АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET приняла участие в ликвидации ботнета Gamarue

8 декабря 2017 года

Завершилась масштабная операция по ликвидации сети ботнетов Gamarue (Andromeda), действовавшей на протяжении нескольких лет. Операция с участием ESET, Microsoft и правохранителных структур продолжалась больше года.

Введение

Gamarue (Win32/TrojanDownloader.Wauchos по классификации ESET) известен с конца 2011 года и продавался в дарквебе под названием Andromeda bot. Бот пользовался спросом, чем обусловлено существование 464 независимых ботнетов на момент ликвидации. В прошлом Wauchos лидировал по числу атак, отраженных продуктами ESET.

В рамках операции ESET обеспечила технологическую экспертизу – мы отслеживали ботнеты в составе сети Wauchos, идентифицировали их C&C-серверы для последующей нейтрализации, отслеживали другие вредоносные программы, которые устанавливались в зараженные системы. Совместно с Microsoft мы предоставили правоохранительным органам следующую информацию:

- 1214 доменов и IP-адресов управляющих C&C-серверов ботнета
- 464 отдельных ботнетов
- 80 связанных семейств вредоносного ПО

На рисунке 1 вы можете видеть карту распространения Wauchos, построенную на основе нашей телеметрии. Очевидно, что Wauchos – глобальная проблема, и операция по его ликвидации стоила затраченных усилий. Приводим данные прошлого года – на пике активности Wauchos.

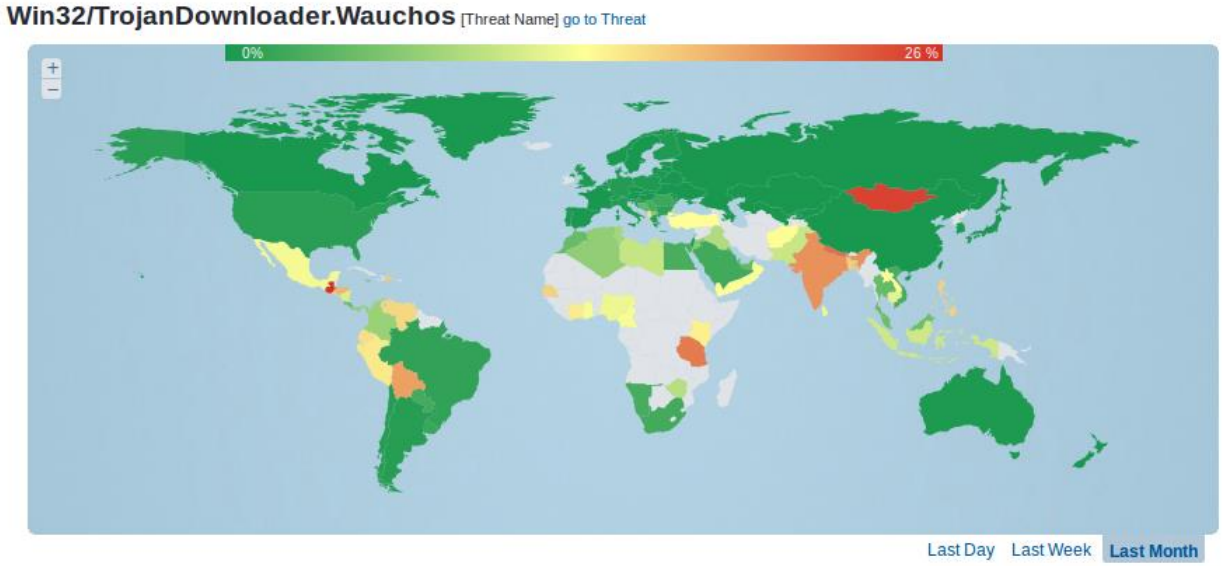

Рисунок 1. Распространение Wauchos (декабрь 2016 года)

Если вы подозреваете, что ваш компьютер на Windows был скомпрометирован, и не являетесь пользователем ESET, загрузите и используйте бесплатный инструмент ESET Online Scanner. Он удалит все угрозы, включая Wauchos, обнаружив их в системе.

Что такое Wauchos?

Это распространенное вредоносное ПО существует с 2011 года. Ранее мы уже писали о нем в блоге (см. «Источники»). В этом разделе мы рассмотрим основу Wauchos: что это и как распространяется, а далее опишем технические детали вредоносной программы.

Wauchos используется преимущественно для кражи учетных данных, а также загрузки и выполнения в системе других вредоносных программ. Таким образом, если система скомпрометирована Wauchos, в ней с большой долей вероятности установлена и другая малварь.

Wauchos имеет модульную архитектуру. Его функциональность можно расширить, добавив соответствующие модули. В числе известных модулей – кейлоггер, шпионское ПО для перехвата введенных логинов и паролей (формграббер), руткит, SOCKS прокси и TeamViewer-бот.

Существует пять основных версий Wauchos, основанных на собственной схеме управления версиями: 2.06, 2.07, 2.08, 2.09 и 2.10. В первых трех номер сборки включен в первый POST-запрос, направляемый ботом на C&C-сервер, поэтому идентифицировать версию довольно просто. В более поздних версиях Wauchos параметр `bv` в POST-запросе удален. Тем не менее, определить версию бота сравнительно легко, если посмотреть на строку идентификаторов, отправляемую на сервер (3):

Версия	Строка идентификаторов
<= 2.06	id:%lu|bid:%lu|bv:%lu|sv:%lu|pa:%lu|la:%lu|ar:%lu
2.07 – 2.08	id:%lu|bid:%lu|bv:%lu|os:%lu|la:%lu|rg:%lu
2.09	id:%lu|bid:%lu|os:%lu|la:%lu|rg:%lu
2.10 *	{"id":%lu,"bid":%lu,"os":%lu,"la":%lu,"rg":%lu}

(* Обратите внимание на переключение в формат JSON)

Типичный POST-запрос показан на рисунке 2. Строка идентификаторов зашифрована с помощью алгоритма RC4 и затем закодирована с base64.

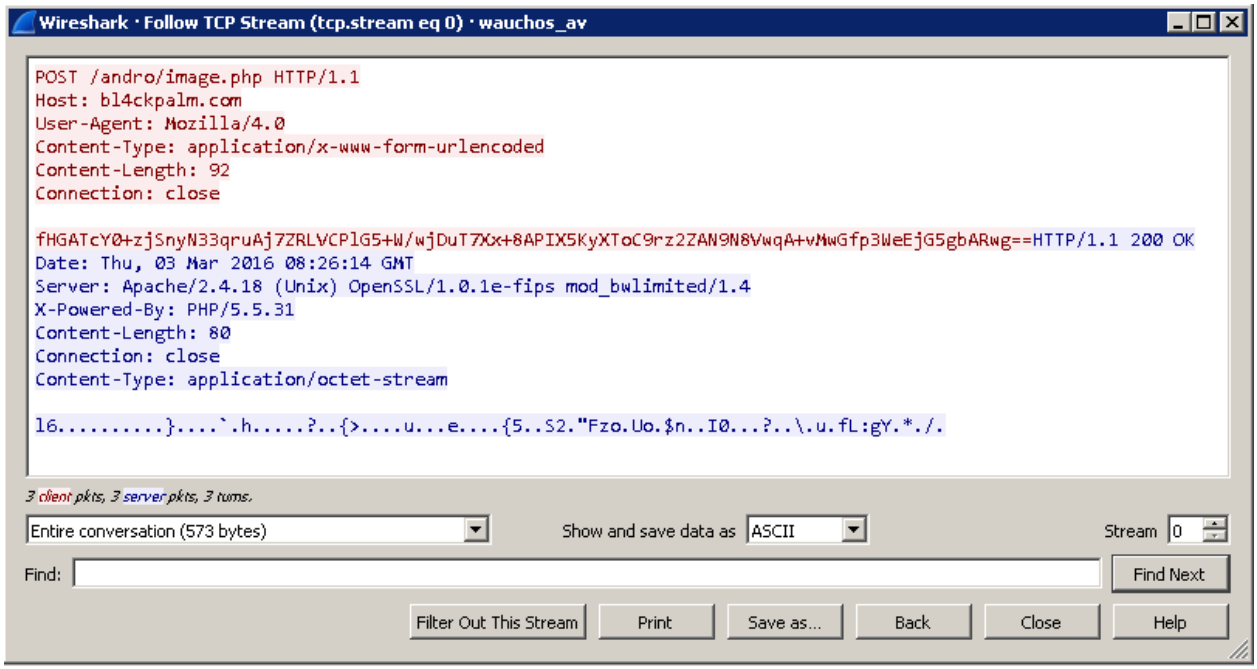

Рисунок 2. Типичный POST-запрос

Поскольку программа-компоновщик для версии 2.06 оказалась в открытом доступе несколько лет назад, мы видели достаточно много версий этого ботнета в данных телеметрии. Тем не менее, по нашим сведениям, наиболее распространена последняя версия – 2.10.

Глобальный характер угрозы также отмечен в разнообразии C&C-серверов, которые используют операторы Wauchos. На протяжении исследования мы открывали новые управляющие серверы каждый месяц. На рисунке 3 представлены домены верхнего уровня, используемые C&C-серверами; на рисунке 4 – география IP-адресов этих серверов на момент соединения с нашим поисковым ботом (crawler) в ноябре и декабре 2016 года.

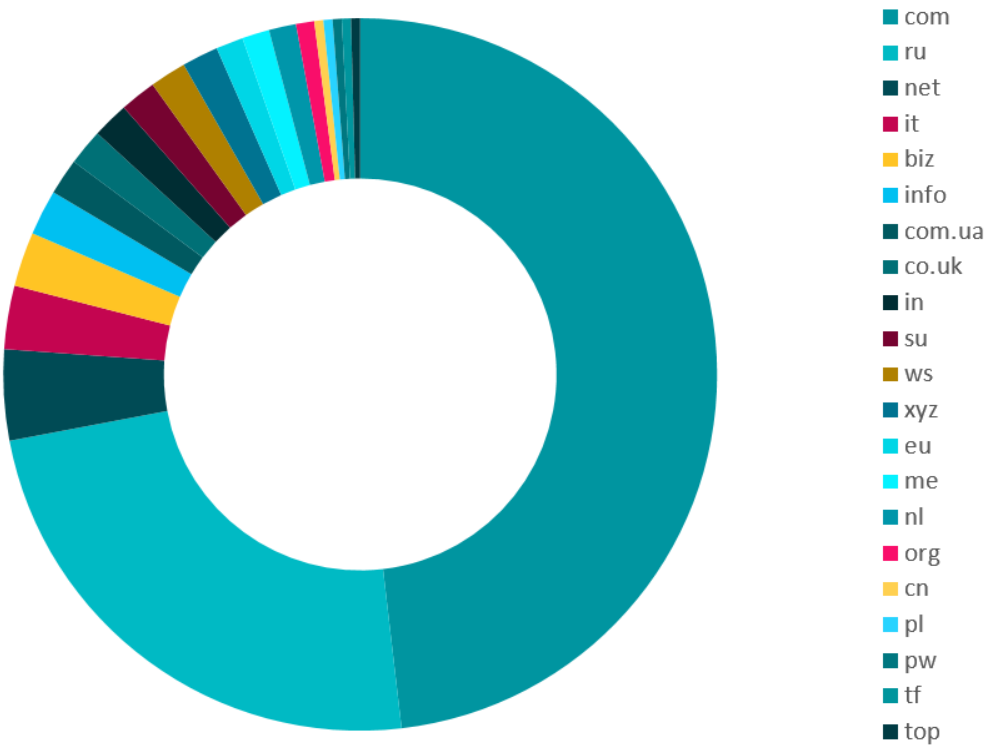

Рисунок 3. Домены верхнего уровня C&C-серверов в ноябре и декабре 2016 года

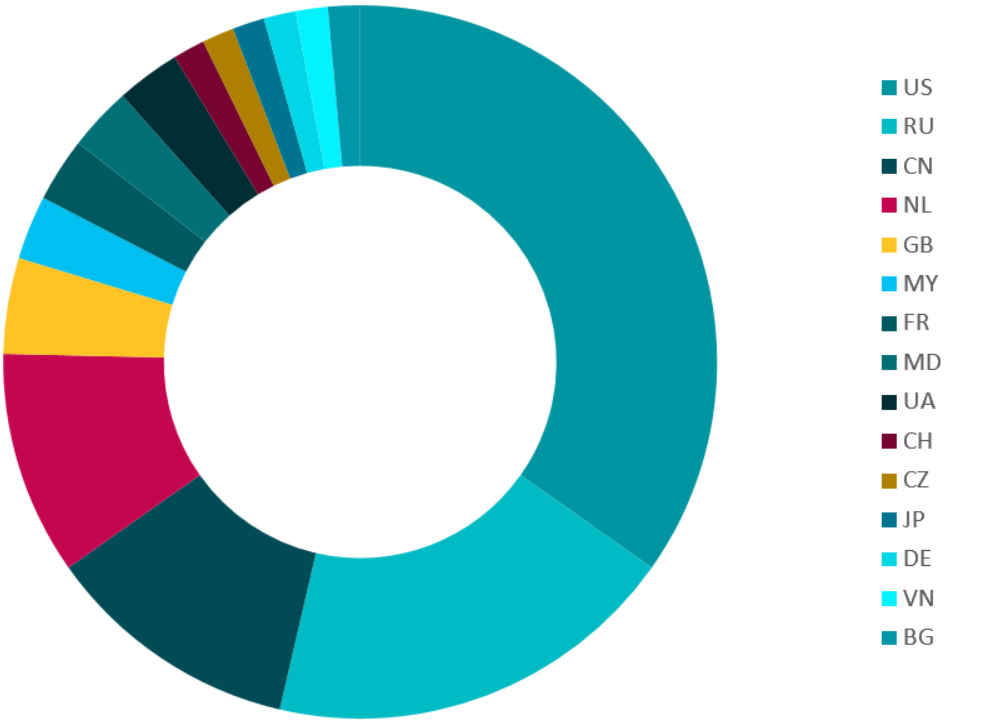

Рисунок 4. География IP-адресов C&C-серверов в ноябре и декабре 2016 года

Интересно, что ряд изученных образцов проверяет настройки клавиатуры и прекращает атаку, если в системе используется русский, белорусский, украинский или казахский языки.

Вектор заражения

Поскольку Wauchos покупают и распространяют разные операторы, для заражения используются разные векторы. Исторически образцы Wauchos распространялись через социальные сети, мессенджеры, съемные носители, спам и наборы эксплойтов. На рисунке 5 представлено типичное письмо с образцом Wauchos в аттаче.

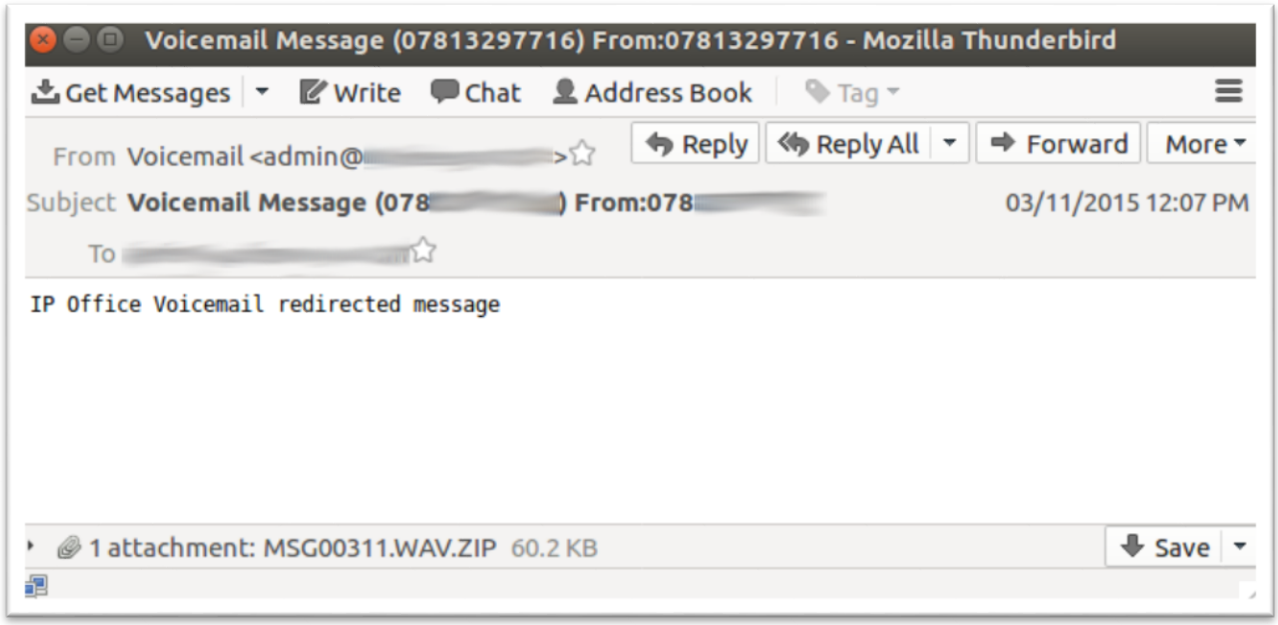

Рисунок 5. Типичный спам с Wauchos в приложении

Установка по схеме pay-per-install

Как сказано ранее, Wauchos используется преимущественно для распространения других вредоносных программ. С помощью наших автоматизированных систем мы собрали статистику о малвари, загружаемой ботами Wauchos, которые мы отслеживали. На рисунке 6 показаны различные модули, которые были загружены нашим поисковым ботом при первом соединении с C&C.

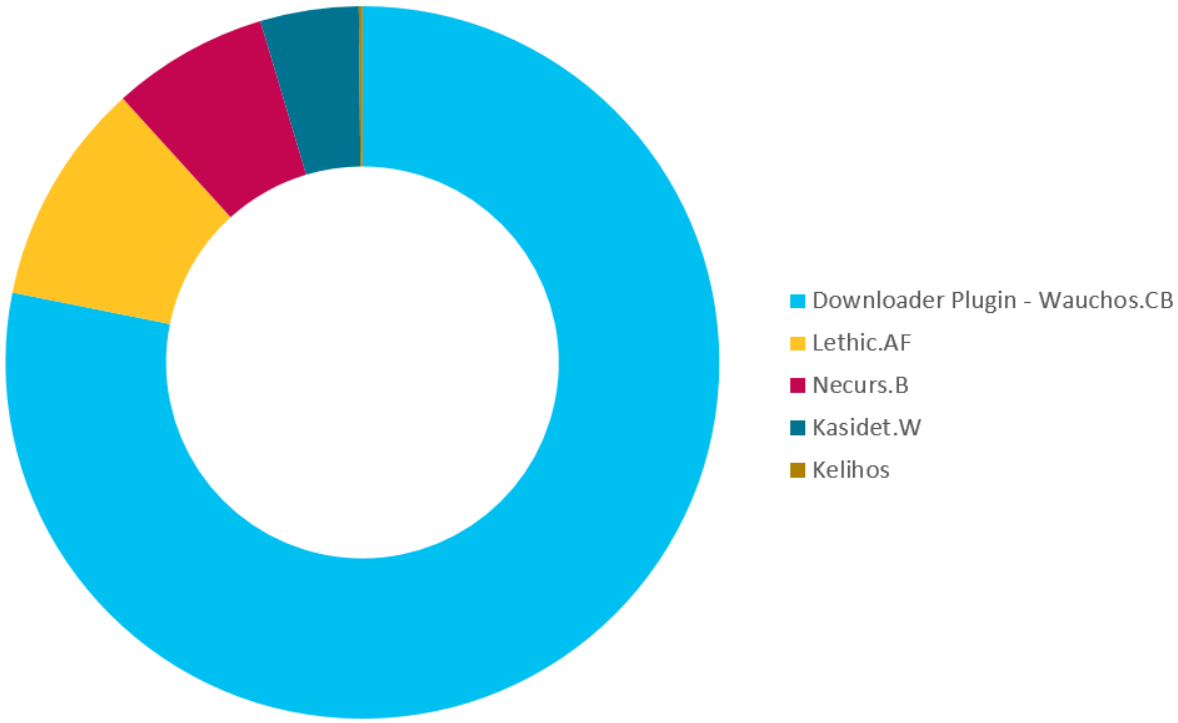

Рисунок 6. Статистика загрузок – декабрь 2016 года

Первая загрузка – как правило, модуль загрузчика, который мы опишем в следующем разделе. Далее производится установка других вредоносных программ – в декабре 2016 года загружались преимущественно спам-боты, в частности, Win32/Kasidet, Win32/Kelihos и Win32/Lethic. Конечно, если говорить о схеме pay-per-install, статистические данные время от времени меняются. Wauchos загружал и другое вредоносное ПО, но, по данным нашей телеметрии, чаще всего это были вышеперечисленные программы.

Технический анализ

В этом разделе мы представим некоторые технические детали, которые публично не обсуждались раньше, но создают контекст на фоне ликвидации ботнета. В частности, мы опишем два модуля, обеспечивающих коммуникации по сторонним каналам для ботмастера (botmaster), повышая устойчивость ботнета к операциям демонтажа.

Версии Wauchos

Прежде всего, мы бы хотели помочь коллегам, интересующимся данным семейством вредоносных программ, и кратко опишем, используя классификацию ESET, основные версии и их возможности.

Win32/Wauchos.B – наиболее распространенный детект компонента Wauchos версии 2.06. Версия 2.10 обычно детектируется как Win32/Wauchos.AW. Помимо этого, в семействе Win32/Wauchos собраны другие модули, упакованные варианты перечисленных версий и другие сборки Wauchos, включая 2.07, 2.08 или 2.09; по данным нашей телеметрии, они менее распространены, а, следовательно, менее актуальны в рамках обсуждения.

В последней версии Wauchos (2.10) бот поддерживает следующие команды:

Command ID	Описание
1	Загрузка и запуск двоичного файла
2	Загрузка модуля
3	Загрузка обновления вредоносной программы
6	Удаление всех модулей
9	Деинсталляция

Модули

Wauchos – расширяемый бот, который позволяет оператору создавать и использовать кастомные модули. Тем не менее, есть несколько широко доступных модулей, которые встречаются в разных ботнетах. В этом разделе мы рассмотрим модули, которые удалось загрузить с помощью нашего механизма отслеживания.

Название	Детектирование	Описание
SOCKS Proxy	Win32/TrojanDownloader.Wauchos.O	Принимает подключения и действует в качестве сетевого прокси
TeamViewer	Win32/TrojanDownloader.Wauchos.BA	Встраивает приложение TeamViewer, которое будет запущено в скрытом режиме и позволит атакующим подключаться и управлять скомпрометированной системой
Form Grabber	Win32/TrojanDownloader.Wauchos.AZ	Похищает контент, который пользователь вводит в веб-формы

Когда бот загружает модуль, он должен сначала расшифровать свой заголовок с ключом RC4. Заголовок содержит уникальный ключ, необходимый для расшифровки полезной нагрузки. После расшифровки последняя операция – распаковка модуля с помощью aPLib. Далее вредоносная программа использует кастомный загрузчик, чтобы загрузить в память бинарный блоб. Бинарные блобы у могут быть загружены *напрямую* в память и выполнены.

Число различных ключей RC4, собранных нашими системами слежения в разных ботнетах, оказалось невелико – около 40. Это позволяет легко расшифровать любые загруженные компоненты, даже те, что не нужны для анализа образца.

Что касается коммуникаций C&C, все проанализированные нами образцы для разрешения C&C-доменов напрямую использовали инфраструктуру DNS Google. Версия 2.06 пытается разрешить IP-адрес C&C-сервера с использованием UDP-сокетов до 8.8.4.4:53. Если это не удается, сначала возвращается к API-интерфейсу DnsQueryA (), а затем к API gethostbyname (). Версия 2.10 перехватывает GetAddrInfoW () и разрешает все вызовы к ней с использованием UDP-пакетов до 8.8.4.4:53, если это не удается, то возвращает к исходному API GetAddrInfoW ().

Новые механизмы персистентности

В этом разделе мы расскажем о двух модулях, которые появились в этом году. Мы считаем, что они предназначены для предотвращения демонтажа, наподобие нынешней операции, и с этой целью обеспечивают для ботмастера сторонний канал коммуникаций. Это поведение было описано в статье по ссылке 4 в разделе «Источники».

Первый модуль представляет собой USB spreader (утилиту для распространения вредоносного ПО по флэшкам). Второй – выполняет бесфайловую атаку с помощью загрузчика, который хранится в реестре и запускается скриптом PowerShell при запуске.

USB spreader – Win32/Bundpil.CS

Модуль позволяет перехватывать функции DNS API, пытается распространяться через съемные носители и использует DGA (алгоритм генерации доменов) для загрузки дополнительных данных.

Один процесс осуществляет сканирование на предмет подключенных съемных носителей и, обнаружив искомое, устанавливает на нем копию вредоносной программы.

Вторая функция модуля – перехват DNS API и замена определенных доменов закодированным. Например, один изученный образец перенаправлял все запросы на эти старые домены Wauchos:

- designfuture.ru
- disorderstatus.ru
- atomictrivia.ru
- differentia.ru

на gvaq70s7he.ru.

В модуле также есть компонент DGA, который пытается подключиться к автоматически генерируемым доменам для загрузки в скомпрометированную систему дополнительных данных. Псевдокод алгоритма DGA можно найти на нашей странице на github. URL-адреса, которых он пытается достичь, соответствуют следующим шаблонам:

- <dga_domain>.ru/mod
- ww1.<dga_domain>.ru/1
- ww2.<dga_domain>.ru/2

Нам удалось загрузить бинарный блоб из схемы с DGA. То, что мы получили, было зашифрованным блобом и начиналось с «MZ». Модуль удалит эти два байта и сохранит блоб в реестре Windows.

Основной бот Wauchos расшифровывает полезную нагрузку, зашифрованную с RC4, распаковывает ее с aPLib и загружает как обычный модуль. Обратите внимание, что для этого процесса используются те же ключи RC4, что и для шифрования модулей. Двоичный файл, полученный таким образом, – обновленная версия USB spreader. Мы предполагаем, что через перехват DNS ботмастер может восстановить управление ботами, загрузив свежую версию модуля с контролируемого домена, и потом перенаправлять жестко закодированные домены в основном на Wauchos.

Загрузчик

Последний модуль – маленький загрузчик, использующий DGA для доступа к следующим URL-адресам, в зависимости от версии:

- <dga_domain>.ru/ld.so
- <dga_domain>.ru/last.so
- <dga_domain>.ru/nonc.so

Модуль используется для загрузки бинарного блоба, который он хранит в реестре. Блоб можно расшифровать с помощью ключа RC4, содержащегося в основной полезной нагрузке Wauchos.

Один из вариантов вредоносного ПО, загружаемый этим модулем, – еще один загрузчик, детектируемый как TrojanDownloader.Small.AHI. Вредоносная программа представляет интерес, поскольку ее единственная задача – загрузить обновленную версию модуля загрузчика и сохранить ее в реестре в зашифрованном виде, но с одним нюансом.

Он также добавляет ключ запуска со скриптом PowerShell, который расшифровывает и выполняет зашифрованный двоичный файл из раздела реестра после каждого запуска компьютера. Прямо сейчас двоичный файл просто обновляется. Тем не менее, его DGA можно использовать как вторичный канал связи для установки новой полезной нагрузки и восстановления контроля над ботами, если кто-либо попытается его перехватить. Процесс представлен на рисунке 7.

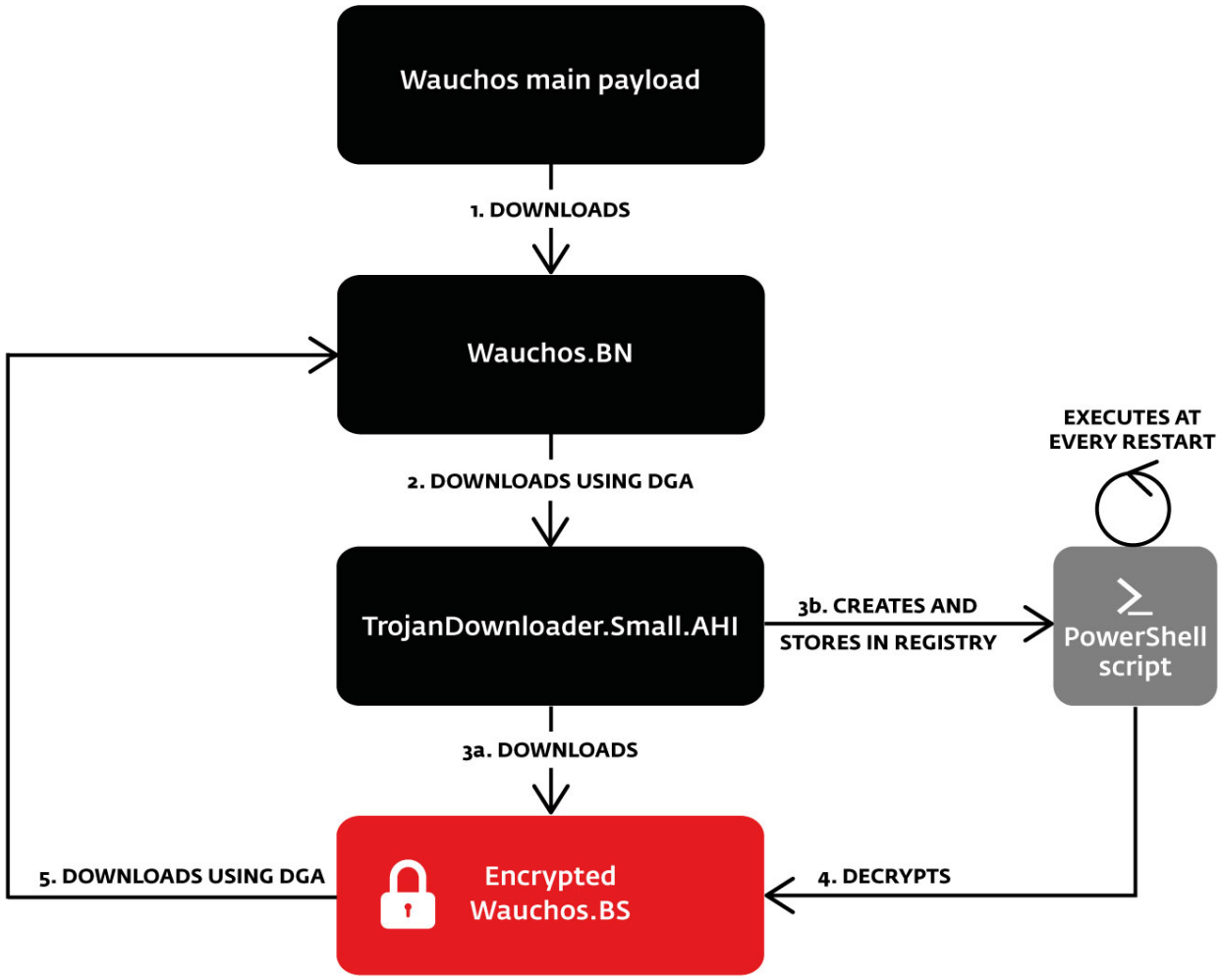

Рисунок 7. Схема работы модуля загрузчика

Интересно отметить, что мы наблюдали загрузку Necurs.B через DGA и этот модуль. Тем не менее, в большинстве загрузок в систему устанавливался Win32/TrojanDownloader.Small.AHI. Фактически эта программа детектировалась многократно, согласно нашей облачной статистике. Наибольшая активность модуля отмечена с помощью нашего поискового бота в августе 2016 года, после чего была сведена к нулю. Неизвестно, были ли мы внесены в черный список, либо операторы малвари просто тестировали функцию в течение короткого периода времени.

Заключение

Wauchos (Gamarue/Andromeda) – старый ботнет, обновляемый на протяжении нескольких лет. Специалисты ESET годами наблюдали за его инфраструктурой, равно как и за другими угрозами. Мониторинг важен для отслеживания любых изменений в поведении вредоносной программы, а также для последующей ликвидации.

Wauchos использует старые методы для компрометации новых систем. Пользователи должны соблюдать осторожность, открывая файлы на съемных носителях, а также файлы, полученные по электронной почте, в соцсетях или мессенджерах. Если вы считаете, что ваша система заражена Wauchos, используйте бесплатный инструмент для проверки и удаления малвари.

Информация о ботнете собиралась с помощью телеметрического сервиса ESET Threat Intelligence. Продукты ESET детектируют тысячи вариантов модулей Wauchos и другие семейства вредоносного ПО, распространяемые ботнетом.

Благодарим за помощь в исследовании Juraj Jánošík, Viktor Lucza, Filip Mazán, Zoltán Rusnák и Richard Vida.

Хеши

SHA-1	Детектирование
CC9AC16847427CC15909A60B130CB7E67D2D3804	Win32/TrojanDownloader.Wauchos.B
BCD45398983EB58B33294DFE852B57B1ADD5117E	Win32/TrojanDownloader.Wauchos.AK
6FA5E48AD60B53761A42725A4B9EC12B85963F90	Win32/TrojanDownloader.Small.AHI
6D5051580DA73570944BBE79A9EA7F2E4D006699	Win32/TrojanDownloader.Wauchos.O

Источники

1. https://blog.fortinet.com/2014/04/16/a-good-look-at-the-Andromeda-botnet
2. https://blog.avast.com/Andromeda-under-the-microscope
3. http://eternal-todo.com/blog/Andromeda-gamarue-loves-json
4. http://blog.trendmicro.com/trendlabs-security-intelligence/usb-malware-implicated-fileless-attacks