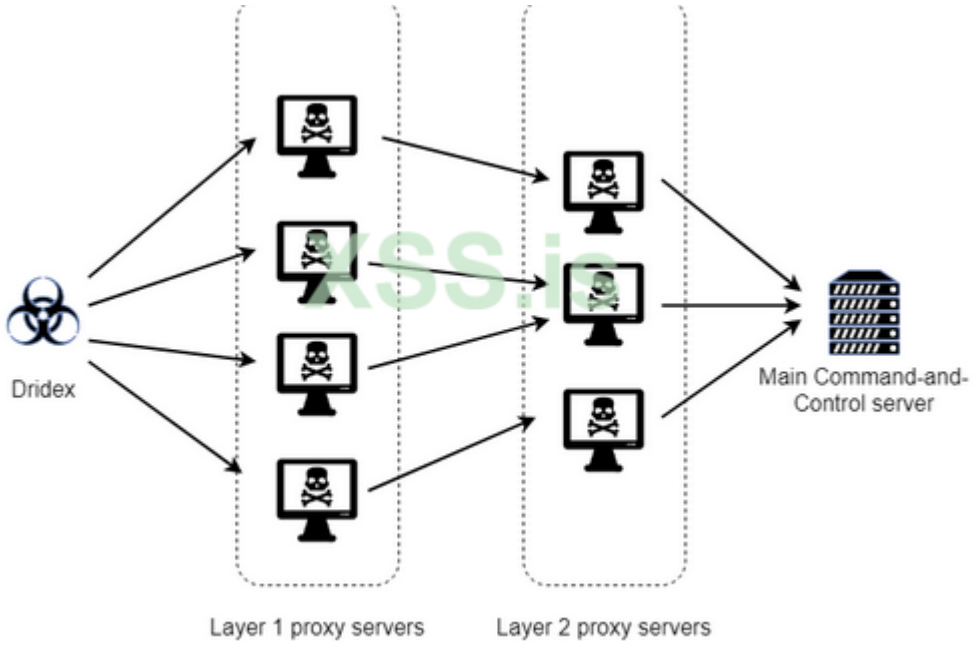


Идентификатор бота в этом примере - 12333. Серверы управления и контроля:

- 92.222.216.44:443
- 69.55.238.203:3389
- 66.228.47.181:443
- 198.199.106.229:5900
- 104.247.221.104:443
- 178.254.38.200:884
- 152.46.8.148:884

Сетевая активность

Dridex отправляет запросы POST на серверы из конфигурации для получения дальнейших команд, ожидая ответов 200 OK. Обратите внимание, что эти серверы не настоящие C&C серверы, а скорее прокси для подключения к реальным.



Информация, отправляемая вредоносным ПО на управляющие серверы, содержит следующие данные:

- Имя компьютера
- ID-номер ботнета
- Тип запроса
- Архитектура ОС
- Список установленного ПО

Эти данные шифруются с помощью алгоритма RC4, ключ которого хранится среди зашифрованных строк внутри вредоносной программы.

Есть как минимум 6 различных типов запросов; Среди них следующие:

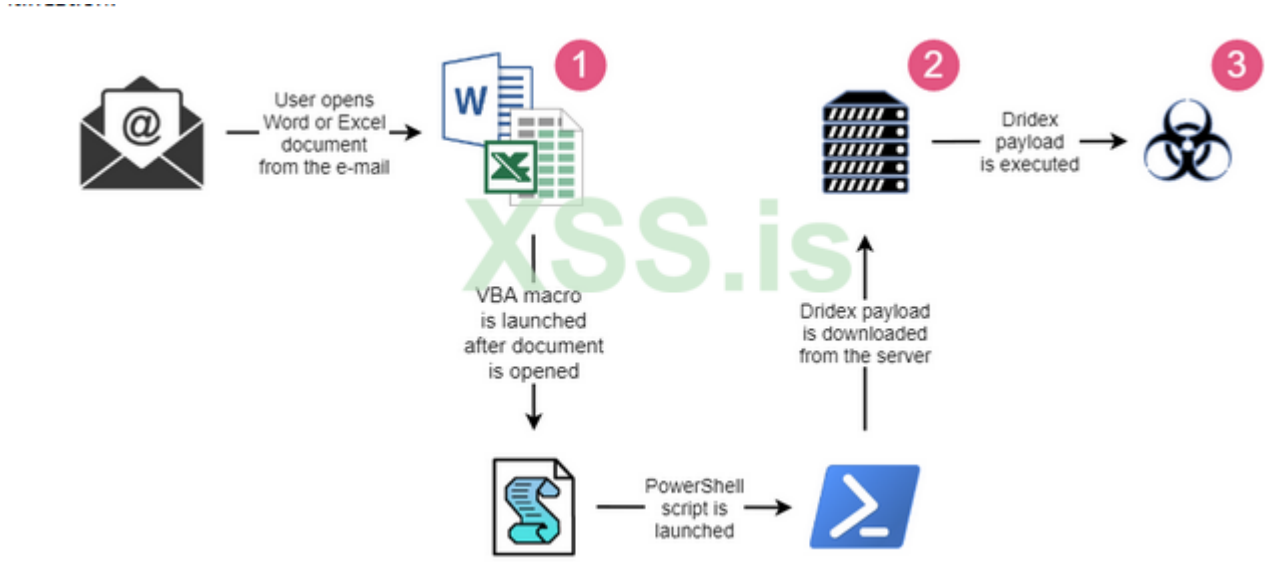
- "список" - получает конфигурацию
- "бот" - получает модуль бота

Собираем IOC вместе

Чем раньше будет обнаружена инфекция, тем выше шансы на ее защиту. Чтобы как можно быстрее заразиться инфекцией, затратив минимум ресурсов, мы хотим сосредоточиться на начальной стадии доставки.

Однако обнаружение - это только один аспект. Мы можем с уверенностью сказать, что это что-то вредоносное, но мы также хотим классифицировать угрозу. Для этого мы должны быть уверены, что это вредоносное ПО действительно Dridex.

Давайте еще раз взглянем на цепочку заражения Dridex и определим различные этапы, которые мы можем использовать для ее обнаружения и идентификации:



На разных стадиях заражения Dridex мы можем использовать следующие индикаторы для его обнаружения.

- 1-й этап, вредоносные документы:
Хэши документов
Изображения внутри документов
Внутренняя структура документа
Макросы, используемые внутри
- 2 этап, серверы:
Домены
URL-адреса

- 3 ступень, погрузчики и полезные нагрузки:
Хеши образцов
IP-адреса в файле конфигурации

Почему так много факторов важно?

Мы увидели корреляцию между инфраструктурами и индикаторами Dridex и других распространенных семейств вредоносных программ, таких как Emotet и Ursnif. Вредоносные документы имеют общие индикаторы при использовании для доставки всех упомянутых выше вредоносных программ. Некоторые серверы C2, а точнее прокси-серверы, используются как Dridex, так и Emotet, хотя порты и типы подключения различаются.

Вот почему мы должны проанализировать множество деталей, прежде чем делать вывод о том, с какими вредоносными программами мы имеем дело. Чем больше уникальных факторов связано с конкретным ботнетом, тем легче сказать, имеет ли другая атака те же шаблоны.

Идеальный способ классификации вредоносных программ - это, конечно, получение и анализ конечной полезной нагрузки: если это Dridex, то все, что было запущено до того, как оно было классифицировано как Dridex. Однако может пройти некоторое время (иногда значительное время после получения исходного вредоносного документа), прежде чем станет известен результат. Мы можем провести классификацию быстрее и с высокой степенью уверенности, проанализировав все показатели, которые мы получаем на самых ранних этапах цепочки заражения.

IP-адреса для рисования карты

Еще одно интересное замечание - использование той же сети для загрузки образцов Dridex. Мы проанализировали домены, используемые для этой цели, разрешили их IP-адреса и обнаружили, что довольно много из них находятся в одной сети 84.38.180.0/22, а всего доступно менее 1024 адресов. Сеть принадлежит российской ASN Selectel, которая редко удаляет вредоносный контент или спам.

Мы видели следующие IP-адреса, связанные с доменами Dridex в сети 84.38.180.0/22 (и других сетях в том же ASN). Даты показывают, когда домен Dridex впервые указал на соответствующие IP-адреса:

IPs	Date	Domains
84.38.182.248	May 10	rokadorc.com nrokadorc.com

84.38.183.77	June 17	juneusdousigninc.com usdousigninc.com
84.38.182.236 84.38.183.213	June 22	marutoba.com terrasimonad.com enterassimonad.com
84.38.181.195	June 28	caranatrium.com
84.38.183.114 84.38.183.237	July 06	menodlap.com turendong.com madustag.com

Хотя одного этого фактора недостаточно для идентификации Dridex, это хорошая вспомогательная деталь, на которую следует ссылаться при работе с IOC Dridex.

Обнаружение

На графиках ниже показаны всплески Dridex в разные даты, когда мы отлавливали входящие угрозы на самых ранних этапах.

Крайне важно уметь как можно раньше перехватить инфекцию Dridex. Во многих случаях, если спам не рассылается в течение нескольких дней подряд, как это было в период с 6 по 8 июля, активность ботнета замедляется на следующий день, и мы не получаем столько совпадений IOC, сколько во время его пика. Учитывая, что новые заражения появляются примерно во второй половине дня по всемирному координированному времени + 3, у нас меньше 12 часов, чтобы отреагировать на входящую угрозу.

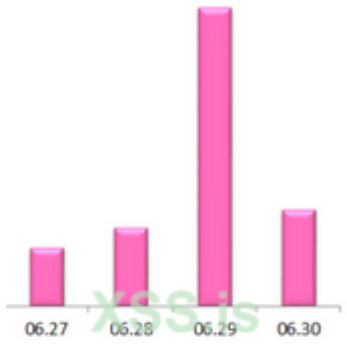
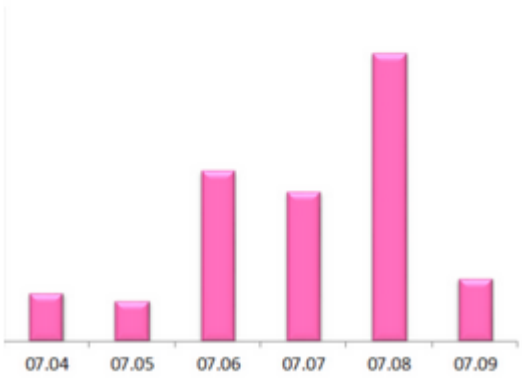


Figure 16 – Dridex infection spike on June 29.



Разработка Dridex

С 22 июля мы не наблюдаем свежих образцов спама от Dridex. 7 сентября компания Dridex снова появилась, показав резкий рост активности в течение 2 дней подряд:

Операторы Dridex обновили 1-й этап выполнения Dridex: они добавили больше URL-адресов, откуда может быть загружена полезная нагрузка, в отличие от одного URL-адреса в самых ранних версиях вредоносных документов. Теперь их количество может достигать 50 в одном документе.

Мы постоянно отслеживаем этот ботнет и обнаруживаем его полезную нагрузку на разных этапах выполнения.

Мы надеемся, что эта публикация предоставила полезные сведения о различных вариантах и методах борьбы с этой угрозой. Мы также считаем, что эти методы могут быть применены и при столкновении с другими угрозами.

По мере того как кибератаки становятся все более уклончивыми, добавляются дополнительные средства контроля, что делает безопасность более сложной и утомительной до такой степени, что это влияет на рабочие процессы пользователей. До настоящего времени.

Опираясь на мощь ThreatCloud, самую мощную аналитику угроз и технологии ИИ для предотвращения неизвестных киберугроз SandBlast Network обеспечивает лучшую защиту нулевого дня, снижая при этом накладные расходы на безопасность и обеспечивая продуктивность бизнеса.

Источник: https://research.checkpoint.com/2021/stopping-serial-killer-catching-the-next-strike/
Автор перевода: yashechka
Переведено специально для https://xss.is