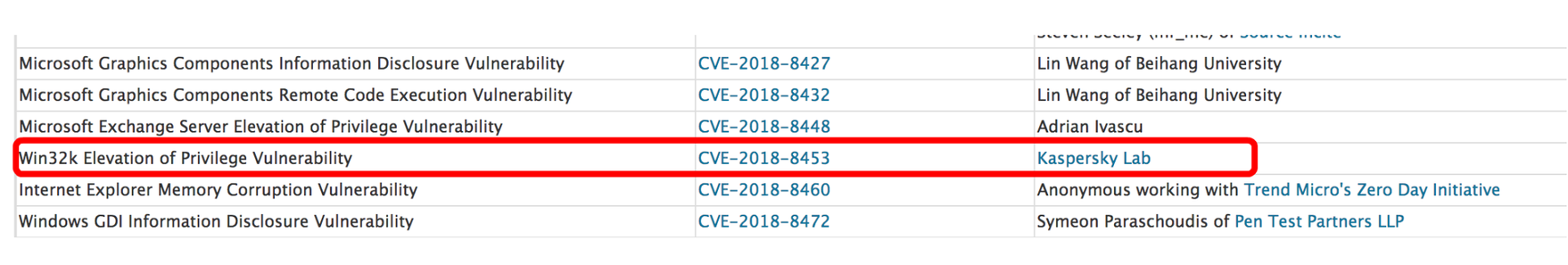
ИССЛЕДОВАНИЕ

Эксплойт нулевого дня (CVE-2018-8453) в целевых атаках

AMR - Октябрь 11, 2018. 15:17

На днях компания Microsoft опубликовала бюллетень безопасности, в который среди прочего вошел патч для CVE-2018-8453. Это уязвимость в win32k.sys, обнаруженная нашими технологиями еще в августе. 17 августа 2018 года мы сообщили о ней представителям Microsoft. В компании подтвердили наличие уязвимости и присвоили ей номер CVE-2018-8453.



Microsoft Graphics Components Information Disclosure Vulnerability	CVE-2018-8427	Lin Wang of Beihang University
Microsoft Graphics Components Remote Code Execution Vulnerability	CVE-2018-8432	Lin Wang of Beihang University
Microsoft Exchange Server Elevation of Privilege Vulnerability	CVE-2018-8448	Adrian Ivascu
Win32k Elevation of Privilege Vulnerability	CVE-2018-8453	Kaspersky Lab
Internet Explorer Memory Corruption Vulnerability	CVE-2018-8460	Anonymous working with Trend Micro's Zero Day Initiative
Windows GDI Information Disclosure Vulnerability	CVE-2018-8472	Symeon Paraschoudis of Pen Test Partners LLP

В августе 2018 года наша «Автоматическая защита от эксплойтов» (AEP) засекла попытку эксплуатации некой уязвимости в операционной системе Microsoft Windows. В ходе дальнейшего анализа была обнаружена брешь нулевого дня в win32k.sys. Эксплойт выполняла первая ступень установщика вредоносного ПО, чтобы получить привилегии, необходимые для закрепления в системе жертвы. Код эксплойта был явно написан со знанием дела, причем целью его авторов было охватить как можно больше сборок MS Windows, включая MS Windows 10 RS4.

До сих пор мы засекли ограниченное число атак с использованием этой уязвимости. Все жертвы находятся на Ближнем Востоке.

Продукты «Лаборатории Касперского» обнаруживают этот эксплойт проактивно благодаря следующим технологиям:

1. Модуль поведенческого анализа и «Автоматическая защита от эксплойтов» (AEP) для рабочих станций
2. Продвинутый модуль «песочницы» и защиты от вредоносного ПО для платформы Kaspersky Anti Targeted Attack (KATA)

Продукты «Лаборатории Касперского» детектируют объекты, обнаруженные в рамках этой кампании, со следующими вердиктами:

- HEUR:Exploit.Win32.Generic
- HEUR:Trojan.Win32.Generic
- PDM:Exploit.Win32.Generic

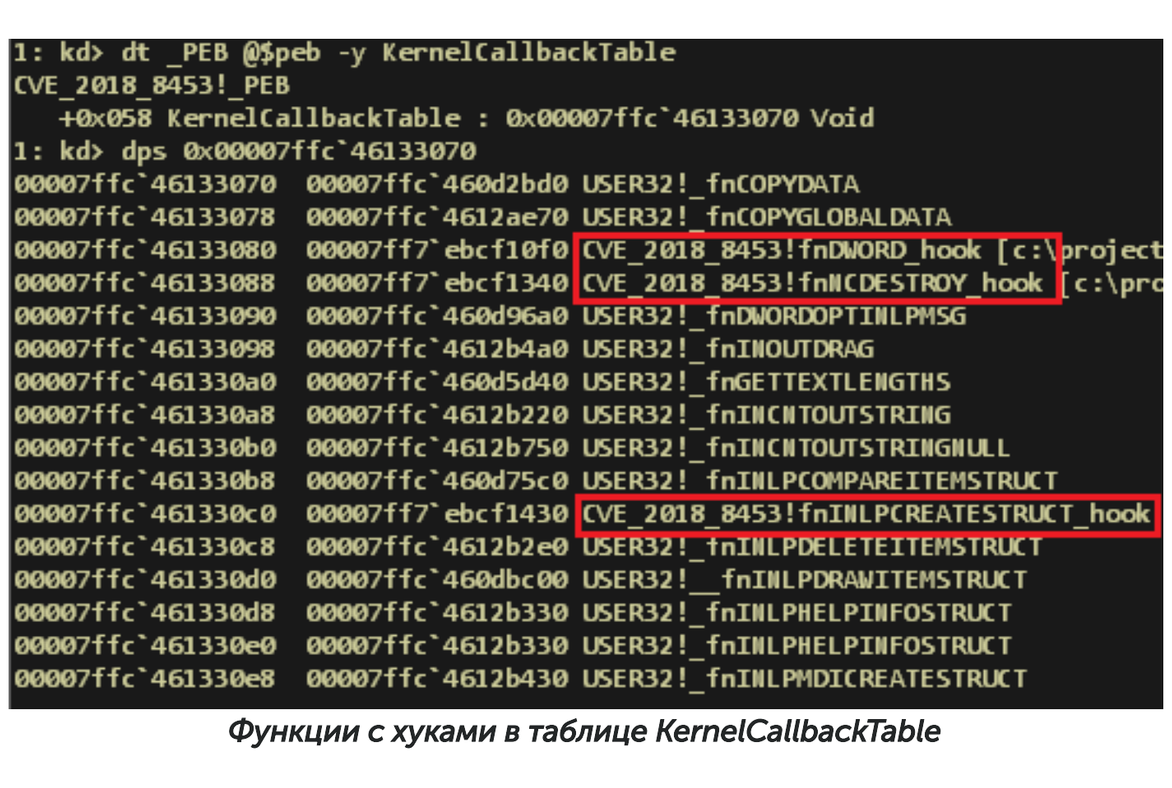
Дополнительная информация об атаке доступна клиентам, подписавшимся на аналитические отчеты «Лаборатории Касперского». Связаться с нами: intelreports@kaspersky.com

Технические подробности

CVE-2018-8453 относится к типу уязвимостей Use-After-Free и находится в коде обработчика системного вызова **win32kfull!xxxDestroyWindow**. Она напоминает более старую уязвимость — CVE-2017-0263. Изначально, в 2017 году, CVE-2017-0263 вместе с эксплойтом PostScript использовала APT-группировка Sofacy.

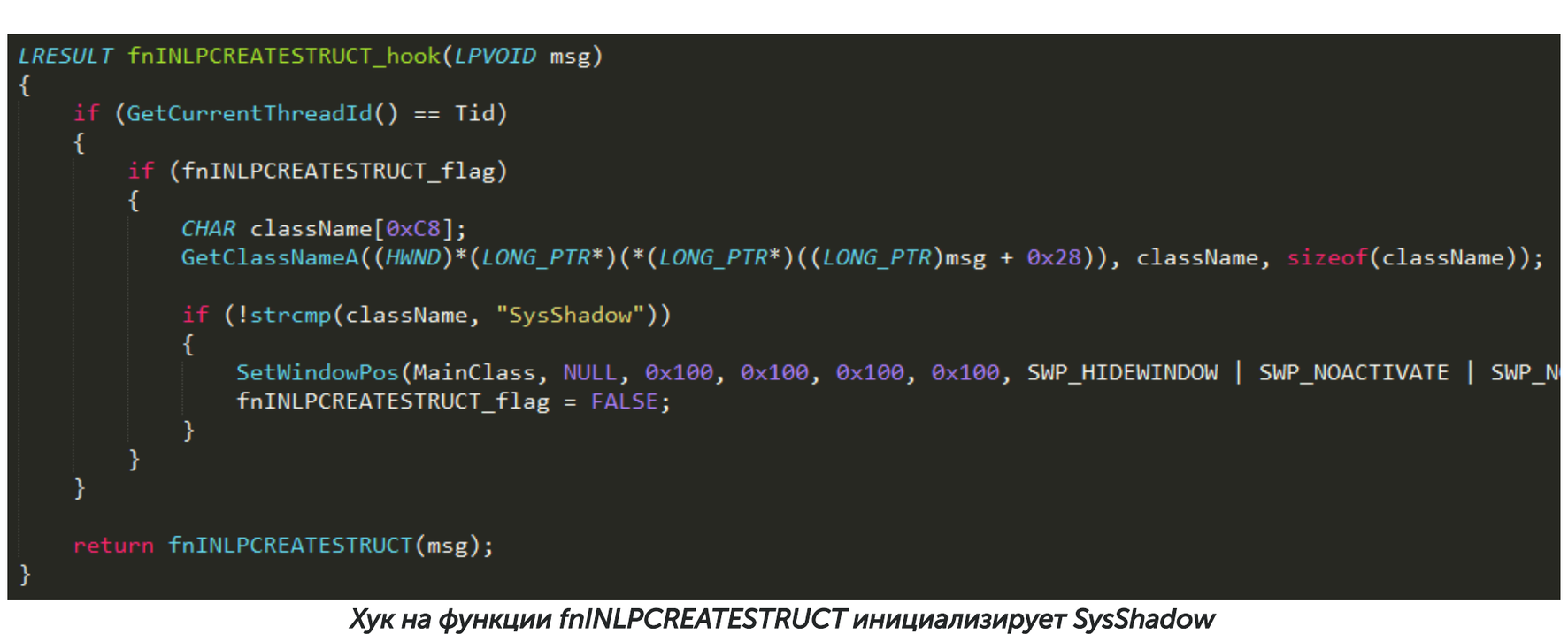
Мы провели полную обратную разработку полученного в образца эксплойта, написав на основе его анализа полноценный PoC.

Эксплуатация уязвимости зависит от последовательности событий, которые запускаются срабатыванием хуков, установленных на трех функциях обратного вызова для пользовательского режима — **fnDWORD**, **fnNCDESTROY** и **fnINLPCREATESTRUCT**. Эксплойт ставит эти хуки путем замены указателей функции в таблице **KernelCallbackTable**.



Функции с хуками в таблице KernelCallbackTable

Внутри хука **fnINLPCREATESTRUCT** эксплойт задает начальную позицию окна класса *SysShadow* в явном виде для его инициализации.



Хук на функции fnINLPCREATESTRUCT инициализирует SysShadow

Во время обработки сообщения **WM_LBUTTONDOWN** хук **fnDWORD** применяет функцию **DestroyWindow** к родительскому элементу, в результате чего окно помечается как свободное, соответственно, сборщик мусора освобождает отведенную под него память.

Однако во время выполнения функции закрытия окна **DestroyWindow** срабатывает пользовательский хук на **fnNCDESTROY**. С ним и связана основная проблема. В коде хука выполняется системный вызов **NtUserSetWindowFNID**, который содержит ошибочную логику, позволяющую изменять статус окна *fnid* без должной проверки того, был ли он предварительно установлен как**FNID_FREED**.

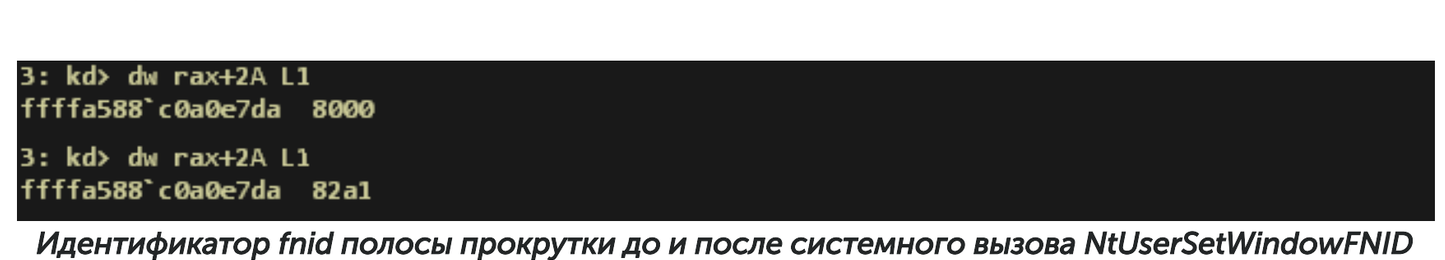
Уязвимый код внутри NtUserSetWindowFNID

Статус окна *fnid* расположен по смещению 0x02a в структуре tagWND.

```
kd> dt win32k!tagWND
…
+0x02a fnid : Uint2B
```

При первом создании полосы прокрутки идентификатор получает значение **FNID_SCROLLBAR** (0x029A).

На следующем рисунке показаны значения *fnid* до и после выполнения системного вызова **NtUserSetWindowFNID**.



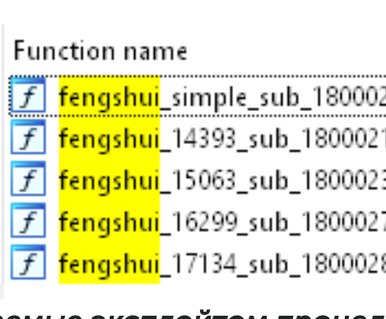
Идентификатор fnid полосы прокрутки до и после системного вызова NtUserSetWindowFNID

Проверить смысл нового значения *fnid* можно, сопоставив его с исходным кодом ReactOS.

```
/* FNID для NtUserSetWindowFNID, NtUserMessageCall */
#define FNID_SCROLLBAR 0x029A
…
#define FNID_BUTTON 0x02A1
…
#define FNID_FREED 0x8000 /* окно получает статус свободного */
```

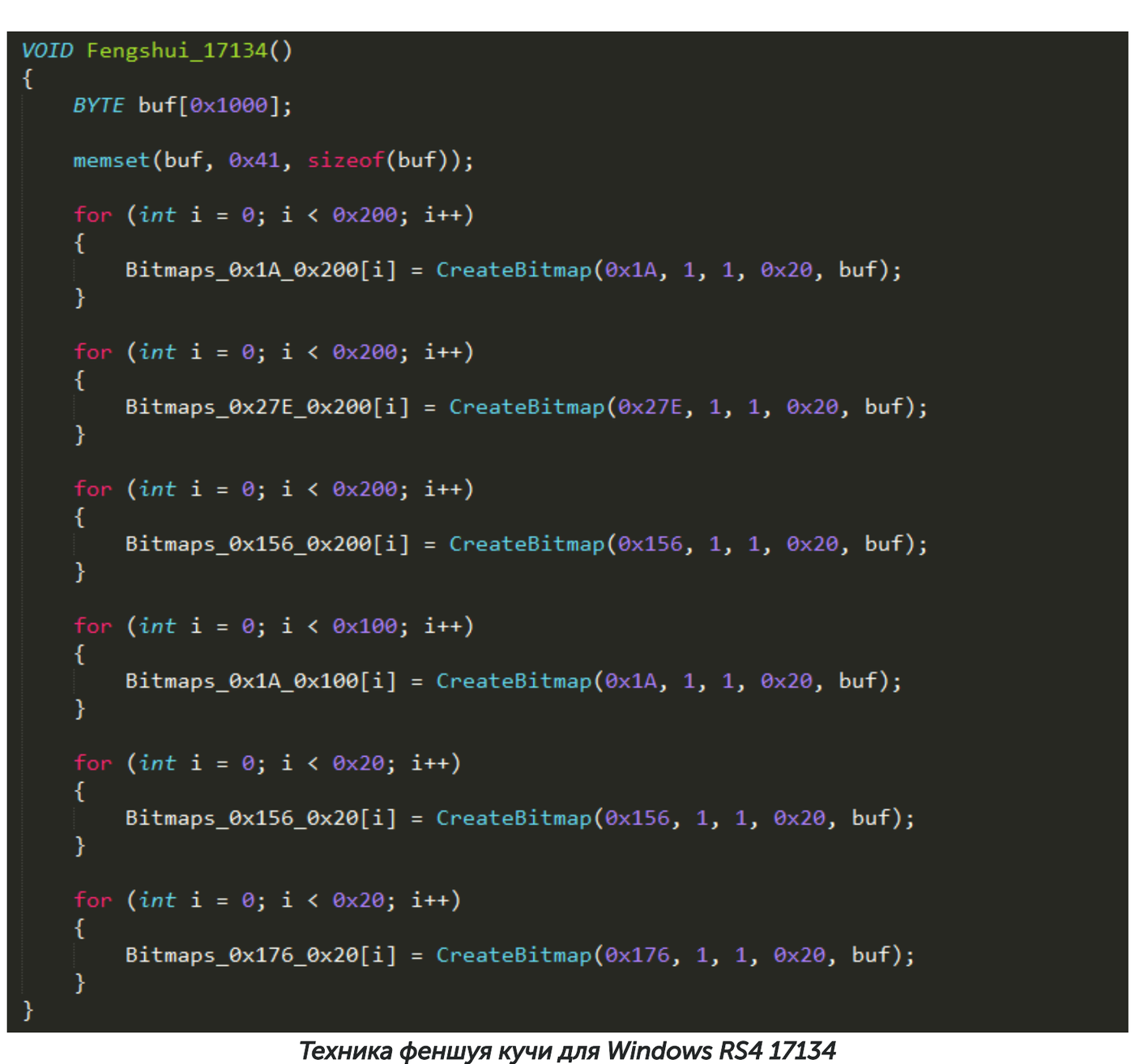
В результате описанного выше действия первая полоса прокрутки уничтожается, однако система все еще сохраняет ссылку на класс *SysShadow*, поскольку полоса прокрутки обозначена уже не как **FNID_FREED**, а как **FNID_BUTTON**.

Чтобы вернуть освобожденный пул памяти, эксплойт содержит множество тактик «феншуя». Процедура распыления кучи (heap spray) зависит от версии Windows, в которой действует эксплойт. Поскольку код зловреда рассчитан на как можно большее число версий операционной системы, в нем предусмотрено пять разных функций для атаки типа heap spray.



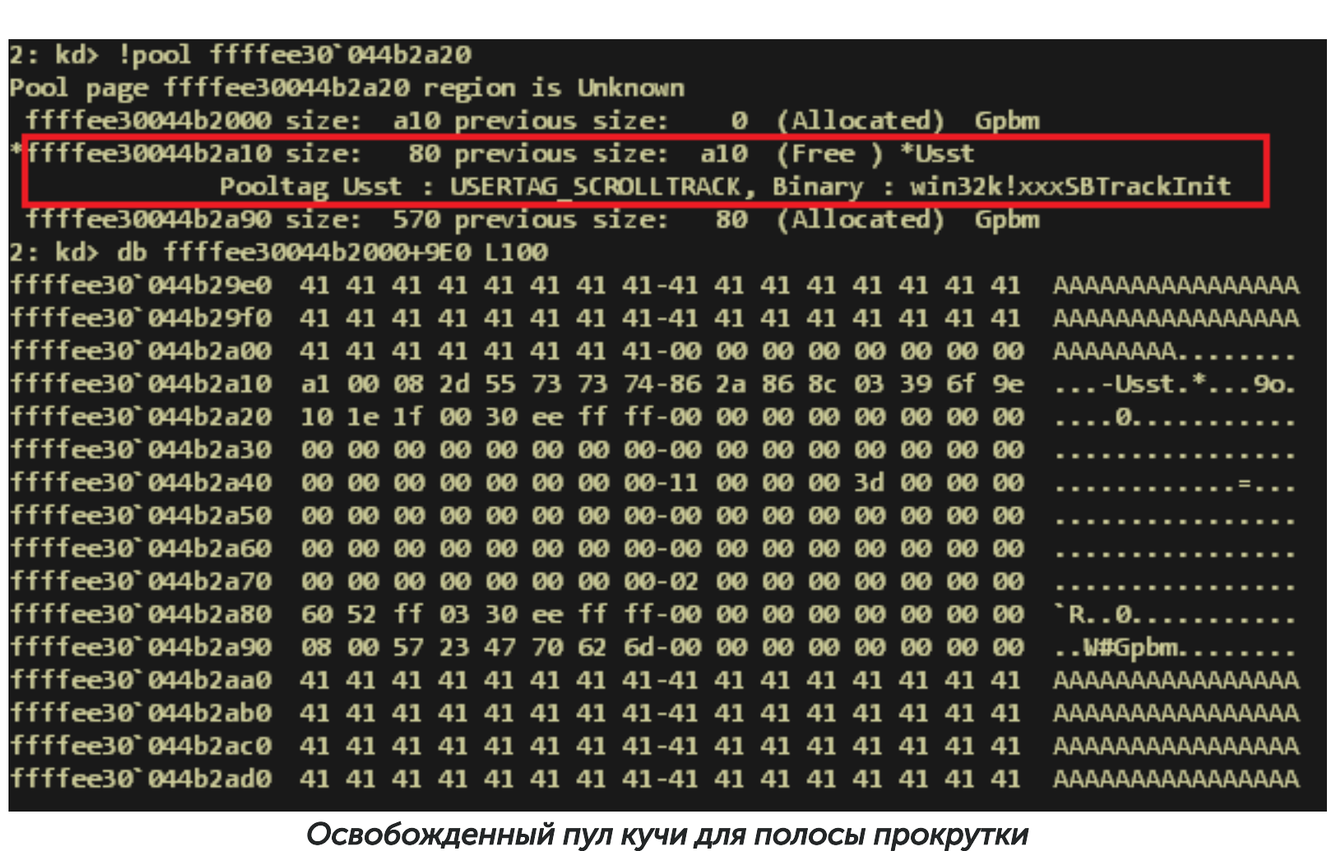
Поддерживаемые эксплойтом процедуры распыления кучи

Тактика распыления для самой новой из поддерживаемых эксплойтом версий ОС (Windows 10 RS4) довольно сложна. В ее рамках ядро перегружается растровыми изображениями разного размера. Это необходимо для того, чтобы истощить возможности распределения памяти в аллокаторе кучи и в конечном итоге обойти предусмотренные в операционной системе функции безопасности направленные на рандомизацию аллокаций памяти, значительно доработанных в последних сборках Windows.



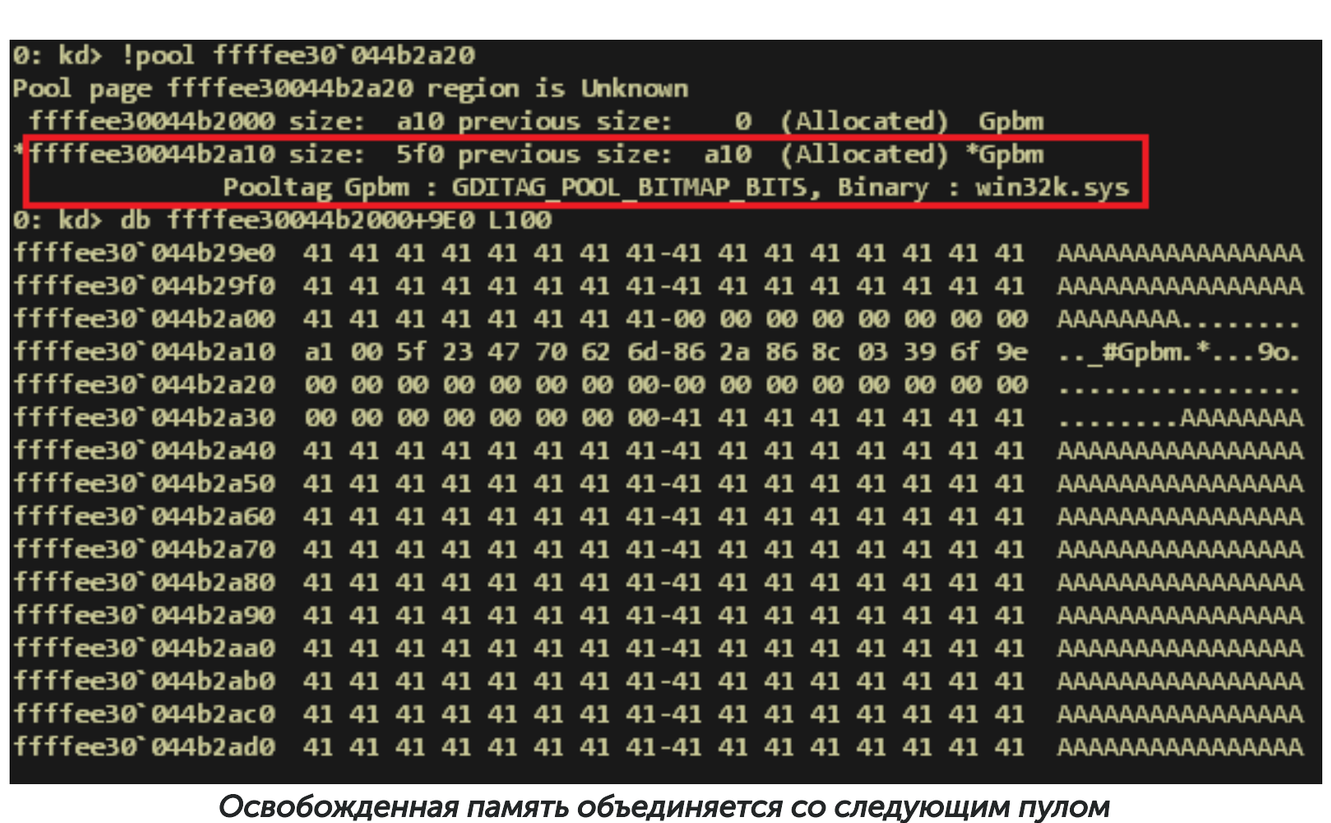
Техника феншуя кучи для Windows RS4 17134

Это приводит к следующей организации памяти, где **USERTAG_SCROLLTRACK** —освобожденный пул памяти.



Освобожденный пул кучи для полосы прокрутки

При назначении другой полосы прокрутки ссылка в памяти на класс *SysShadow* используется повторно, но ее содержимое контролируется атакующим, поскольку освобожденные пулы *Usst (ffffee30044b2a10)* и *Gpbm* (*ffffee30044b2a90)* были слиты в единый блок.



Освобожденная память объединяется со следующим пулом

Это позволяет исполнять произвольные команды чтения и записи ядра с помощью примитивов GDI Bitmap даже в последних версиях Windows.

После успешного исполнения эксплойта в дело вступает слегка модифицированная полезная нагрузка для кражи токена, которая подменяет значение токена текущего процесса произвольным значением из структуры SYSTEM EPROCESS.

Модифицированная полезная нагрузка для кражи токена процесса

До сих пор мы наблюдали использование этого эксплойта в небольшом количестве целевых атак, в которых эксплойт был упакован в установщик вредоносного ПО. Для установки полезной нагрузки установщику требуются системные привилегии. Сама полезная нагрузка представляет собой сложный имплант, с помощью которого атакующие получают постоянный доступ к машине жертвы. Вот некоторые из его основных характеристик:

- Он шифрует главную полезную нагрузку по алгоритму AES-256-CBC с хэшем SHA-1 на основе SMBIOS UUID. Это делает невозможной расшифровку полезной нагрузки на других машинах, если идентификатор SMBIOS UUID неизвестен.
- Для связи с командными серверами зловред использует Microsoft BITS (Background Intelligent Transfer Service), что само по себе достаточно необычно.
- Основная полезная нагрузка хранится в произвольно поименованном файле на диске. Загрузчик содержит хэш с именем файла и ищет полезную нагрузку, сравнивая хэш имени файла со всеми файлами в директории Windows.

Дополнительные подробности о зловреде и стоящей за ним APT-группировке доступны подписчикам аналитических отчетов «Лаборатории Касперского». Связаться с нами: intelreports@kaspersky.com

Жертвы

Атака выглядит очень целенаправленной: пока, по данным нашей телеметрии, известно около десятка жертв на Ближнем Востоке.

Кто виноват

В процессе расследования мы обнаружили, что атакующие использовали PowerShell-бэкдор, который ранее применялся только APT FruityArmor. Кроме того, командные серверы, задействованные в новой волне заражений, частично совпадают с серверами, засветившимися в предыдущих кампаниях FruityArmor. Это позволяет нам довольно уверенно предполагать, что именно группировка FruityArmor несет ответственность за атаки через CVE-2018-8453.

Заключение

Несмотря на то, что использование эксплойтов нулевого дня сегодня, похоже, встречается чаще, чем раньше, это уже второй известный нам случай, когда FruityArmor обратилась к этому способу распространения вредоносного ПО. Сложность методики и самой полезной нагрузки говорит о серьезных ресурсах и навыках этой APT-группировки.

До сих пор кампания оставалась точечной: нападению подверглось всего несколько жертв на Ближнем Востоке. Вероятно, эти лица представляют интерес для атакующих. Однако четко определить профиль жертв по такой малой выборке невозможно.

Хотя активность FruityArmor в последние два года постепенно растет, узконаправленные целевые атаки помогают группировке держаться в тени.

Приложение I — Индикаторы заражения

Домены:

weekendstrips[.]net
shelves-design[.]com

APT | MICROSOFT WINDOWS | PROOF-OF-CONCEPT | УЯЗВИМОСТИ 0-DAY | УЯЗВИМОСТИ И ЭКСПЛОЙТЫ

Share post on:

Публикации на схожие темы

ДОБАВИТЬ КОММЕНТАРИЙ

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Enter your comment here

Имя *

E-mail *

Save my name, email, and website in this browser for the next time I comment.

Сообщите мне, когда появятся новые комментарии.

SUBMIT

Я не робот
reCAPTCHA
Конфиденциальность - Условия использования

В ЭТОЙ КАТЕГОРИИ

Пиратская матрешка
Грабитель банкоматов WinPot
Razy в поисках криптовалюты
От зловреда до майнера: эволюция «USB-угроз»
Новые тренды в мире IoT-угроз