



PT

# Обнаружение и обход песочниц

Как изменилось  
вредоносное ПО за 10 лет

[ptsecurity.com](http://ptsecurity.com)

# Содержание

Введение	3
Что такое песочница	4
Резюме	5
Эволюция методов обхода песочниц	6
Популярные методы обхода средств виртуализации	10
Проверка запущенных процессов	10
WMI-запросы	10
Проверка значений ключей реестра	12
Иные проверки окружения	13
Должна ли песочница выявлять все методы	13
Противодействие анализу и отладке	14
Заключение	15

## Введение

Первым этапом большинства кибератак является сбор информации о жертве. Злоумышленники собирают данные о системе и внутренней сети, для того чтобы оценить, какую пользу они смогут извлечь из этой атаки, а также спланировать свои дальнейшие действия. При этом преступникам важно понимать, что они получили доступ к реальной рабочей станции в инфраструктуре компании, а не к виртуальной среде, предназначенной для анализа поведения исполняемых файлов. Поэтому во вредоносное программное обеспечение встраиваются функции для обнаружения и обхода средств защиты, а также для сокрытия вредоносной функциональности в случае запуска в песочнице или анализаторе кода.

Мы проанализировали 36 семейств ВПО, которые использовали не менее 23 АРТ-группировок по всему миру с 2010 года по первую половину 2020-го. Выборка была сформирована на основании данных [MITRE](#) и данных о новых образцах ВПО, исследованных экспертами [PT Expert Security Center](#).

В атаках на российские компании был замечен 31% ВПО; 25% ВПО были активны в 2019—2020 годах.

---

*В этом исследовании мы покажем, как менялись техники обхода средств виртуализации и анализа за последние 10 лет.*



## Что такое песочница

Песочница запускает файл в изолированной виртуальной среде, анализирует действия, которые он совершает в системе, и выдает вердикт о том, безопасен этот файл или нет. Песочницы бывают с агентом и безагентные.

### Решение с агентом

Внутри виртуальной машины присутствует вспомогательный агент (специальный процесс), который отвечает за управление состоянием системы, получение и передачу интересных событий и артефактов. При этом при порождении нового процесса происходит перехват вызовов API-функций (изменение адреса в памяти процесса или кода в теле функции).

В таком решении есть существенный недостаток: необходимо скрывать и защищать объекты, ассоциированные с агентом, от ВПО.

### Безагентное решение

Используется процессорная технология вложенного разбиения на страницы (second level address translation, SLAT), то есть аппаратная виртуализация. В процессорах AMD эта технология поддерживается с помощью Rapid Virtualization Indexing (RVI), а в процессорах Intel с помощью Extended Page Table (EPT).

Эта технология представляет собой промежуточные страницы памяти, которые располагаются между гостевой физической памятью и хостовой виртуальной памятью. Это позволяет:

- изучить отображение страниц памяти гостевой машины;
- выделить интересные участки (например, содержащие адреса или код ядерных функций);
- разметить выбранные страницы таким образом, чтобы права доступа к страницам памяти в EPT не совпадали с правами доступа к страницам в гостевой машине;
- отловить обращение к размеченным участкам памяти (в этот момент случится ошибка доступа (EPT violation), в результате гостевая машина будет приостановлена);
- проанализировать состояние, извлечь необходимую информацию о событии;
- переразметить страницу памяти в правильное состояние;
- восстановить работу гостевой машины.

Наблюдение за всем происходящим осуществляется за пределами изолированной машины, соответственно ВПО, которое находится внутри, не может обнаружить факт наблюдения.

## Резюме

1. Чаще всего техники обхода песочниц и обнаружения средств анализа внедряют в ВПО для удаленного доступа (56% среди рассмотренного ВПО) и загрузки (14%). Это объясняется тем, что подобные программы используются как раз в разведке и сборе информации о целевой системе. Если злоумышленники обнаружат, что ВПО начало исполнение в виртуальной среде, то они не станут развивать этот вектор атаки и загружать вредоносную нагрузку, а постараются скрыть свое присутствие, прекратив работу ВПО.

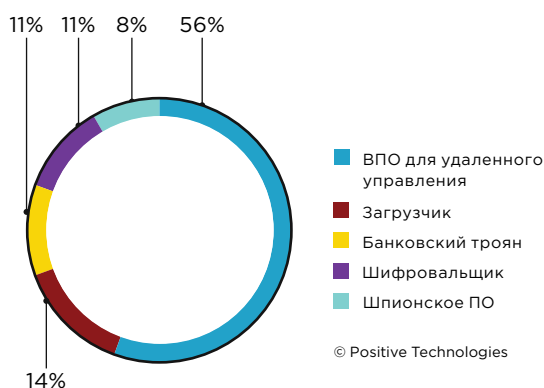


Рисунок 1. Типы исследованного ВПО

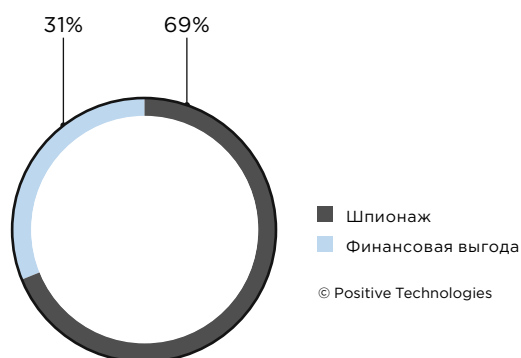


Рисунок 2. Мотивы использования ВПО

2. В атаках, совершаемых с целью шпионажа, применялось 69% рассмотренного ВПО. В таких атаках для преступников особенно важно длительное скрытое присутствие в системе жертвы, поэтому они ищут способы как можно дольше оставаться незамеченными.
3. Часто для выявления средств виртуализации (песочниц) злоумышленники отправляют WMI-запросы (25% ВПО) либо реализуют иные проверки окружения (33%), а также проверяют список запущенных процессов (19%). Причем информацию о среде виртуализации злоумышленники могут использовать также для того, чтобы определить линию поведения в последующих атаках.

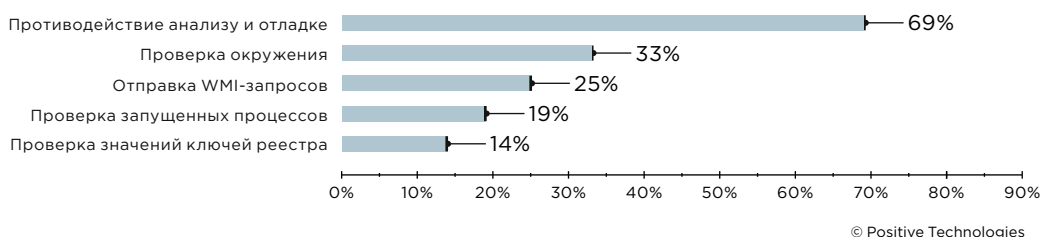


Рисунок 3. Наиболее популярные методы обхода и обнаружения средств виртуализации и анализа (доля ВПО)

4. Становится все сложнее проводить статический анализ вредоносных файлов, сопоставлять подозрительные файлы с известными сигнатурами и хеш-суммами, поскольку разработчики ВПО применяют методы обфускации (запутывания) кода и стараются затруднить экспертам по безопасности его анализ. Поэтому мы рекомендуем проводить анализ поведения файлов при запуске в защищенной виртуальной среде — песочнице.

# Эволюция методов обхода песочниц

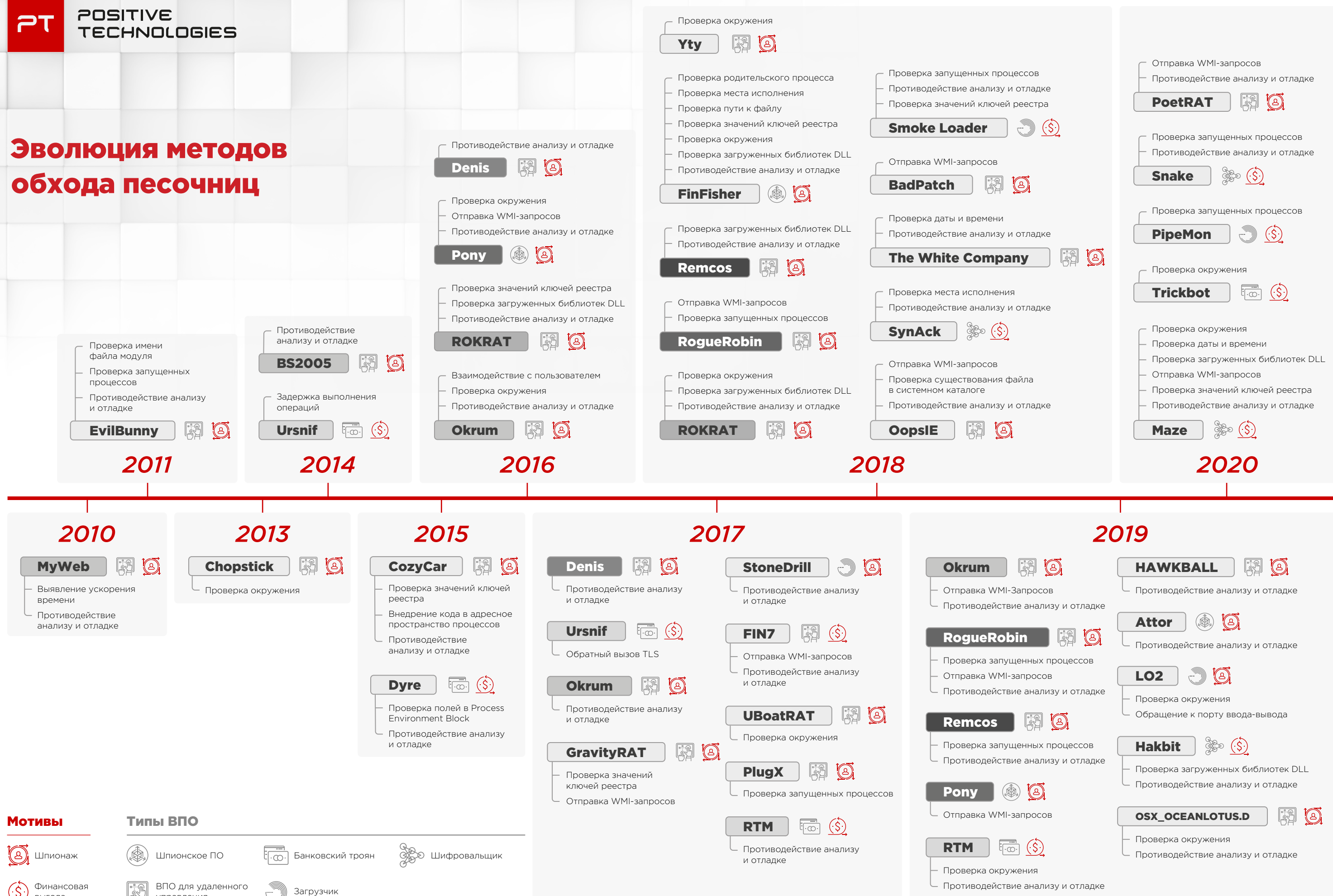


Рисунок 4. Методы обнаружения и обхода средств виртуализации и анализа, применяемые в ВПО в 2010—2020 годы

Мы проследили изменения в методах обхода песочниц и средств анализа и видим, что одно и то же ВПО в разные годы использует разные методы. Кроме того, злоумышленники стараются использовать одновременно несколько технологий. В случае если один из методов не сработает и будет перехвачен песочницей, ВПО попытается по другому какому-то признаку определить, что выполняется в среде виртуализации, чтобы вовремя прекратить свою работу.

*APT-группировка Ke3chang (также известна как APT15) в 2010 году использовала бэкдор MyWeb, затем в 2014 году — BS2005, а в 2016–2019 годах — Okrum. Злоумышленники меняли методы обхода и обнаружения средств виртуализации и анализаторов кода. Они проверяли взаимодействие с пользователем, ожидая трех нажатий на левую кнопку мыши или определяя положение курсора, а объем физической памяти узнавали то с помощью вызова функции `GetGlobalMemoryStatusEx`, то с использованием WMI-запросов.*

Приведем еще несколько примеров.

## ROKRAT

**Тип:** ВПО для удаленного управления

**Группировка:** APT37, активна с 2012 года

**Цель:** организации в Южной Корее

**Вектор заражения:** фишинг (вредоносные документы HWP, распространяемые по электронной почте и эксплуатирующие уязвимость CVE-2013-0808)

**Мотив:** шпионаж

Методы обхода и обнаружения средств виртуализации и анализа	2016	2018
Проверка загруженных библиотек <code>SbieDll.dll</code> , <code>Dbghelp.dll</code> , <code>Api_log.dll</code> , <code>Dir_watch.dll</code>	+	+
Получение значения ключа <code>SystemBiosVersion</code> ветки реестра <code>HARDWARE\DESCRIPTION\System</code>	+	–
Использование инструкции <code>NOP</code> (No Operation) в качестве наполнителя в самоизменяющемся коде для защиты от отладки	+	–
Вызов функции <code>IsDebuggerPresent</code> для выявления отладки	–	+
Вызов функции <code>GetTickCount</code> дважды, чтобы проверить пошаговое выполнение	–	+
Проверка существования файла <code>C:\Program Files\VMware\VMware Tools\vmtoolsd.exe</code>	–	+

## RogueRobin

**Тип:** ВПО для удаленного управления

**Группировка:** DarkHydrus, активна с 2016 года

**Цель:** государственные и образовательные учреждения на Ближнем Востоке

**Вектор заражения:** фишинг (вредоносные документы Microsoft Office, распространяемые через Google Drive)

**Мотив:** шпионаж

### Методы обхода и обнаружения средств виртуализации и анализа

	2016	2018
Отправка WMI-запросов для проверки версии и производителя BIOS	+	+
Отправка WMI-запросов для проверки количества ядер процессора. Значение должно быть больше 1	+	+
Отправка WMI-запросов для проверки объема физической памяти. Значение должно быть не менее 2 900 000 000 байт	+	+
Проверка количества запущенных процессов для Wireshark и Sysinternals	+	+
Обфускация PowerShell-скрипта с использованием инструмента Invoke-Obfuscation	+	+
Проверка наличия отладчика при каждом DNS-запросе	-	+

## Remcos

**Тип:** ВПО для удаленного управления

**Группировка:** Gorgon Group, активна с 2018 года

**Цель:** государственные учреждения России, Великобритании, Испании и США

**Вектор заражения:** фишинг (вредоносные документы Microsoft Word, распространяемые по электронной почте и эксплуатирующие уязвимость CVE-2017-0199)

**Мотив:** шпионаж

### Методы обхода и обнаружения средств виртуализации и анализа

	2016	2018
Проверка наличия в системе устаревшего артефакта SbieDll.dll	+	-
Шифрование исходного кода с использованием алгоритмов RC4 и Base64	+	+
Проверка vmtoolsd.exe и vbox.exe в списке запущенных процессов	-	+
Вызов функции IsDebuggerPresent для проверки, запущен ли вызывающий ее процесс в контексте отладчика	-	+



Отметим также, что в 2018—2019 годах увеличилось количество ВПО, которое применяет методы обхода песочниц. Однако на эту статистику повлиял, вероятнее всего, тот факт, что эксперты стали чаще исследовать образцы ВПО.

Преступники, продающие ВПО в дарквебе, также уделяют особое внимание функциям обнаружения и обхода песочниц и антивирусов, противодействию анализу и отладке. Цены на ВПО, применяющее методы обхода песочниц, начинаются от 30 долл. США. А за 20 долл. злоумышленники предлагают услуги по дополнительной защите ВПО от обнаружения антивирусами и песочницами.

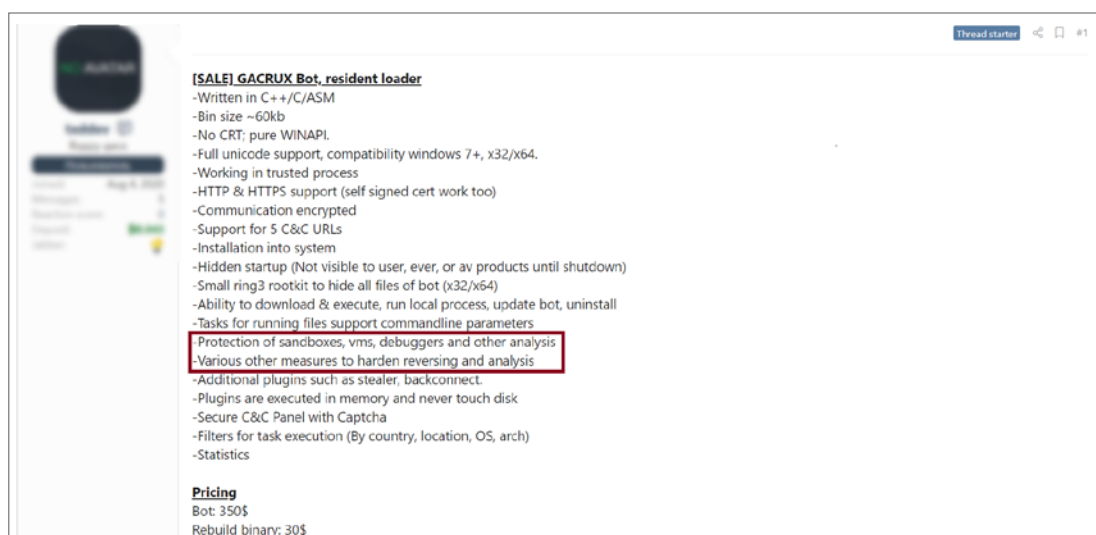


Рисунок 5. Объявление о продаже загрузчика с функциями обхода средств защиты

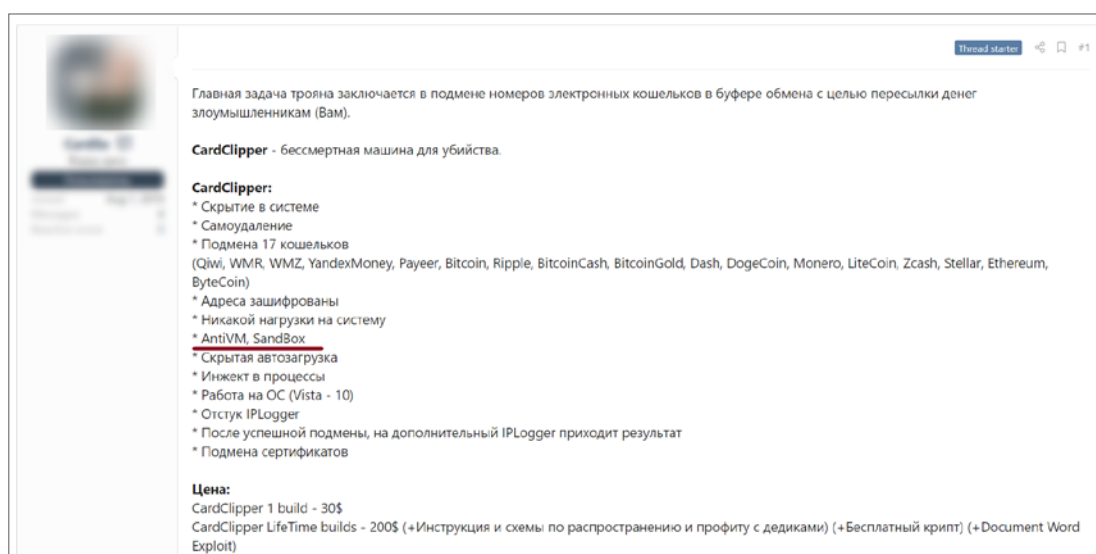


Рисунок 6. Предложение услуг по защите ВПО от обнаружения песочницами

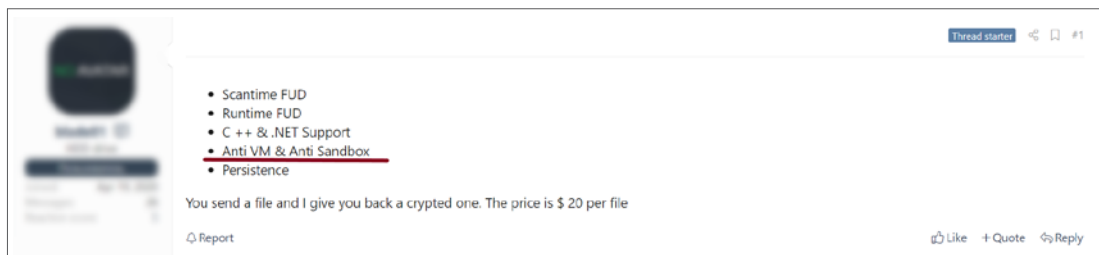


Рисунок 7. Объявление о продаже ВПО с функциями обхода средств виртуализации

## Популярные методы обхода средств виртуализации

### Проверка запущенных процессов

Применяется в *EvilBunny*, *FinFisher*, *PlugX*, *Remcos*, *RogueRobin*, *Smoke Loader*, *PipeMon*, *Snake*

Каждое пятое ВПО для выявления средств виртуализации (песочниц) анализирует список запущенных процессов. Например:

- ВПО для удаленного управления *EvilBunny* продолжает работу только в том случае, если в среде запущено не менее 15 процессов;
- *PlugX* (бэкдор, который широко используется АРТ-группировками на протяжении 10 лет) проверяет, что инструменты VMware в фоновом режиме не работают, выполняя поиск любых процессов с именем «vmtoolsd»;
- *Remcos*, применяемый группировкой Gorgon Group в фишинговых атаках на госучреждения, в списке запущенных процессов ищет «vmtoolsd» и «vbox.exe».

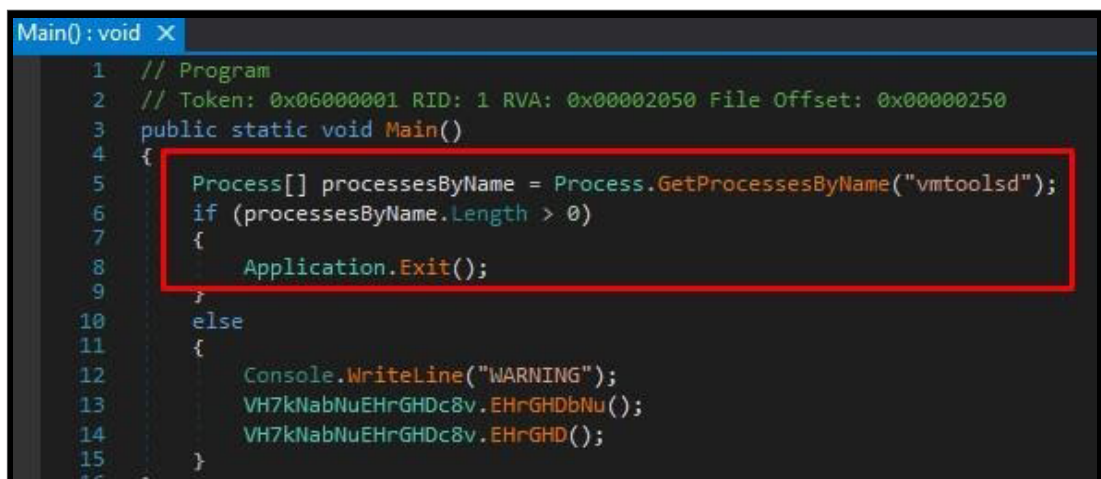


Рисунок 8. Поиск процесса vmtoolsd (Remcos)

### WMI-запросы

Применяется в *BadPatch*, *Fin7*, *GravityRAT*, *OopsIE*, *Pony*, *RogueRobin*

**Windows Management Instrumentation (WMI)** — технология для централизованного управления различными частями компьютерной инфраструктуры под управлением Windows.

При создании ВПО злоумышленники с 2016 года активно используют WMI-запросы для обращения к устройствам, учетным записям, сервисам, процессам, сетевым интерфейсам и другим программам. Этой технологией пользуются разработчики каждого четвертого ВПО. Наиболее часто встречаются проверки используемых моделей жесткого диска, материнской платы, версий ОС, BIOS.

Троян для удаленного доступа GravityRAT использует интересный способ обнаружения средств виртуализации. С помощью WMI-запроса `SELECT * FROM MSAcpi_ThermalZoneTemperature` он проверяет температуру процессора: в случае запуска на физическом устройстве запрос возвращает цифровое значение температуры. Если же в результате выполнения команды ВПО получит «ERROR» или «Not Supported», значит, исполнение происходит в среде виртуализации.

```
C:\WINDOWS\system32>wmic /namespace:\\root\WMI path MSAcpi_ThermalZoneTemperature get CurrentTemperature
CurrentTemperature
3062
2732
2911
2922
2922
2932
2921
```

Рисунок 9. Результат выполнения команды `SELECT * FROM MSAcpi_ThermalZoneTemperature` на физическом устройстве

```
C:\Windows\system32>wmic /namespace:\\root\WMI path MSAcpi_ThermalZoneTemperature get CurrentTemperature
Node - DESKTOP-FU7KSUL
ERROR:
Description - Not supported
```

Рисунок 10. Результат выполнения команды `SELECT * FROM MSAcpi_ThermalZoneTemperature` в среде виртуализации

WMI-запросы использует и группировка OilRig (APT34, Helix Kitten), которая уже более пяти лет атакует государственные учреждения, а также финансовые, энергетические, телекоммуникационные и другие компании, преимущественно в ближневосточном регионе. Например, бэкдор этой группировки OopsIE с помощью WMI-запроса `SELECT * FROM Win32_Fan` проверяет состояние работы вентилятора процессора. Этот запрос должен вернуть класс, описывающий статистику работы вентилятора, и если ответ будет пуст, значит, исполнение ВПО происходит в среде виртуализации.

```
Select Administrator: Windows PowerShell
PS C:\Windows\system32> $q = "Select * from win32_Fan"
PS C:\Windows\system32> Get-WmiObject -Query $q

__GENUS                : 2
__CLASS                 : Win32_Fan
__SUPERCLASS            : CIM_Fan
__DYNASTY               : CIM_ManagedSystemElement
__RELPATH               : Win32_Fan.DeviceID="root\\cimv2 0"
__PROPERTY_COUNT       : 22
__DERIVATION            : {CIM_Fan, CIM_CoolingDevice, CIM_LogicalDevice, CIM_LogicalElement...}
__SERVER               : \\.\root\cimv2
__NAMESPACE            : \\.\root\cimv2
__PATH                 : \\.\root\cimv2:Win32_Fan.DeviceID="root\\cimv2 0"
ActiveCooling           : True
Availability            : 1
Caption                : Cooling Device
ConfigManagerErrorCode : 
ConfigManagerUserConfig : 
CreationClassName       : Win32_Fan
Description             : Cooling Device
DesiredSpeed            : 
DeviceID               : root\cimv2 0
ErrorCleared            : 
ErrorDescription        : 
InstallDate             : 
LastErrorCode          : 
Name                   : Cooling Device
PNPDeviceID             : 
PowerManagementCapabilities : 
PowerManagementSupported : Other
Status                 : 2
StatusInfo              : 
SystemCreationClassName : Win32_ComputerSystem
SystemName              : 
VariableSpeed           : 
PSComputerName          :
```

Рисунок 11. Результат выполнения команды `SELECT * FROM Win32_Fan` на физическом устройстве

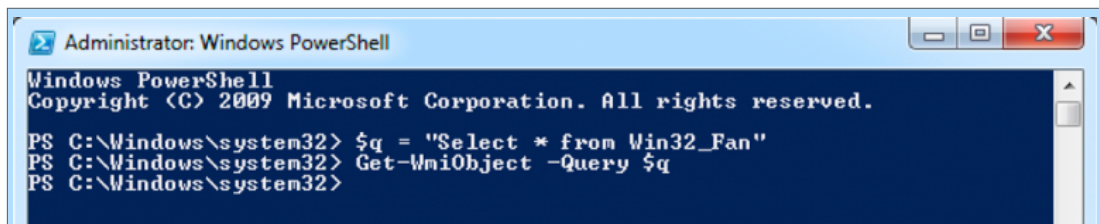


Рисунок 12. Результат выполнения команды SELECT \* FROM Win32\_Fan в среде виртуализации

## Проверка значений ключей реестра

Применяется в CozyCar, Smoke Loader, FinFisher, GravityRAT, ROKRAT

Часть ВПО (14%) считывает значения ключей реестра и ищет в них подстроки, указывающие на использование средств виртуализации. Например:

- Загрузчик банковского трояна Smoke Loader, который использует группировка TA505, считывает значения ключей реестра System\CurrentControlSet\Enum\IDE и System\CurrentControlSet\Enum\SCSI и ищет в них подстроки продуктов виртуализации QEMU, VirtualBox, VMware и Xen. Smoke Loader (Smoke bot) продается в дарквебе. Полная комплектация ВПО оценивается в 1650 долл.

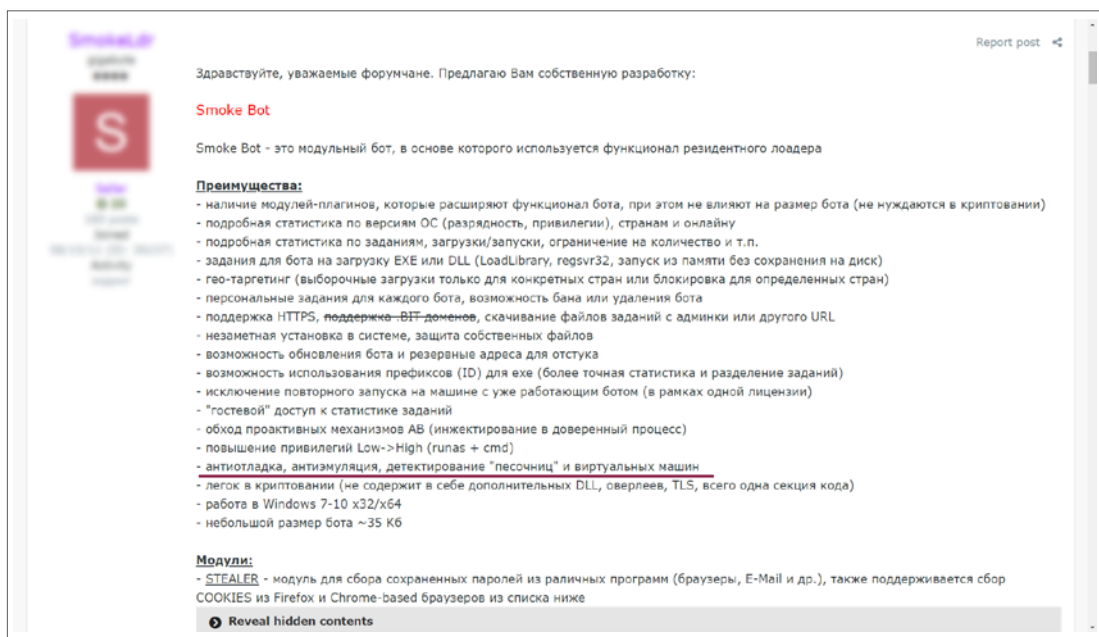


Рисунок 13. Объявление о продаже банковского бота Smoke bot



Рисунок 14. Стоимость банковского бота Smoke bot в дарквебе

- FinFisher проверяет, что HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid не совпадает с “6bald002-21ed-4dbe-afb5-08cf8b81ca32”; HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId не совпадает с “55274-649-6478953-23109”, “A22-00001”, “47220”; HARDWARE\Description\System\SystemBiosDate не содержит “01/02/03”.
- CozyCar, используемый группировкой APT29, проверяет значения ключей реестра SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall в поисках средств защиты информации.

## Иные проверки окружения

Помимо просмотра запущенных процессов, проверки значений ключей реестра и использования WMI-запросов, злоумышленники используют и другие способы проверки окружения. Например, банковский троян RTM (Redaman) проверяет существование следующих файлов и каталогов на дисках C и D:

- cuckoo,
- fake\_drive,
- perl,
- strawberry,
- targets.xls,
- tsl,
- wget.exe,
- \*python\*.

И если что-нибудь будет обнаружено, это станет сигналом для ВПО, что оно выполняется в песочнице или запущено в анализаторе кода.

APT-группировка APT37 (также известная как ScarCruft, Group123, TEMP.Reaper) на протяжении нескольких лет модифицировала бэкдор ROKRAT. Помимо проверки ключей реестра это ВПО проверяет существование файла C:\Program Files\VMware\VMware Tools\vmtoolsd.exe, а также проверяет, загружены ли следующие библиотеки анализаторов кода и отладчиков:

- SbieDll.dll,
- Dbghelp.dll,
- Api\_log.dll,
- Dir\_watch.dll.

Для того чтобы не попасться на следующую уловку, достаточно правильно настроить виртуальную машину. ВПО для удаленного доступа PoetRAT, используемое в целенаправленных атаках на ICS и SCADA-системы энергетической отрасли, по размеру жесткого диска определяет, что исполнение происходит в песочнице. Предполагается, что все песочницы имеют жесткий диск размером менее 62 ГБ, поэтому если выделить больше пространства для виртуальной машины, это ВПО удастся обмануть.

## Должна ли песочница выявлять все методы

Не все методы обхода песочниц легко обнаружить. Некоторые проверки, такие как, например, проверка пути к файлу, проверка MAC-адреса, проверка даты и времени, проверка времени выполнения операций, — слишком похожи на легитимные действия, поэтому их обнаружение будет выдавать много ложных срабатываний и мешать работе других программ. Однако это не означает, что ВПО удастся скрыться. Песочнице не обязательно уметь выявлять каждый метод обхода, поскольку у ВПО есть множество других признаков, по которым оно может быть перехвачено на других этапах работы. Но все же чем больше техник «видит» песочница, тем выше вероятность выявить новые образцы ВПО и впоследствии применить полученную информацию для реагирования на киберугрозы.



## Противодействие анализу и отладке

Для того чтобы ВПО как можно дольше не обнаруживали антивирусные программы, злоумышленники стараются избежать его анализа экспертами по безопасности. Для этого они обфусцируют код и выявляют инструменты отладки.

Например, ВПО для удаленного управления [Remcos](#) в 2019 году обогатилось методом выявления инструментов отладки. Если загрузчик после вызова функции `IsDebuggerPresent` обнаруживает отладчик в системе, он отображает сообщение: «This is a third-party compiled Autolt script» — и завершает исполнение.

Авторы шпионского ПО FinFisher предприняли множество дополнительных шагов для запутывания своего вредоносного кода, чтобы затруднить его анализ. Например, код операции 0x1A должен представлять функцию JB (переход, если меньше), но он реализуется с помощью инструкции установки флага переноса (STC), за которой следует JMP в код диспетчера, который будет проверять установленное состояние флага переноса.

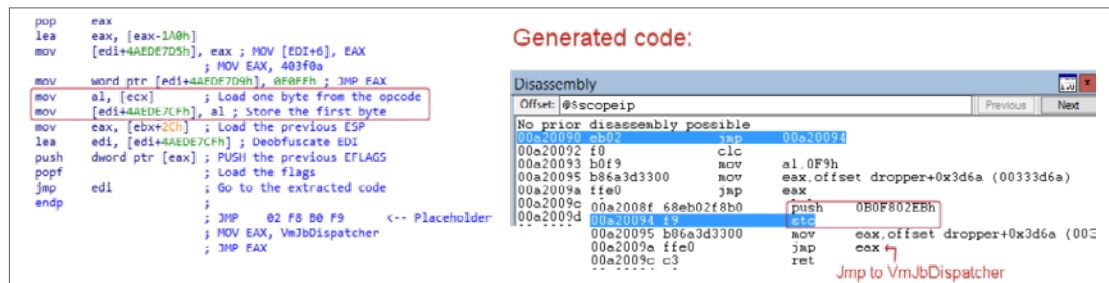


Рисунок 15. Один из способов обфускации (FinFisher)



Рисунок 16. Двойной вызов функций (EvilBunny)

Для проверки пошагового выполнения, которое применяется в отладчиках, EvilBunny выполняет вызов функций `NtQuerySystemTime`, `GetSystemTimeAsFileTime` и `GetTickCount`. Каждая функция вызывается дважды для вычисления разницы (дельты) при выполнении операции сна между первой и второй итерацией. Если любая из трех дельт меньше 998 миллисекунд, выполнение будет прервано.

Поскольку становится все сложнее выполнить статический анализ ВПО, выявить его характерные идентифицирующие свойства — сигнатуры и хеш-суммы, то в дополнение к статистическому анализу рекомендуется запускать подозрительные файлы в виртуальной среде и анализировать их поведение.

## Заключение

Злоумышленники регулярно вносят изменения в ВПО для того, чтобы как можно дольше избегать обнаружения. Особенно в этом преуспели АРТ-группировки. При сборе информации об инфраструктуре компании-жертвы преступники стараются использовать такое ВПО, в которое встроены функции выявления и обхода средств виртуализации и анализа кода. Кроме того, загрузчики и ВПО для удаленного доступа, продаваемые в дарквебе, содержат, как правило, базовые функции для обхода песочниц. По крайней мере, продавцы ВПО стараются заявлять о наличии этих функций.

Мы видим, что в последние годы разработчики ВПО стали особенно избегать анализаторов кода. Злоумышленники стремятся тщательно скрыть вредоносные функции от исследователей и минимизировать вероятность обнаружения ВПО по известным индикаторам компрометации (indicators of compromise, IOC). Поэтому классические средства защиты могут не справиться с обнаружением вредоносных программ, и мы рекомендуем для выявления современных образцов ВПО анализировать поведение файла в безопасной виртуальной среде. Кроме того, использование песочниц позволяет обогащать базу IOC и применять полученную информацию для реагирования на киберугрозы. Так, дополнив базы всех средств защиты информации в компании индикаторами компрометации, можно своевременно обнаружить даже новые версии ВПО при повторной попытке атаки на инфраструктуру компании. Например, если злоумышленники собрали новую версию ВПО, но не изменили в нем адрес командного центра, то ВПО будет выявлено по этому адресу.

С выявлением большинства популярных методов обхода средств виртуализации, применяемых в ВПО, песочницы уже научились справляться. Если же ВПО применяет методы, похожие на легитимные процессы, например проверяет текущие дату и время, то, как правило, у этого ВПО найдутся иные признаки, по которым песочница сумеет его вычислить. Мы видим, что злоумышленники постоянно совершенствуют свое ВПО, меняют техники обнаружения песочниц, применяют одновременно несколько техник, а значит и песочнице необходимо обладать гибкостью и умением быстро подстраиваться, имитируя реальную рабочую станцию. Песочница должна хорошо скрывать свое присутствие, чтобы не дать ВПО преждевременно прекратить свою работу и иметь возможность собрать индикаторы компрометации.

### О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/  
PositiveTechnologies  
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте [ptsecurity.com](#).