Самораспространение вредоносного программного обеспечения в локальной сети

Андрей Жданов

Аннотация

В статье рассказывается о способах самораспространения вредоносного программного обеспечения (ВПО) в локальной сети. Автор отмечает, что в настоящее время использование функционала самораспространения в ВПО потеряло свою актуальность. Сейчас для самораспространения гарантированно можно использовать только легитимные механизмы — создание групповой политики, использование общих административных сетевых ресурсов (Admin Shares) и использование общих ресурсов для самораспространения. Автор приводит примеры применения этих техник, а также даёт рекомендации по защите сетей и устройств от самораспространяемого ВПО.

Ключевые слова:

ВПО, вредоносное программное обеспечение, вирус, червь, летигимные механизмы.

Первым знаменитым образцом вредоносной программы, использующей механизм самораспространения в сети, стал в 1988 году сетевой червь Морриса. Червь назван по имени его автора — аспиранта Корнельского университета Роберта Таппана Морриса (Robert Tappan Morris). По словам автора, червь был написан в исследовательских целях, однако наличие ошибок в его исходном коде привело к массовому заражению компьютеров в сети ARPANET, которая в то время была предшественником современного Интернета. В результате червём была парализована работа нескольких тысяч компьютеров, а общий ущерб был оценен в 98 миллионов долларов.

Основы теории механизмов самовоспроизведения заложил еще в 1951 году американский математик и физик Джон фон Нейман (John von Neumann). Поэтому неудивительно, что именно вирусы и черви стали первыми образцами вредоносного программного обеспечения (ВПО).

Вирусы внедряют свой код в различные объекты, в которых он может выполняться и продолжать своё распространение дальше. Такими объектами могут быть, например, исполняемые файлы, скрипты, исходный код, загрузочные секторы и т.п. При этом код вируса может видоизменяться (полиморфные вирусы). Черви же, в отличие от вирусов, не внедряют свой код для самораспространения, а создают свои копии,

которые также могут различаться между собой. Черви, использующие сеть для распространения, относят к сетевым. Вирусы и черви объединяют под понятием вирусное ВПО.

Одно из официальных определений ВПО в соответствии с ГОСТ Р 53113.1-2008 (https://bdu.fstec.ru/ubi/terms/terms/view/id/12):

Вредоносная программа (программное обеспечение) — программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа и/или деструктивного воздействия на информацию или ресурсы информационной системы, нарушение их целостности и/или доступности.

Поначалу вредоносные программы преимущественно разрабатывались из хулиганских побуждений, они могли в процессе своего функционирования производить изощрённые звуковые и видеоэффекты, но были и вирусы-вандалы, которые уничтожали данные и даже могли вывести из строя компьютер (вирус CIH/Чернобыль) Со временем доля вирусов и червей в ВПО становилась всё меньше и меньше, львиную часть стали составлять троянские программы. По аналогии с «Троянским конём», троянскими программами считают вредоносные программы, маскирующиеся под легитимные и полезные. В зависимости от их целей троянские программы разделяют на бэкдоры, шпионские программы, программы-вымогатели и т.п. Однако до сих пор по традиции двадцатилетней давности многие называют вирусами все вредоносные программы без разбора.

Массовое распространение вирусов и червей приводило к масштабным эпидемиям. Примеры наиболее громких и знаковых эпидемий с использованием сетевых червей:

- в 2000 году — ILOVEYOU (LoveLetter) (https://www.theregister.com/2020/05/05/iloveyou_20_years/);
- в 2001 году — Code Red (https://www.kaspersky.ru/blog/history-lessons-code-red/33795/);
- в 2003 году — Slammer (Sapphire) (https://threatpost.com/inside-story-sql-slammer-102010/74589/);
- в 2004 году — Mydoom (https://yourstory.com/2025/01/worst-computer-virus-time-digital-plague-spreading);
- в 2007 году — Storm (https://www.schneier.com/blog/archives/2007/10/the_storm_worm.html);
- в 2008 году — Conficker (Kido) (https://www.anti-malware.ru/news/2020-09-15-111332/33688);
- в 2010 году — Stuxnet, который стал первым известным образцом кибероружия (http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/20230411161526_0531.pdf).

В апреле 2017 года хакерская группировка «The Shadow Brokers» опубликовала материалы под названием «Lost in Translation», в которых содержались инструменты Equation Group, которую связывают с Агентством национальной безопасности США (АНБ) (https://research.checkpoint.com/2020/nazar-spirits-of-the-past/). В составе фреймворка FuzzBunch содержался набор эксплойтов для уязвимостей нулевого дня [1] и бэкдоров [2]. Наиболее печально известными из них стали эксплойт EternalBlue и бэкдор DoublePulsar. Спустя месяц, в мае 2017 года, инструментами из публикации «The Shadow Brokers» воспользовалась группировка неизвестной принадлежности, создавшая программу-вымогатель WannaCry (WanaCryptor), которая, по сути, представляла собой сетевой червь (https://www.kaspersky.ru/blog/wannacry-hsitory-lessons/33853/). Для доставки непосредственно программы-вымогателя на компьютеры локальной сети червь использовал уязвимость Microsoft Server Message Block 1.0 (SMBv1) CVE-2017-0145 (MS17-010), которую реализовал эксплойт EternalBlue. В результате успешной эксплуатации в качестве полезной нагрузки на целевой компьютер загружался бэкдор DoublePulsar. А уже с помощью установленного бэкдора на компьютер загружалась непосредственно программа-вымогатель WannaCry и далее осуществлялось шифрование данных на компьютере. За расшифровку вымогатели требовали всего 300 долларов США в криптовалюте. Общий же ущерб от эпидемии составил по различным оценкам не менее 4 миллиардов долларов США. А в июне 2017 года произошла эпидемия вайпера NotPetya, использовавшего те же инструменты АНБ.

До сих пор различное ВПО, преимущественно связанное с криптоджекингом* и вымогательством, использует связку эксплойта EternalBlue и бэкдора DoublePulsar для распространения своих модулей в уязвимой сетевой инфраструктуре.

В настоящее время можно с уверенностью говорить о закате эры вирусов и червей, если, конечно, у кого-то вдруг снова не окажется в рукаве козырного туза в виде новой разрушительной уязвимости нулевого дня, что выльется в очередную эпидемию. Но ВПО сейчас стало криминальным бизнесом, поэтому кажутся маловероятными подобные публикации в будущем. Цена таких эксплойтов на чёрном рынке достигает миллионов долларов, и никто не будет разбрасываться ими просто так. Да и спецслужбы провели работу над ошибками, чтобы избегать таких утечек.

Надобность в бесконтрольном самораспространении ВПО со временем отпала, как, впрочем, и в многофункциональных вредоносных мегакомбайнах. Атакующие сейчас используют для разведки сети и распространения в сетевой инфраструктуре жертвы отдельные специализированные инструменты, а серьёзные вредоносные программы имеют модульную структуру и выполняют свои конкретные задачи. Также стоит учесть, что избыточные функциональные возможности могут демаскировать ВПО (например, бэкдор или шпионскую программу) в скомпрометированной системе.

Среди ВПО программы-вымогатели — это отдельная история. В случае WannaCry и NotPetya использование уязвимости SMBv1 для самораспространения позволило осуществить массовое шифрование/уничтожение данных без непосред-

* Криптоджекинг — использование компьютера для добычи криптовалюты, часто через веб-сайты, против воли пользователя или без его ведома.

ственного участия атакующих. Сейчас же в атаках программы-вымогатели размещаются в инфраструктуре жертвы и запускаются на самом последнем этапе атаки, когда атакующими уже получен полный контроль над инфраструктурой жертвы: выгружена на ресурсы злоумышленников конфиденциальная информация жертвы и нейтрализованы защитные средства, в том числе и антивирусное ПО. При этом нередко атакующие используют само антивирусное ПО для распространения в локальной сети своих инструментов. В этом случае функция самораспространения в программах-вымогателях может быть полезна с точки зрения наибольшего охвата данных для шифрования с целью нанесения максимального ущерба жертве, причём эти действия произведутся автономно, без непосредственного участия злоумышленников.

Реализация функции самораспространения является весьма непростой задачей. При отсутствии уязвимостей, подобных SMBv1, необходимо применять легитимные механизмы, а для них требуется наличие корректных доменных учётных записей. Учётные данные могут быть получены атакующими на предыдущих этапах атаки или подобраны самой вредоносной программой в результате перебора.

Программы-вымогатели с подобным функционалом можно пересчитать по пальцам, в основном они разрабатывались крупными «солидными» партнёрскими программами (RaaS, Ransomware-as-a-Service), не скупящимися на разработку и поддержание своего имиджа. В качестве примера можно привести такие известные шифровальщики, как LockBit 3.0 (Black), BlackCat и Qilin.

Как уже сказано выше, доля вирусов и червей в ВПО сейчас мала, также невелико и число программ-вымогателей, имеющих функционал самораспространения, да и он имеет уже второстепенное значение. Поэтому употребление в обиходе термина «вирус-шифровальщик», как и «вирусы» в отношении всего ВПО, совершенно некорректно, это так же неверно, как в биологии называть вирусами все патогенные микробы.

Итак, на вооружении разработчиков ВПО остались легитимные техники самораспространения, если не брать в расчёт уязвимости наподобие SMBv1. Далее речь пойдёт о Windows-системах, но это не означает, что в Linux-системах нельзя реализовать самораспространение, например, с помощью таких сервисов, как SSH (Secure Shell) и SFTP (Secure File Transfer Protocol). Всё же на практике чаще всего применяется самораспространение в ВПО, разработанном для Windows-платформ.

Такими популярными техниками самораспространения в локальной сети в Windows-системах являются создание групповой политики и использование общих административных сетевых ресурсов (Admin Shares). В активно используемой против российских компаний программе-вымогателе LockBit 3.0 (Black) реализованы обе техники.

Создание групповой политики

Данную технику мы рассмотрим на примере известной программы-вымогателя — LockBit 2.0, в которой одной из первой была реализована эта техника. Впоследствии другие программы-вымогатели заимствовали эту реализацию из LockBit 2.0.

В случае, если программа-вымогатель запущена с администраторскими правами на контроллере домена, программа с помощью групповой политики предоставляет общий доступ к дискам хостов, останавливает службы и завершает процессы на хостах, а также осуществляет своё распространение в локальной сети.

Для этого вредоносная программа создаёт в корневом каталоге Group Policy Object (GPO) на контроллере домена структуру каталогов и файлов, определяющих новую групповую политику:

<GPO_GUID>\GPT.ini

<GPO_GUID>\Machine\Preferences\NetworkShares\NetworkShares.xml

<GPO_GUID>\Machine\Preferences\Services\Services.xml

<GPO_GUID>\Machine\comment.cmtx

<GPO_GUID>\Machine\Registry.pol

<GPO_GUID>\User\Preferences\Files\Files.xml

<GPO_GUID>\User\Preferences\ScheduledTasks\ScheduledTasks.xml

GPO_GUID — GUID новой групповой политики

NetworkShares.xml предназначен для предоставления общего доступа к дискам хостов домена с целью доступа программы-вымогателя к большему количеству файлов в сети жертвы для их шифрования.

Services.xml предназначен для остановки и запрета системных служб на хостах домена, связанных в основном с системами управления базами данных (рис. 1).

Файлы **Registry.pol** и **comment.cmtx** предназначены для отключения Windows Defender на хостах путём модификации соответствующих параметров системного реестра.

Программа-вымогатель копирует свой исполняемый файл в каталог общедоступных файлов **Active Directory SYSVOL**:

\\< DNS_DOMAIN_NAME>\sysvol\< DNS_DOMAIN_ NAME>\scripts\

DNS_DOMAIN_ NAME — имя домена DNS.

Files.xml предназначен для копирования файла программы-вымогателя из каталога общедоступных файлов Active Directory SYSVOL в каталог на хосте.

ScheduledTasks.xml предназначен для создания на хосте задач планировщика. Одна задача планировщика завершает определённые процессы на хостах домена, вторая же про-

```
<?xml version="1.0" encoding="utf-8"?>
<NTServices clsid="{2CFB484A-4E96-4b5d-A0B6-093D2F91E6AE}">
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLPBDMS" image="4"
  changed="2023-01-23 18:21:25" uid="{3945152F-3312-4CCE-92EE-C28F8437C16D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLPBDMS" serviceAction="STOP" timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLPBENGINE" image="4"
  changed="2023-01-23 18:21:25" uid="{196B0DD4-BFD3-4BDF-87DF-040A0F56A12D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLPBENGINE" serviceAction="STOP" timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="MSSQLFDLauncher" image="4"
  changed="2023-01-23 18:21:25" uid="{37238E24-B477-4F07-AFA8-B919C215ECAC}" userContext="0"
  removePolicy="0" disabled="0">
    <Properties startupType="DISABLED" serviceName="MSSQLFDLauncher" serviceAction="STOP"
    timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLSERVERAGENT" image="4"
  changed="2023-01-23 18:21:25" uid="{09458DFA-77DE-4B07-9D90-40C391EEE14D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLSERVERAGENT" serviceAction="STOP"
    timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="MSSQLServerOLAPService" image="4"
  changed="2023-01-23 18:21:25" uid="{77B4ED31-EEDA-4F4B-87FA-FBC1734F6B45}" disabled="0">
    <Properties startupType="DISABLED" serviceName="MSSQLServerOLAPService" serviceAction="STOP"
    timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SSASTELEMETRY" image="4"
  changed="2023-01-23 18:21:25" uid="{F6E00BAB-91EF-46B9-BBD0-B2183F09AF12}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SSASTELEMETRY" serviceAction="STOP"
    timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLBrowser" image="4"
```

Рис.1. Начальный фрагмент Services.xml (пример).

изводит вызов исполняемого файла программы-вымогателя, содержащегося в локальном каталоге хоста. Аргументы командной строки программы для задачи формируются на основе аргументов запущенной программы-вымогателя. Задачи планировщика запускаются сразу после их создания.

Обновление же групповых политик на компьютерах домена осуществляется с помощью запуска следующей команды PowerShell:

```
powershell.exe -Command «Get-ADComputer -filter * -Searchbase 'AD_SEARCHPATH' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}»
```

AD_SEARCHPATH — путь AD для поиска:

```
DC=<DC1>,DC=<DC2>
```

DC1, DC2 — компоненты домена (domain components).

Для самораспространения с помощью данной техники программа-вымогатель LockBit 3 (Black) может быть запущена на любом компьютере домена, но должна содержать в своих конфигурационных данных корректные доменные учётные записи.

Использование общих административных сетевых ресурсов (Admin Shares)

Эта техника реализована в популярной легитимной утилите PsExec из набора утилит PsTools Sysinternals компании Microsoft, предназначенной для выполнения команд в удалённых системах (https://learn.microsoft.com/en-us/sysinternals/downloads/psexec). В программах-вымогателях BlackCat и Qilin не стали изобретать велосипед и просто поместили непосредственно утилиту PsExec в код программы-вымогателя.

Так, программа-вымогатель Qilin при самораспространении извлекает в каталог %Temp% под случайным именем утилиту PsExec и запускает её для каждого найденного компьютера текущего домена следующим образом:

```
%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process
```

Если в конфигурационных данных Qilin указаны полученные злоумышленниками на предыдущих этапах атаки учётные

данные (accounts), то запуск утилиты PsExec осуществляется с указанием имени пользователя и пароля:

```
%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -u <USER_NAME> -p <PASSWORD> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process
```

Где **PSEXEC_NAME** — сгенерированное имя утилиты PsExec;

HOST_IP — IP-адрес хоста;
USER_NAME — имя пользователя;
PASSWORD — пароль;
LOCKER_PATH — путь к программе-вымогателю;
LOCKER_ARGS — аргументы командной строки, заданные при запуске программы-вымогателя.

Для получения списка хостов домена Qilin предварительно запускает следующий скрипт PowerShell:

```
«powershell» -Command «Import-Module ActiveDirectory ; Get-ADComputer -Filter * | Select-Object -ExpandProperty DNSHostName»
```

В LockBit 3.0 (Blacks) техника реализована разработчиком самостоятельно, а опция в конфигурационных данных, включающая этот механизм, имеет характерное название — «psexec_netspread». Для самораспространения необходимо в конфигурации включить эту опцию и указать корректные администраторские учётные данные. Программа-вымогатель определяет имя домена и осуществляет перебор учётных записей, указанных в конфигурации, и производит попытку аутентификации для каждой записи с помощью функции API LogonUserW. Если такая учётная запись найдена, программа запускает свой исполняемый файл в контексте безопасности этой учётной записи с помощью CreateProcessAsUserW или CreateProcessWithLogonW, при этом при запуске добавляет параметр командной строки «-psex». Для взаимодействия между процессами LockBit 3.0 (Black) используются каналы IPC (Inter-Process Communication) в виде именованных пайпов (pipe).

Вредоносная программа получает список хостов для самораспространения: перечисляет контроллеры домена с помощью функций API DsGetDcOpenW / DsGetDcNextW и компьютеры Active Directory с помощью запросов LDAP. Для перечисления компьютеров используются функции API ADsOpenObject, ADsBuildEnumerator, ADsEnumerateNext и интерфейсы IADs, IADsContainer.

Далее для каждого хоста из полученного списка хостов создаётся поток, в функцию потока передаётся имя целевого хоста в виде:

```
\\<COMP_NAME>.<DOMAIN_NAME>\
```

COMP_NAME — имя компьютера, DOMAIN_NAME — имя домена.

В каждом потоке с помощью функции API WNetAddConnection2W осуществляется подключение к административным сетевым ресурсам компьютера (Admin Shares) ADMIN$ и IPC$. Подключение к ресурсу IPC$ позволяет осуществлять удалённое взаимодействие между процессами LockBit.

Программа-вымогатель создаёт на другом компьютере каталог «\\<COMP_NAME>.<DOMAIN_NAME>\ADMIN$\Temp» и копирует в него свой исполняемый файл.

Далее на компьютере удалённо создаётся и запускается служба, для которой используется скопированный на компьютер исполняемый файл программы-вымогателя со следующими аргументами командной строки:

```
%%SystemRoot%%\Temp\<APP_NAME>.exe -k LocalServiceNetworkRestricted
```

APP_NAME — имя скопированной на компьютер программы-вымогателя.

Далее при запуске в качестве службы программа-вымогатель запускает на компьютере себя с первоначальными аргументами командной строки, загруженными через IPC канал. При выполнении на компьютере вредоносная программа повторяет описанные выше действия для распространения далее, а затем осуществляет шифрование данных на этом компьютере.

Использование общих ресурсов для самораспространения

Эта техника не в полной мере является техникой самораспространения, так как подразумевает соответствующие действия пользователя. Но и не упомянуть о ней было бы несправедливым.

Данная техника эффективна с точки зрения ВПО в организациях, чрезмерно злоупотребляющих общими сетевыми ресурсами для централизованного хранения электронных документов.

В качестве примера реализации техники можно привести атаки группировки RedCurl. Бэкдоры RedCurl имеют модульную архитектуру, за реализацию указанной техники отвечает отдельный вредоносный модуль. Этот модуль создаёт на доступном общем сетевом ресурсе файл-ярлык под именем уже существующего файла-документа и с соответствующей иконкой. В тот же каталог с файлом-ярлыком помещается tmp-файл, представляющий собой программу-контейнер (дроппер) RedCurl. При удалённом открытии пользователем файла-ярлыка, мимикрирующего под файл-документ, осуществляется инфицирование компьютера этого пользователя с помощью такой команды:

```
shell32.dll,Control_RunDLL .\349a1c90-8151-4ad6-936d-0263f47a9356.tmp file=12.pdf
```

При этом также открывается и сам документ-приманка.

Дополнительным неожиданным эффектом в одном из случаев из нашей практики была передача архива с документами с общего сетевого ресурса скомпромети-

рованного подрядчика в родительскую компанию и её дальнейшая компрометация.

Заключение

История ВПО началась с вирусов и червей, однако в настоящее время использование функционала самораспространения в ВПО потеряло свою актуальность. Сейчас для самораспространения гарантированно можно использовать только легитимные механизмы, однако они требуют наличия привилегированных учётных записей. Выявление универсальных уязвимостей, позволяющих ВПО самостоятельно распространяться, а также публикация к ним эксплойтов в ближайшем будущем маловероятны.

Распространение в сетевой инфраструктуре жертвы осуществляется атакующими после разведки сети и сбора необходимых учётных данных с помощью специализированных инструментов. Все эти действия требуют от атакующих высокой квалификации.

Использование в ВПО механизмов самораспространения ограничено, и целесообразность его применения связана с классом ВПО.

Рекомендации

1. Регулярно осуществлять установку критических обновлений операционной системы и используемых программных продуктов.
2. Настроить стойкие парольные политики для локальных и доменных учётных записей. Убедиться в использовании различных паролей для локальных администраторов на всех хостах инфраструктуры.
3. При разграничении прав доступа руководствоваться принципом минимально необходимых привилегий в системе, уделяя особое внимание сервисным учётным записям, а также учётным записям, используемым для выполнения автоматизированных задач и удалённого доступа.
4. Запретить прямой доступ по протоколу RDP к рабочим станциям и серверам из-за пределов внутренней сети.
5. Обеспечить надёжную защиту средств удалённого доступа в IT-инфраструктуру, в том числе с помощью мультифакторной аутентификации.
6. Ограничить возможность использования личных устройств сотрудников для доступа в корпоративную сеть, в том числе через VPN.
7. Обеспечить глубину хранения журналов событий операционной системы и средств защиты информации не менее 3 месяцев.
8. Настроить расширенный сбор Windows- и Linux-событий, связанных с безопасностью.
9. Реализовать централизованный сбор событий в инфраструктуре и их передачу в систему сбора данных (например: стек ELK, SIEM).
10. Использовать для защиты конечных устройств решение MXDR.

Ссылки:

[1] https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня

[2] https://ru.wikipedia.org/wiki/Бэкдор

Об авторе

Жданов Андрей Николаевич, Лаборатория цифровой криминалистики и исследования вредоносного кода компании F6, главный специалист.