Кампания EastWind: новые атаки CloudSorcerer на госорганизации в России

GReAT ⋮⋮ 8/8/2024

Авторы

- Expert GReAT

В конце июля 2024 года мы выявили активную серию целевых кибератак на десятки компьютеров российских государственных организаций и IT-компаний. В ходе этих атак злоумышленники заражали устройства при помощи фишинговых писем с вложениями, содержащими вредоносные файлы ярлыков. При нажатии на ярлыки происходила установка вредоносного ПО, которое в дальнейшем получало команды через облачное хранилище Dropbox. С помощью этого ПО злоумышленники загружали на зараженные компьютеры дополнительных троянцев, в частности инструменты, используемые кибергруппировкой APT31, а также обновленный бэкдор CloudSorcerer. Мы назвали эту кампанию EastWind.

Ниже приводим наиболее интересные факты об имплантах, использованных в ходе этой кампании:

- Троянская программа, загружаемая злоумышленниками из облачного хранилища Dropbox, использовалась группировкой APT31 как минимум с 2021 года. Мы назвали ее GrewApacha.
- Бэкдор CloudSorcerer, который мы описали в начале июля 2024 года, был обновлен после нашей публикации. Теперь в нем в качестве первоначального командного сервера

используются профили в блоге «Живой Журнал» и на сайте вопросов и ответов Quora.
- В атаках используется ранее неизвестный имплант с функциональностью классического бэкдора, который мы назвали PlugY. Он загружается через бэкдор CloudSorcerer, обладает обширным набором команд и поддерживает три различных протокола общения с командным центром. Кроме того, его код схож с кодом бэкдора DRBControl (также известен как Clambling), который несколько ИБ-компаний приписывают группировке APT27.

Техническая информация

Как мы уже упомянули, атакующие использовали целевой фишинг для первоначального заражения. Злоумышленники отправляли на электронные адреса, принадлежащие затронутым организациям, вредоносные письма с RAR-архивами во вложении. Архивы имели следующие названия:

- инициативная группа из Черниговского района Приморского края.rar;
- вх.rar.

Они содержали следующие файлы:

- Папку .con, в которой хранились:
  - Легитимный документ-приманка 1.docx
  - Легитимный файл desktop.exe
  - Вредоносный файл VERSION.dll
- Вредоносный ярлык (примеры названий: обращение черниговский район.docx.lnk, вх. от 10_04_24.docx.lnk)

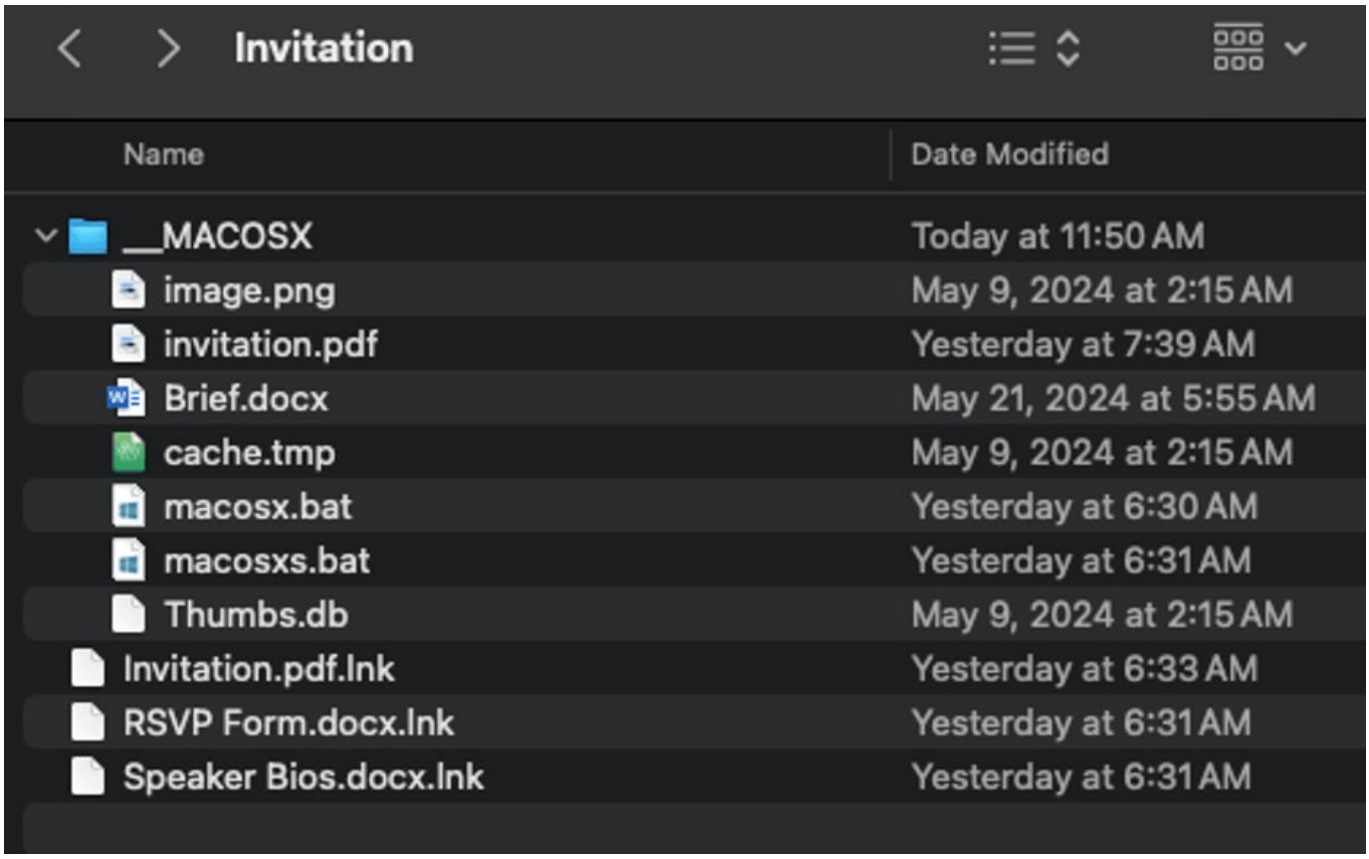
При нажатии на вредоносный ярлык выполнялась следующая шелл-команда:

PowerShell

```
C:\Windows\System32\cmd.exe /c .con\1.docx & echo F | move .con\doc
%public%\Downloads\desktop.exe & move .con\docs %public%\Downloads\VERSION.dll &
start /b %public%\Downloads\desktop.exe && exit
```

Она открывает на компьютере документ, содержащийся в архиве, копирует файлы desktop.exe и VERSION.dll в папку C:\Users\Public\Downloads, а затем запускает файл desktop.exe.

Примечательно то, что аналогичный метод заражения применялся в атаке на одну организацию в США с использованием бэкдора CloudSorcerer — об этом сообщила компания Proofpoint в июле 2024 года:



Содержимое вредоносного архива, использованного при атаке на организацию в США

Библиотека VERSION.dll — бэкдор, использующий Dropbox

Злоумышленники используют классическую технику DLL sideloading: при запуске файла desktop.exe в соответствующий ему процесс загружается вредоносная библиотека VERSION.dll:

MD5	1f5c0e926e548de43e0039858de533fc
SHA1	426bbf43f783292743c9965a7631329d77a51b61
SHA256	668f61df2958f30c6a0f1356463e14069b3435fb4e8417a948b6738f5f340dd9
Размер файла	9,82 МБ

Эта библиотека представляет собой бэкдор, упакованный при помощи инструмента VMProtect. При запуске он пытается связаться с облачным сервисом Dropbox при помощи жестко закодированного токена аутентификации. Подключившись к облаку, бэкдор считывает команды, которые необходимо исполнить, из содержащегося в хранилище файла <имя компьютера>/a.psd. Всего бэкдор поддерживает пять команд со следующими именами:

- DIR
- EXEC
- SLEEP
- UPLOAD
- DOWNLOAD

Результаты выполнения этих команд загружаются в облачное хранилище в файл <имя компьютера>/b.psd.

GrewApacha, RAT-троянец группировки APT31 из 2021

Злоумышленники использовали вышеописанный бэкдор, чтобы собирать информацию о зараженных компьютерах и устанавливать на них дополнительное вредоносное ПО. В частности, на одном из компьютеров мы наблюдали загрузку следующих файлов в директорию C:\ProgramData\USOShared\Logs\User:

- msedgeupdate.exe — легитимный исполняемый файл, подписанный корпорацией Microsoft;
- msedgeupdate.dll — вредоносная библиотека;
- wd — файл с зашифрованной полезной нагрузкой.

Когда злоумышленники запускали файл msedgeupdate.exe, в его процесс методом DLL sideloading загружалась вредоносная библиотека msedgeupdate.dll:

MD5	f6245f64eaad550fd292cfb1e23f0867
SHA1	fccdc059f92f3e08325208f91d4e6c08ae646a78
SHA256	e2f87428a855ebc0cda614c6b97e5e0d65d9ddcd3708fd869c073943ecdde1c0
Размер файла	9 МБ

Хотя набор из трех файлов напоминает «троицу», характерную для атак с использованием PlugX, анализ этих файлов показал, что они являются RAT-троянцем группировки APT31, который ранее уже описывали в 2021 и 2023 годах. Мы назвали этот троянец GrewApacha.
Поведение загрузчика (msedgeupdate.dll) спустя год после последней публикации о нем не изменилось. Как и раньше, он расшифровывает хранящуюся на диске полезную нагрузку при помощи XOR-ключа 13 18 4F 29 0F и загружает ее в процесс dllhost.exe.

Сам RAT-троянец также мало отличается от того, что был описан в 2023 году. Однако в его работу злоумышленники внесли небольшие изменения: например, в новой версии используется два сервера управления вместо одного. В качестве начального сервера злоумышленники задействуют биографию профиля в сервисе GitHub — в ней содержится закодированная алгоритмом Base64 строка, которую считывает троянец.

Glory-A-McNair

Follow

YTc1YzI1Y2ZmNTg4NDFjfHltaH1sJ3p9f
G1gZmJoenlse3picCdqZmQAPT06ADs=
YjVhZDI1MGUzNjJmMThkZmI

Профиль созданного атакующими пользователя на GitHub

Извлеченную из профиля GitHub строку зловред декодирует, а затем расшифровывает однобайтовым алгоритмом XOR с ключом 0x09, тем самым получая адрес основного сервера управления (для скриншота выше — update.studiokaspersky[.]com).

Новая версия бэкдора CloudSorcerer

Мы также выяснили, что помимо запуска описанного выше троянца GrewApacha злоумышленники загружали на зараженные компьютеры бэкдор CloudSorcerer. Чтобы это сделать, они сначала загружали на устройство и запускали утилиту с именем GetKey.exe, упакованную протектором VMProtect.

MD5	bed245d61b4928f6d6533900484cafc5
SHA1	e1cf6334610e0afc01e5de689e33190d0c17ccd4
SHA256	5071022aaa19d243c9d659e78ff149fe0398cf7d9319fd33f718d8e46658e41c
Размер файла	51 КБ

Утилита получает четырехбайтовое число (значение функции GetTickCount() в момент исполнения), шифрует его при помощи функции CryptProtectData, а затем выводит число и его

шифротекст. Скриншот кода функции main этой утилиты представлен ниже:

```
  pDataIn.cbData = 0;
  pDataIn.pbData = 0;
  pDataOut.cbData = 0;
  pDataOut.pbData = 0;
  TickCount = GetTickCount();
  for ( i = 0; i < 4; ++i )
    printf("%02X", *((unsigned __int8 *)&TickCount + i));
  pDataIn.pbData = (BYTE *)&TickCount;
  pDataIn.cbData = 4;
  if ( CryptProtectData(&pDataIn, 0, 0, 0, 0, 4u, &pDataOut) )
  {
    for ( j = 0; j < pDataOut.cbData; ++j )
      printf("%02X", pDataOut.pbData[j]);
    printf("\n");
    LocalFree(pDataOut.pbData);
  }
  return 0;
}
```

Результаты работы утилиты злоумышленники использовали на своей стороне в качестве уникального ключа для шифрования файла полезной нагрузки, который можно расшифровать только на компьютере жертвы, после чего загружали на зараженные компьютеры следующие файлы:

- Переименованное (пример имени: WinDRMs.exe) легитимное приложение dbgsrv.exe, подписанное корпорацией Microsoft.
- Вредоносная библиотека dbgeng.dll.
- Файл с расширением .ini, содержащий зашифрованную полезную нагрузку. Имя этого файла различалось на разных инфицированных машинах.

Так же как в случае с GrewApacha, описанным выше, этот набор напоминает «троицу», характерную для атак с использованием PlugX.

В большинстве случаев злоумышленники загружали файлы в одну из поддиректорий каталога C:\ProgramData, например C:\ProgramData\Microsoft\DRM. Далее они при помощи планировщика заданий настраивали автозапуск переименованного приложения dbgsrv.exe при загрузке операционной системы. Для этого они использовали утилиту schtasks (пример команды, которая использовалась для ее вызова: schtasks /create /RL HIGHEST /F /tn \Microsoft\Windows\DRM\DRMserver /tr "C:\ProgramData\Microsoft\DRM\WinDRMs.exe -t run" /sc onstart /RU SYSTEM").

При запуске переименованного приложения в его процесс загружалась вредоносная библиотека dbgeng.dll — опять же, при помощи техники DLL sideloading.

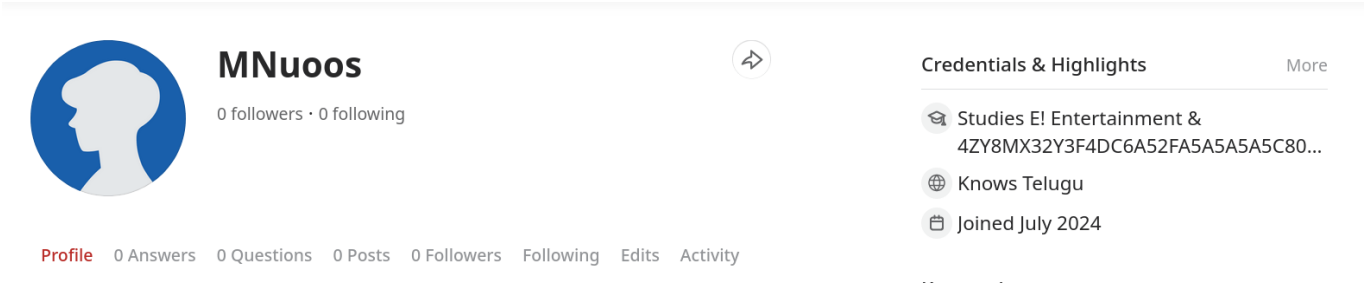
MD5	d0f7745c80baf342cd218cf4f592ea00
SHA1	c0e4dbaffd0b81b5688ae8e58922cdaa97c8de25
SHA256	bd747692ab5db013cd4c4cb8ea9cafa7577c95bf41aa2629a7fea875f6dcbc41
Размер файла	1,11 МБ

Библиотека, в свою очередь, читала упомянутый выше .ini-файл, который содержит:

- Шифротекст четырехбайтового числа, сгенерированного и зашифрованного утилитой GetKey.exe.
- PE-файл, сжатый алгоритмом LZNT1 и зашифрованный при помощи XOR с использованием четырехбайтового числа в качестве ключа.

Соответственно, в ходе работы библиотека сначала при помощи функции CryptUnprotectData расшифровывала четырехбайтовое число, использовала его для дешифровки файла .ini, а затем загружала расшифрованный файл в память текущего процесса.

Анализ расшифрованных файлов .ini показал, что они представляют собой обновленные версии бэкдора CloudSorcerer. После того как мы публично описали этот бэкдор в начале июля 2024 года, злоумышленники внесли в него изменения: в новой версии CloudSorcerer в качестве первоначального командного сервера используются страницы профилей в русскоязычной социальной сети «Живой Журнал» и на сайте вопросов и ответов Quora:



Как и в случае с прошлыми версиями CloudSorcerer, в биографиях профилей содержится зашифрованный токен аутентификации для взаимодействия с облачным сервисом.

Имплант PlugY, схожий с инструментами группировки APT27

Проанализировав активность, наблюдаемую при исполнении новых образцов бэкдора CloudSorcerer, мы установили, что при помощи него злоумышленники загружали на зараженные компьютеры ранее неизвестный нам имплант. Он соединяется с сервером управления, используя один из трех методов:

- Протокол TCP
- Протокол UDP
- Named pipes

Набор команд, который этот имплант может принимать от сервера, довольно обширен: от работы с файлами и исполнения шелл-команд до наблюдения за действиями на экране и, логирования нажатий клавиатуры и слежения за буфером обмена.

Хотя анализ импланта еще продолжается, можно с высокой степенью уверенности утверждать, что при его разработке использовался код бэкдора DRBControl (также известен как Clambling). Этот бэкдор описали в 2020 году компании Trend Micro и Talent-Jump Technologies. Впоследствии компании Security Joes и Profero связали его с кибергруппировкой APT27. Также прослеживается его сходство с PlugX.

Кроме того, в ходе сравнения образцов импланта PlugY (пример MD5: faf1f7a32e3f7b08017a9150dccf511d) и бэкдора DRBControl (MD5: 67cfecf2d777f3a3ff1a09752f06a7f5) мы установили, что эти два троянца имеют идентичную архитектуру. Помимо этого, многие команды в них реализованы практически одинаково. Это видно из скриншотов ниже:

```
do
{
  *(a3 + 36i64 * v5 + 10) = GetDriveTypeW(v6);
  wcscpy_s((a3 + 36i64 * v5 + 14), 4ui64, v6);
  if ( !GetDiskFreeSpaceExW(v6, (a3 + 36i64 * v5 + 30), (a3 + 36i64 * v5 + 22), (a3 + 36i64 * v5 + 38)) )
  {
    *(a3 + 36i64 * v5 + 30) = 0i64;
    *(a3 + 36i64 * v5 + 22) = 0i64;
    *(a3 + 36i64 * v5 + 38) = 0i64;
  }
  v7 = -1i64;
  v8 = v6;
  do
  {
    if ( !v7 )
      break;
    v9 = *v8++ == 0;
    --v7;
  }
  while ( !v9 );
  ++v5;
  v6 += ~v7;
}
while ( *v6 );
v4 = a2;
}
```

```
do
{
  *v6 = GetDriveTypeW(v7);
  wcscpy_s((v6 + 4), 4ui64, v7);
  if ( !GetDiskFreeSpaceExW(v7, (v6 + 20), (v6 + 12), (v6 + 28)) )
  {
    *(v6 + 20) = 0i64;
    *(v6 + 12) = 0i64;
    *(v6 + 28) = 0i64;
  }
  v8 = -1i64;
  v9 = v7;
  do
  {
    if ( !v8 )
      break;
    v10 = *v9++ == 0;
    --v8;
  }
  while ( !v10 );
  v6 += 36i64;
  ++v5;
  v7 += ~v8;
}
while ( *v7 );
v4 = a2;
}
```

Код команды, реализующий получение информации о подключенных дисках в бэкдоре DRBControl (слева) и импланте (справа)

```
if ( hWnd != GetForegroundWindow() || dword_14002E018 >= 0x1F8 )
{
  ForegroundWindow = GetForegroundWindow();
  v1 = dword_14002E018;
  hWnd = ForegroundWindow;
  word_14002DE10[dword_14002E018] = 0;
  if ( v1 )
  {
    sub_1400077F8(&word_14002EB20, word_14002DE10, &unk_14002E910);
    ForegroundWindow = hWnd;
  }
  dword_14002E018 = 0;
  if ( !GetWindowTextW(ForegroundWindow, &word_14002EB20, 260) )
    word_14002EB20 = 0;
  GetWindowThreadProcessId(hWnd, &dwProcessId);
  v2 = OpenProcess(0x410u, 0, dwProcessId);
  if ( qword_14002E6C8 )
    qword_14002E6C8(v2, 0i64, &unk_14002E910, 260i64);
  else
    sub_1400044B0(v2, &unk_14002E910);
  if ( v2 )
    CloseHandle(v2);
}
```

```
if ( hWnd != GetForegroundWindow() || dword_1800248A0 >= 0x1F8 )
{
  ForegroundWindow = GetForegroundWindow();
  v1 = dword_1800248A0;
  hWnd = ForegroundWindow;
  word_1800248B0[dword_1800248A0] = 0;
  if ( v1 )
  {
    sub_180005C74(&String, word_1800248B0, &unk_180025310, 0i64);
    ForegroundWindow = hWnd;
  }
  dword_1800248A0 = 0;
  if ( !GetWindowTextW(ForegroundWindow, &String, 260) )
    String = 0;
  GetWindowThreadProcessId(hWnd, &dwProcessId);
  v2 = OpenProcess(0x410u, 0, dwProcessId);
  GetModuleFileNameExW(v2, 0i64, &unk_180025310, 260i64);
  if ( v2 )
    CloseHandle(v2);
}
```

Код команды, реализующий получение информации об активном окне в бэкдоре DRBControl (слева) и импланте (справа)

```
LastError = sub_14000B538(a1, hdc, DCW, DeviceCaps, cy, 32, 0i64);
if ( !LastError )
{
  LOWORD(hdcSrc) = 32;
  LastError = sub_14000B538(a1, v19, DCW, a3, cy, hdcSrc, 0i64);
  if ( !LastError )
  {
    LOWORD(hdcSrca) = 32;
    LastError = sub_14000B538(a1, v21, DCW, a3, a4, hdcSrca, 0i64);
    if ( !LastError )
    {
      LOWORD(hdcSrcb) = a5;
      LastError = sub_14000B538(a1, v22, DCW, a3, a4, hdcSrcb, a6);
      if ( !LastError )
      {
        LastError = sub_14000B6A8(a1);
        if ( !LastError )
        {
          if ( BitBlt(hdc[0], 0, 0, DeviceCaps, cy, DCW, 0, 0, 0x40CC0020u) )
          {
            GdiFlush();
            LastError = sub_14000AE58(a1, DeviceCaps, cy, a3, hdc[3], v20);
            if ( !LastError )
            {
              LastError = sub_14000B064(a1, a3, cy, a4, v20, v21[3]);
              if ( !LastError )
              {
                if ( BitBlt(v22[0], 0, 0, a3, a4, v21[0], 0, 0, 0x40CC0020u) )
                  memmove(a7, v22[3], 4 * a4 * ((a5 * a3 + 31) / 32));
```

```
LastError = sub_180008D1C(a1, hdc, DCW, DeviceCaps, cy, 32, 0i64);
if ( !LastError )
{
  LOWORD(hdcSrc) = 32;
  LastError = sub_180008D1C(a1, v19, DCW, a3, cy, hdcSrc, 0i64);
  if ( !LastError )
  {
    LOWORD(hdcSrca) = 32;
    LastError = sub_180008D1C(a1, v21, DCW, a3, a4, hdcSrca, 0i64);
    if ( !LastError )
    {
      LOWORD(hdcSrcb) = a5;
      LastError = sub_180008D1C(a1, v22, DCW, a3, a4, hdcSrcb, a6);
      if ( !LastError )
      {
        LastError = sub_180008E8C(a1);
        if ( !LastError )
        {
          if ( BitBlt(hdc[0], 0, 0, DeviceCaps, cy, DCW, 0, 0, 0x40CC0020u) )
          {
            GdiFlush();
            LastError = sub_18000863C(a1, DeviceCaps, cy, a3, hdc[3], v20);
            if ( !LastError )
            {
              LastError = sub_180008848(a1, a3, cy, a4, v20, v21[3]);
              if ( !LastError )
              {
                if ( BitBlt(v22[0], 0, 0, a3, a4, v21[0], 0, 0, 0x40CC0020u) )
                  memmove(a7, v22[3], 4 * a4 * ((a5 * a3 + 31) / 32));
```

Код команды, реализующий снятие скриншотов экрана в бэкдоре DRBControl (слева) и импланте (справа)

Следовательно, можно с высокой степенью уверенности утверждать, что в ходе разработки импланта использовался код, ранее наблюдаемый в атаках кибергруппировки APT27.

В ходе анализа импланта PlugY мы также заметили, что в нем используется примечательная вредоносная библиотека для соединения с сервером управления при помощи протокола UDP. Эту же библиотеку мы обнаружили в бэкдоре DRBControl, а также в нескольких образцах бэкдора PlugX, популярного среди китаеязычных кибергруппировок. Помимо DRBControl и PlugX, данная библиотека ни в каком другом вредоносном ПО замечена не была.

```
v13 = WSASocketA(a4, 2, 17, 0i64, 0, 1u);
*(CompletionKey + 16504) = v13;
if ( v13 == -1i64 )
  return WSAGetLastError();
vInBuffer = 0;
vOutBuffer = 0;
cbBytesReturned = 0;
*optval = 0x400000;
WSAIoctl(v13, 0x9800000C, &vInBuffer, 4u, &vOutBuffer, 4u, &cbBytesReturned, 0i64, 0i64);
setsockopt(*(CompletionKey + 16504), 0xFFFF, 4097, optval, 4);
setsockopt(*(CompletionKey + 16504), 0xFFFF, 4098, optval, 4);
setsockopt(*(CompletionKey + 16504), 0, 14, &vInBuffer, 4);
if ( !CreateIoCompletionPort(*(CompletionKey + 16504), a3, CompletionKey, 0) )
{
  LastError = GetLastError();
  v15 = sub_18000B7F0(0i64);
  sub_18000C030(v15, *a2);
  closesocket(*(CompletionKey + 16504));
  *(CompletionKey + 16504) = -1i64;
  return LastError;
}
```

Скриншот библиотеки, осуществляющей связь с сервером управления по протоколу UDP

Советы по обнаружению следов выявленной атаки

Выявленные в ходе атаки троянцы сильно отличаются друг от друга. Поэтому для обнаружения каждого из них необходимо использовать отдельный набор индикаторов компрометации.

Чтобы выявить работу бэкдора, распространяемого через электронную почту и использующего Dropbox для взаимодействия со злоумышленниками, можно провести поиск сравнительно больших по размеру (более 5 МБ) DLL-файлов, расположенных внутри директории C:\Users\Public. О работе этого бэкдора может также свидетельствовать регулярное обращение к облаку Dropbox в сетевом трафике.

Троянец GrewApacha группировки APT31 может быть обнаружен поиском неподписанного файла с именем msedgeupdate.dll на файловой системе. Размер этого файла также составляет несколько мегабайт.

Имплант PlugY, доставляемый при помощи бэкдора CloudSorcerer, в ходе своей работы запускает процесс с именем msiexec.exe для каждого вошедшего в систему пользователя, а также создает именованные каналы с шаблоном имени \.\PIPE\Y<число>. Присутствие этих двух индикаторов на системе с высокой степенью уверенности свидетельствует о заражении.

Заключение

В ходе атак на государственные организации Российской Федерации злоумышленники часто используют наборы инструментов, в которых реализуются самые разные техники и тактики. Разрабатывая эти инструменты, они прилагают немало усилий для того, чтобы максимально замаскировать вредоносную активность в сетевом трафике. Так, злоумышленники, стоящие за кампанией EastWind, использовали в качестве командных серверов популярные сетевые сервисы — GitHub, Dropbox, Quora, а также российские «Живой Журнал» и «Яндекс.Диск».

Примечательно, что в кампании EastWind было замечено вредоносное ПО двух различных китаеязычных группировок: APT27 и APT31. Этот пример наглядно показывает, что APT-группировки очень часто работают совместно, активно делясь друг с другом знаниями и инструментами для атак. Чтобы успешно противодействовать подобным коллаборациям, мы тщательно отслеживаем техники и тактики различных APT-группировок.