УДК 004

ОПИСАНИЕ ОБЩИХ ПРИНЦИПОВ И РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ ОТ НЕКОТОРЫХ ВИДОВ ВИРУСНЫХ АТАК

И.В МИСЕВИЧ
(Представлено канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В данной статье описаны общие рекомендации для защиты от некоторых видов вирусных атак.

Целью данной статьи является проведение анализа поведения типичного вирусного ПО, поиск решений для устранения последствий с наименьшими усилиями, а также написание общих рекомендаций для быстрого восстановления работоспособности ОС Windows после вирусной атаки.

Актуальность данной темы обусловлена тем, что ОС Windows наиболее широко используется, и как следствие, чаще всего подвергается атаке. В данной статье описаны общие принципы работы и закономерности в поведении некоторых классов вредоносного ПО, а также способы устранения последствий их работы. Здесь не будут описываться алгоритмы работы реальных вирусов, но будут общие рекомендации по профилактическим и экстренным восстановительным мерам.

Задача состояла в анализе изменений реестра, которые вносились вирусным ПО. В основном изучались группы вирусов, направленных на остановку работы ОС (например, WinLock), которые делают невозможной дальнейшую работу ОС Windows, а, следовательно, лишают пользователя возможности устранить последствия в штатном режиме, находясь в среде штатно установленной ОС. Также рассмотрены некоторые профилактические меры общего характера, актуальные не только при использовании ОС Windows.

В любой версии ОС Windows (начиная с Windows 95) имеется реестр, представляющий из себя базу данных, в которой хранятся записи параметров, необходимых для работы различного ПО – как установленного, так и входящего в состав самой ОС. Для любых ОС Windows имеются типичные секции реестра, которые не изменяются от версии к версии, для обеспечения совместимости при работе ПО в различных версиях Windows. Например, существуют типичные места для автоматического старта программ.

В реестре имеется множество секций, которые могут быть – как созданными изначально (при установкеWindows), так и создаваемыми другим ПО, для хранения его параметров.

В реестре Windows содержатся не только параметры старта, но и множество других параметров, необходимых для работы различного ПО. Например, сведения о лицензировании, персональных настройках и так далее.

Типичные секции реестра Windows, в том числе и те, которые отвечают за автозагрузку, как правило часто используются при работе различного вирусного ПО. Вирусы прописываются в эти секции, так как любая ОС Windows отреагирует на них одинаково без дополнительных настроек, что обеспечит наибольшую поражающую силу. Некоторые вирусы, например –Trojan WinLock, загружаются при старте любого пользователя Windows, поэтому приходится выполнять аварийное восстановление ОС, изменяя параметры её реестра, и при этом находиться за её пределами (например, при загрузке с различных дисков аварийного восстановления). На многих дисках могут содержаться антивирусные средства. Есть и такие диски, которые специально предназначены для этого (например – KasperskyRescueDisk). Однако, в базе сигнатур конкретного антивирусного ПО может не быть данной модификации вируса и/или могут отсутствовать драйвера сетевой карты в самой ОС, которая содержится на данном диске. Это лишает пользователя возможности подключиться к Интернету, и как следствие - не даёт обновить вирусную базу.

Несмотря на то, что коды различных вирусов постоянно совершенствуются и шифруются, поведение многих из них остаётся схожим, так как алгоритмы для реализации тех или иных команд Windows часто остаются неизменными. Зачастую, можно обойтись очисткой всех секций реестра, отвечающих за автозагрузку программ. Это даёт возможность отменить старт множества вирусов, затем штатно удалить сами файлы, содержащие их.

Ниже приведён пример простейшего пакетного файла сценария Windows, содержащего вредоносный код:

```
@echo off
reg add "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\poli-
cies\system" /v DisableTaskMgr /t reg_dword /d 1 /f>nul
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\poli-
cies\system" /v DisableTaskMgr /t reg_dword /d 1 /f>nul
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
/v Shell /t reg_sz /d %windir%\TestVirus.bat /f>nul
taskkill /f /im explorer.exe>nul
chcp 1251
shutdown /s /f /t 10 /c "Тестовый вирус">nul
xcopy /y TestVirus.bat %windir%\>nul
```

Данный код выполняет отключение диспетчера задач у всех пользователей. После этого прописывает себя в секцию реестра Windows, вместо стандартного проводника. Потом даёт команду на выключение компьютера с отсрочкой в 10 секунд, выводит предупреждающую надпись и копирует себя в папку Windows.

Так как в стандартном случае интерфейс Windows стартует автоматически, то прописанный в его секцию вирус будет стартовать вместо него у всех пользователей. Но даже после удаления файла с вирусом пользователь не получает интерфейс, так как вместо стандартной команды Explorer.exe в секции Shell прописан вирус, и проводник не стартует. Для возврата работоспособности ОС требуется вернуть стандартные значения в секции Shell и те, которые отвечают за диспетчер задач.

Конечно, этот вирус легко обойти. Например, зайдя в безопасном режиме с поддержкой командной строки. Плюс ко всему, код из BAT-скрипта легко читаем. Однако, это - не пример реального блокирующего вируса, а тестовый код, который показывает приблизительную логику работы такого класса вирусов.

Многие вирусы оставляют после себя неверные значения реестра, а некоторые из них и вовсе удаляются сами, после изменения вышеупомянутых. Как уже было сказано выше, полная очистка секций автозагрузки в большинстве случаев даёт положительный эффект. Очевидным преимуществом такого подхода являются простота и быстрое достижение результата.

Конечно, данный подход имеет множество недостатков. Например, все программы, которые загружались автоматически (за исключением тех, ссылки на которые помещены в папку автозагрузки), не будут загружаться сами, и пользователю нужно будет заново войти в эти программы и выставить соответствующие опции (например, в Skype и других программах). Но, чаще всего это не является проблемой. В большинстве случаев ОС не подвергается негативным изменениям, а блокировка снимается.

Также учтены и некоторые другие изменения, которые часто производятся вирусами, но которые можно вернуть к стандартным значениям, не навредив пользователю. Например, можно удалить файл HOSTS, и скачать новый – со стандартными значениями. Это нужно сделать для отмены работы вирусов, которые "блокируют" попадание на конкретный сайт, перенаправляя пользователя на другой. Так как файл hosts является локальной таблицей соответствия между доменным именем сайта и его IP-адресом (выполняет функцию базы DNS-сервера на конкретном компьютере), то при нахождении IP-адреса к нужному доменному имени Windowsпопадает именно по адресу, который написан в этом файле, а не отправляет запрос по цепочке DNS-серверов (для снижения нагрузки на них). Зачастую, вирусы типа "блокираторов соц. сетей" действуют именно так, меняя адрес конкретного сайта на подставной или локальный (127.0.0.1). Аналогично действуют и некоторые мошеннические программы: подменяют адрес сайта (например, банковского) на адрес сайта-имитатора, который полностью повторяет внешний вид оригинала, но на котором встроен скрипт, ворующий персональные данные. Такой ложный сайт может также не только отправить введённые данные в свои базы, но и передать их оригинальному сайту, перенаправив пользователя на него. Ничего не подозревающий пользователь набирает верное доменное имя, попадает на идентичный по внешнему виду сайт, вводит свои данные и авторизуется уже на оригинальном сайте, при этом не догадываясь, что его данные продублированы злоумышленникам и переданы третьим лицам.

Для исключения таких проблем можно удалить файл hosts, а также не лишним будет очистка кэшей браузеров и удаление сомнительных расширений (дополнений). Также следует отключить разрешение на автоматическую установку и обновление расширений в настройках браузера для всех сайтов. Аналогично стоит поступить и с авто перенаправлениями на другие страницы.

Также, в качестве меры предосторожности можно создать несколько закладок с часто посещаемыми сайтами, в которых прописать их прямой IP-адрес, а не доменное имя. В этом случае соответствие не потребуется, и запрос пользователя будет попадать прямо на прописанный конкретный адрес. Есть множество сервисов, на которых можно узнать IP-адрес конкретного сайта. Например, на сайте 2ip.ru имеется сервис для определения своего IP, IPдругих сайтов, измерения скорости интернет соединения и так далее.

Также следует отключить авто-сохранение паролей, и вообще авторизоваться на сайтах в «приватном» режиме, когда браузер не запоминает историю посещений и не сохраняет файлы cookie, так как эта информация может быть украдена вирусом.

Также следует создать отдельного пользователя с ограниченными правами, а лучше – виртуальную машину с отдельной гостевой ОС. Это нужно в случаях, когда есть необходимость переходить по сомнительным ссылкам. В гостевой ОС не следует оставлять своих данных, иначе она станет бесполезна для вышеприведённой ситуации. На виртуальной машине, которая создана для этих целей, не следует авторизоваться на проверенных сайтах, оставлять какие-либо конфиденциальные данные, пароли и так далее. Существует множество программ для работы с виртуальными машинами. Например, Oracle Virtual Box (бесплатная), VMWare (платная) и так далее. Общий принцип создания и настройки виртуальной машины достаточно прост. Все программы подобного рода эмулируют работу различных основных устройств (видеокарты, звуковой платы и т.д.). Под эти виртуальные устройства имеются пакеты драйверов, которые идут в комплекте с самой программой для работы с ВМ. Гостевая ОС работает не с реальными устройствами, а с эмулированными, а сама программа для работы с ВМ преобразует команды реальных устройств в команды для работы с виртуальными. Также эмулируется работа отдельного ПЗУ, который является файлом (или набором файлов), реальная разметка накопителей и файловые системы разделов – не затрагиваются. Такой подход делает возможной изоляцию гостевой ОС от основной, а также делает гостевую ОС программно-независимой от реального оборудования. Однако, стоит помнить, что ресурсы для работы виртуальной машины даёт основная ОС, а сама она берёт их от реального оборудования, распределяя ресурсы между приложениями.

Если работает виртуальная машина, то вирусы, проникшие на неё, не поразят основную ОС, так как гостевая ОС работает на более высоком уровне абстракции, чем основная, и программа для запуска виртуальных машин работает как обычное приложение в основной ОС.

В заключение хотелось бы отметить, что даже соблюдение всех вышеупомянутых мер не является панацеей, однако существенно снижает вероятность атаки на пользователя. Ещё раз подведем краткий список рекомендаций:

- При блокировке Windows вирусным ПО, очищать все места автозагрузки;
- Запретить изменения файла hosts (все изменения вносить только вручную, при необходимости);
- Запретить автоматическую установку расширений (дополнений) браузеров;
- Запретить автоматические перенаправления на другие страницы;
- Не использовать авто-сохранение паролей;
- Периодически очищать кэши браузеров;
- Авторизоваться на сайтах в “приватном” режиме;
- Не сохранять/удалять файлы cookie, для сайтов, требующих авторизации;
- Использовать виртуальную машину с гостевой ОС, для посещения сомнительных ресурсов в Интернете, а также для работы с неизвестным ПО.

ЛИТЕРАТУРА

1. Официальный сайт компании Microsoft [Электронный ресурс] URL: https://www.microsoft.com дата доступа: 26.09.2020
2. Официальный сайт лаборатории Касперского [Электронный ресурс] URL:http://www.kaspersky.ru дата доступа: 26.09.2020
3. Официальный сайт компании Dr.Web[Электронный ресурс] URL:http://www.drweb.ru дата доступа: 26.09.2020
4. Официальный сайт компании AvastSoftware [Электронный ресурс] URL:https://www.avast.ru/ дата доступа: 26.09.2020
5. Официальный сайт компании VBA [Электронный ресурс] URL:http://www.anti-virus.by дата доступа: 26.09.2020
6. Официальный сайт компании Symantec [Электронный ресурс] URL:https://www.symantec.com. Дата доступа: 26.09.2020.