Статья Исследование CL0P Ransomware

xss.is/threads/46761

TA505 (также известная как FIN11) является финансово мотивированным субъектом киберпреступности. Они проводят операции Big Game Hunting, такие как развертывание программ-вымогателей и вымогательство крупного выкупа. В прошлом я объяснял, как они работают, и внимательно изучал их инструменты. Если вы не знакомы с TA505 и CL0P, я рекомендую вам сначала прочитать наш профиль злоумышленника TA505.

В 2020 году наблюдались три волны спама, исходящие от TA505: они начались в январе / феврале, затем последовали более длительный период летом с июня по сентябрь и очень короткий период в начале декабря. За месяцы отсутствия спама они добавляли все больше и больше жертв на свой портал вымогателей «CLoP^-LEAKS». В этом сообщении блога рассказывается об их операциях с программами-вымогателями. Во-первых, я подробно расскажу об активности этих операций за последние месяцы. Далее я опишу, какую информацию о жертвах содержат образцы CLoP, и исследую, почему часто есть несколько образцов CLoP, которые можно

отнести к одной жертве. Наконец, я посмотрю на их два онлайн-портала, которые поддерживают их операции: их портал утечки «CLoP^-LEAKS» и их портал переговоров, который они используют, чтобы прийти к соглашению с жертвами. Наша служба реагирования на инциденты Deutsche Telekom Security GmbH может быстро расследовать и устранять текущие вторжения TA505. Пожалуйста, свяжитесь с security-info@t-systems.com для получения дополнительной информации.

Операции TA505 и CLoP с июня 2020 г. по декабрь 2020 г.
Далее я дам обзор активности TA505 во второй половине 2020 года. Было два периода активности спама, за которыми следовали два периода развертывания CLoP.

Первый период активности:

Первый период рассылки спама начался 02.06.2020 и закончился 11.09.2020. В течение этого периода TA505 рассылал фишинговые письма почти каждый рабочий день, чтобы закрепиться во многих сетях. Впоследствии они будут отфильтровывать интересные корпоративные сети, а затем продвигать свое вторжение, двигаясь в боковом направлении.

Дата окончания наблюдаемой спамерской активности особенно интересна в связи с объявлением Secura. 11 сентября 2020 года, что было пятницей и, следовательно, последним днем обычной недели спама TA505, Secura объявила об уязвимости Zerologon. Это только предположение, почему TA505 не продолжил рассылку спама в следующий понедельник: либо публикация Zerologon резко прекратила их рассылку, либо они воспользовались возможностью быстро продвинуться в отдельных сетях.

В сентябре и октябре 2020 года CLoP удалось развернуть программу-вымогатель на нескольких жертвах. Наблюдаемые случаи в основном имели место в пятницу и субботу.
Второй период активности:

В середине декабря 2020 года TA505 вернулся менее чем за две недели спама, что могло поставить под угрозу возможные сети жертв для развертывания CLoP во время рождественских праздников 2020 года. Еще одним мотивом может быть получение доступа к новым сетям жертв, чтобы возобновить работу в январе / Февраль 2021 г.

На момент написания статьи на их портале утечек «CLoP ^ -LEAKS» новых жертв не было. Однако я нашел несколько образцов CLoP, указывающих, по крайней мере, на то, что операторы CLoP пытались развернуть свои программы-вымогатели в двух сетях во время Рождества. Ходят слухи, что одна из этих жертв заплатила выкуп в размере более 200 биткойнов (BTC) (почти шесть миллионов долларов).

Программа-вымогатель CLoP:

CLoP - это программа-вымогатель, которая развертывается после первоначального вторжения TA505. Каждый образец CLoP уникален для жертвы. Во-первых, он содержит 1024-битный открытый ключ RSA, используемый для шифрования данных. Во-вторых, он содержит персональную записку о выкупе.

Программа-вымогатель написана на C ++ и разработана в Visual Studio 2015 (14.0). Пока что я наблюдал только образцы CLoP для архитектуры x86. Размер неупакованного образца составляет от 100 до 200 КБ. CLoP переименовывает зашифрованные файлы и добавляет окончание файла либо «.Cllp», либо «.CIop». Программа-вымогатель содержит 1024-битный открытый ключ RSA, уникальный для каждой жертвы. Хотя 1024-битные ключи RSA устарели, до факторизации 1024-битных ключей еще далеко. По состоянию на январь 2021 года самый крупный публично известный ключ RSA, который был разложен в рамках RSA Factoring Challenge, имел 829 бит.

Уже есть хорошее описание функциональности CLoP от S2W LAB. Поэтому я воздержусь от описания того, как CLoP шифрует систему. Вместо этого я рассмотрю, как он расшифровывает свою встроенную записку о выкупе, и случаи, когда есть несколько образцов, которые можно отнести к жертве.

Расшифровка встроенной записки о выкупе

Каждый образец CLoP содержит записку с требованием выкупа, которая хранится как ресурс в исполняемом файле PE. В нескольких образцах CLoP строка ресурса 0x99AB и тип ресурса ID_HTML были согласованы. Этот ресурс представляет собой двоичный большой двоичный объект, закодированный с помощью шифра XOR. Каждая выборка содержит жестко закодированный ключ XOR длиной 33 байта. На момент написания я натолкнулся на два разных ключа, которые операторы CLoP повторно использовали в нескольких образцах.

На следующем снимке экрана показана функция, отвечающая за хранение записки о выкупе. Его единственный параметр - это путь, по которому будет храниться записка о выкупе. Название записки о выкупе жестко закодировано («README_README.txt»). Сначала эта функция строит полный путь к записке с требованием выкупа и пытается создать там файл (строки 15-17). В случае успеха он выбирает ресурс с именем 0x99AB и резервирует память для дешифрованной записки о выкупе (строки 19-25). В цикле for каждый байт зашифрованной записки о выкупе подвергается операции XOR с байтом жестко закодированного ключа XOR. Этот ключевой байт определяется с использованием позиции текущего байта по модулю размера жестко закодированного ключа, который составляет 33 байта (строки 26-27). После этого функция сохраняет расшифрованную записку о выкупе и очищает ее (строки 28 - 37).

```
HGLOBAL __cdecl drop_ransom_note(int current_path)
{
  HGLOBAL result; // eax
  DWORD NumberOfBytesWritten; // [esp+0h] [ebp-24h] BYREF
  void *Src; // [esp+4h] [ebp-20h]
  HGLOBAL hResData; // [esp+8h] [ebp-1Ch]
  HRSRC hResInfo; // [esp+Ch] [ebp-18h]
  HMODULE hModule; // [esp+10h] [ebp-14h]
  HANDLE hFile; // [esp+14h] [ebp-10h]
  SIZE_T dwBytes; // [esp+18h] [ebp-Ch]
  LPCVOID lpBuffer; // [esp+1Ch] [ebp-8h]
  SIZE_T i; // [esp+20h] [ebp-4h]

  SetErrorMode(1u);
  wsprintfW(FileName, L"%s\\README_README.txt", current_path);
  result = (HGLOBAL)open_file(FileName);
  if ( !(_BYTE)result )
  {
    hModule = GetModuleHandleW(0);
    hResInfo = FindResourceW(hModule, (LPCWSTR)0x99AB, L"ID_HTML");
    hResData = LoadResource(hModule, hResInfo);
    Src = LockResource(hResData);
    dwBytes = SizeofResource(hModule, hResInfo);
    lpBuffer = GlobalAlloc(0x40u, dwBytes);
    memmove_0((void *)lpBuffer, Src, dwBytes);
    for ( i = 0; i < dwBytes; ++i )
      *((_BYTE *)lpBuffer + i) ^= xor_key[(int)i % 33];
    NumberOfBytesWritten = 0;
    hFile = CreateFileW(FileName, 0x40000000u, 2u, 0, 2u, 0x80u, 0);
    if ( hFile != (HANDLE)-1 )
    {
      WriteFile(hFile, lpBuffer, dwBytes, &NumberOfBytesWritten, 0);
      CloseHandle(hFile);
    }
    result = GlobalFree((HGLOBAL)lpBuffer);
  }
  return result;
}
```

Эта записка создана специально для жертвы. Давайте посмотрим на отредактированную записку с требованием выкупа, выпавшую из недавнего образца CLoP:

README_README - Editor

Datei Bearbeiten Format Ansicht Hilfe

```
 HELLO DEAR [REDACTED]

_______DO NOT ATTEMPT TO RESTORE OR MOVE THE FILES YOURSELF. THIS MAY DESTROY THEM_______

Also a lot of sensitive data has been downloaded from your network.

FOR EXAMPLE:
==================================
\\[REDACTED]82\C$\Users\[REDACTED]
\\[REDACTED]00\C$\Users\[REDACTED]
\\[REDACTED]22\C$\Users\[REDACTED]
\\[REDACTED]22\D$
\\[REDACTED]00\C$\Users\[REDACTED]
\\P[REDACTED]60\C$\Users\[REDACTED]
\\[REDACTED]mb2\[REDACTED]
\\[REDACTED]mb2\[REDACTED]
\\[REDACTED]mb1\[REDACTED]
==================================
THIS IS A SMALL PART, ABOUT [REDACTED]%. more then [REDACTED] tb info

If you refuse to cooperate, all data will be published for free download on our portal
(USE TOR BROWSER):
http://[REDACTED].onion/


CONTACT->S:
[REDACTED]@tutanota.com
AND
unlock@[REDACTED].com
OR
unlock@[REDACTED].com

OR WRITE TO THE CHATS->
(USE TOR BROWSER):
http://[REDACTED].onion/[REDACTED]
```

Повторим, что содержит эта записка о выкупе:
Имя жертвы
Информация о конфиденциальных данных, которые они извлекли
Пути к общим файловым ресурсам
Имена пользователей как часть этих путей
Объем извлеченных данных
Ссылка .onion на их портал утечек «CLoP ^ -LEAKS».
Несколько адресов электронной почты для связи
Ссылка на их переговорный портал

Во-первых, это конфиденциальная информация о жертве. Во-вторых, это информация для взаимодействия с операторами CLoP. Поэтому рекомендуется никогда не загружать образцы программ-вымогателей в Интернет.
Учитывая записку о выкупе, возможно приписывание жертве. Далее я буду использовать это, чтобы исследовать очень интересное поведение методом проб и ошибок, наблюдаемое во время вторжений CLoP.
Метод проб и ошибок: почему на каждую жертву приходится несколько образцов?

За последние три месяца я смог найти более десятка образцов CLoP на VirusTotal. Во многих случаях имеется несколько образцов CLoP, которые можно отнести к одной жертве. Эти образцы собираются за пару часов. По крайней мере, в одном взаимодействии по реагированию на инцидент мы могли бы подтвердить это поведение.

Возникает вопрос, почему на каждую жертву приходится несколько образцов? В следующих разделах я расследую дела четырех жертв CLoP, в которых несколько образцов могут быть отнесены к одной и той же жертве. Атрибуция жертвы происходит на основе двух точек данных. Во-первых, образцы CLoP содержат записку о выкупе, в которой упоминается имя жертвы. Во-вторых, я считаю, что временные метки CLoP являются законными. Это соответствует тому, что мы видели в нескольких мероприятиях по реагированию на инциденты.

Жертва A

Случай с жертвой A произошел в субботу осенью 2020 года. Оба образца были собраны в один день в течение 30 минут. В следующей таблице перечислены важные свойства обоих образцов:

Property	Sample 1	Sample 2
time stamp	15:59:25	16:29:46
service name	MMCCSS	VVSBUILDTPT2
anti antivirus routine	McAfee	Appcheck
mutex name	GJLKWHTJIOPK#GBFSgt233r2fdsfds;6y2#666	Gslkjrhtoji4k32mtiguj42kl
certificate	signed (revoked)	not signed

Первое развертывание CLoP завершилось неудачно, так как обнаружение конечной точки заблокировало образец 1. Как следствие, они скомпилировали образец 2. Они изменили имя службы, которую регистрирует CLoP, а также имя мьютекса, которое он использует, чтобы гарантировать, что не более одного экземпляра работает на система. Кроме того, они обменялись функциональностью для работы с антивирусом McAfee. Операторы по умолчанию перестали работать с Appcheck, что уже наблюдалось в декабре 2019 года.

Интересно то, что первый образец подписан (теперь) отозванным сертификатом, а второй образец не подписан. Либо операторы забыли подписать второй образец после компиляции, либо подписание выполняется как услуга другой организацией, и операторы не удосужились подписать второй образец.

Жертва B

Дело жертвы B произошло в субботу ноября 2020 года. Оба образца были собраны в один день в течение 15 минут. Я перечисляю соответствующие свойства обоих образцов в следующей таблице:

Property	Sample 1	Sample 2
time stamp	14:28:00	14:43:58
service name	WinCheckDRVs (not installed)	WinCheckDRVs
anti antivirus routine	Many	None
mutex name	GKLJHWRnjktn32uyhrjn23io#666	666GKLJHWRnjktn32uyhrjn23io#666
certificate	Signed (revoked)	not signed

Образец 1 не поддерживает шифрование. Операторы CLoP изменили функцию WinMain в этом примере так, что вместо шифрования системы она запускает длинную последовательность вызовов ShellExecuteA, чтобы убить несколько процессов и остановить несколько служб. На следующем снимке экрана показана часть декомпилированной функции WinMain.

```
52        if ( !v13 )
53        {
54          EraseTape(0, 5u, 1);
55          sub_40C000();
56          ShellExecuteA(0, 0, "cmd", "/C net stop McAfeeEngineService /y", 0, 0);
57          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbsnmp.exe /F", 0, 0);
58          ShellExecuteA(0, 0, "cmd", "/C net stop \"Symantec System Recovery\" /y", 0, 0);
59          ShellExecuteA(0, 0, "cmd", "/C net stop NetMsmqActivator /y", 0, 0);
60          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM steam.exe /F", 0, 0);
61          ShellExecuteA(0, 0, "cmd", "/C net stop MSExchangeMGMT /y", 0, 0);
62          ShellExecuteA(0, 0, "cmd", "/C net stop SepMasterService /y", 0, 0);
63          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM PNTMon.exe /F", 0, 0);
64          ShellExecuteA(0, 0, "cmd", "/C net stop tmlisten /y", 0, 0);
65          ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecDeviceMediaService /y", 0, 0);
66          ShellExecuteA(0, 0, "cmd", "/C net stop ShMonitor /y", 0, 0);
67          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM dbeng50.exe /F", 0, 0);
68          ShellExecuteA(0, 0, "cmd", "/C net stop VeeamRESTSvc /y", 0, 0);
69          ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecVSSProvider /y", 0, 0);
70          ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer /y", 0, 0);
71          ShellExecuteA(0, 0, "cmd", "/C net stop VeeamDeploySvc /y", 0, 0);
72          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM powerpnt.exe /F", 0, 0);
73          ShellExecuteA(0, 0, "cmd", "/C net stop SQLAgent$PROD /y", 0, 0);
74          ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos Message Router\" /y", 0, 0);
75          ShellExecuteA(0, 0, "cmd", "/C net stop McShield /y", 0, 0);
76          ShellExecuteA(0, 0, "cmd", "/C net stop BackupExecJobEngine /y", 0, 0);
77          ShellExecuteA(0, 0, "cmd", "/C net stop swi_filter /y", 0, 0);
78          ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos AutoUpdate Service\" /y", 0, 0);
79          ShellExecuteA(0, 0, "cmd", "/C net stop \"Sophos MCS Agent\" /y", 0, 0);
80          ShellExecuteA(0, 0, "cmd", "/C net stop MsDtsServer100 /y", 0, 0);
81          ShellExecuteA(0, 0, "cmd", "/C net stop IMAP4Svc /y", 0, 0);
82          ShellExecuteA(0, 0, "cmd", "/C net stop SQLSERVERAGENT /y", 0, 0);
83          ShellExecuteA(0, 0, "cmd", "/C net stop \"SQLsafe Filter Service\" /y", 0, 0);
84          ShellExecuteA(0, 0, "cmd", "/C net stop Antivirus /y", 0, 0);
85          ShellExecuteA(0, 0, "cmd", "/C net stop DCAgent /y", 0, 0);
86          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM firefoxonfig.exe /F", 0, 0);
87          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM mspub.exe /F", 0, 0);
88          ShellExecuteA(0, 0, "cmd", "/C net stop SQLAgent$BKUPEXEC /y", 0, 0);
89          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM mysqld-opt.exe /F", 0, 0);
90          ShellExecuteA(0, 0, "cmd", "/C net stop MSSQLSERVER /y", 0, 0);
91          ShellExecuteA(0, 0, "cmd", "/C taskkill /IM isqlplussv.exe /F", 0, 0);
92          ShellExecuteA(0, 0, "cmd", "/C net stop \"Zoolz 2 Service\" /y", 0, 0);
93          ShellExecuteA(0, 0, "cmd", "/C net stop mfevtp /y", 0, 0);
```

Поскольку операторы CLoP скомпилировали Пример 1, в котором большая часть логики WinMain была заменена вызовами ShellExecuteA, имеется много мертвого кода и строк, на которые нет ссылок, соответственно. Например, имя службы и строки имени мьютекса хранятся в двоичном файле, но никогда не создаются.

Пример 2, который использовался для шифрования инфраструктуры, полностью рабочий. Он не содержит каких-либо функций для работы с антивирусными продуктами. Этого (вероятно) и добился Образец 1. Было использовано то же имя службы, но они немного изменили имя мьютекса, добавив к строке имени мьютекса еще одно «666».

Опять же, Образец 1 подписан (теперь) отозванным сертификатом, но Образец 2 не подписан.
В случае жертвы B банда CLoP зашифровала сеть, но они не достигли своей цели - получить выкуп.

Жертва C + D

Случаи жертвы C и жертвы D произошли во время рождественских праздников 2020 года. Оба случая произошли в один и тот же день. Все три известных мне образца были собраны в один день в течение семи часов. В следующей таблице приведены их важные свойства:

Property	Sample 1	Sample 3	Sample 4
time stamp	14:35:55	15:42:22	21:45:45
service name	None	BFEFservs	BFEFservs
anti antivirus routine	Many	None	None
mutex name	None	TWrsg24gredgre#W#666	TWrsg24gredgre#W#666
certificate	not signed	not signed	not signed

В случае жертвы C я смог найти только один образец (Образец 1), а второй мне не хватает (Образец 2). Операторы CLoP снова скомпилировали Пример 1 с длинной последовательностью вызовов ShellExecuteA для уничтожения служб / остановки процессов. Это включает несколько решений безопасности, таких как McAfee и Sophos. В примере 1 не выполняется шифрование файлов, поскольку он завершается после вызова ShellExecuteA. Опять же, есть много мертвого кода, но на этот раз нет ни строки имени службы, ни строки имени мьютекса. К сожалению, мне не удалось найти Образец 2, который якобы зашифровал инфраструктуру жертвы C.

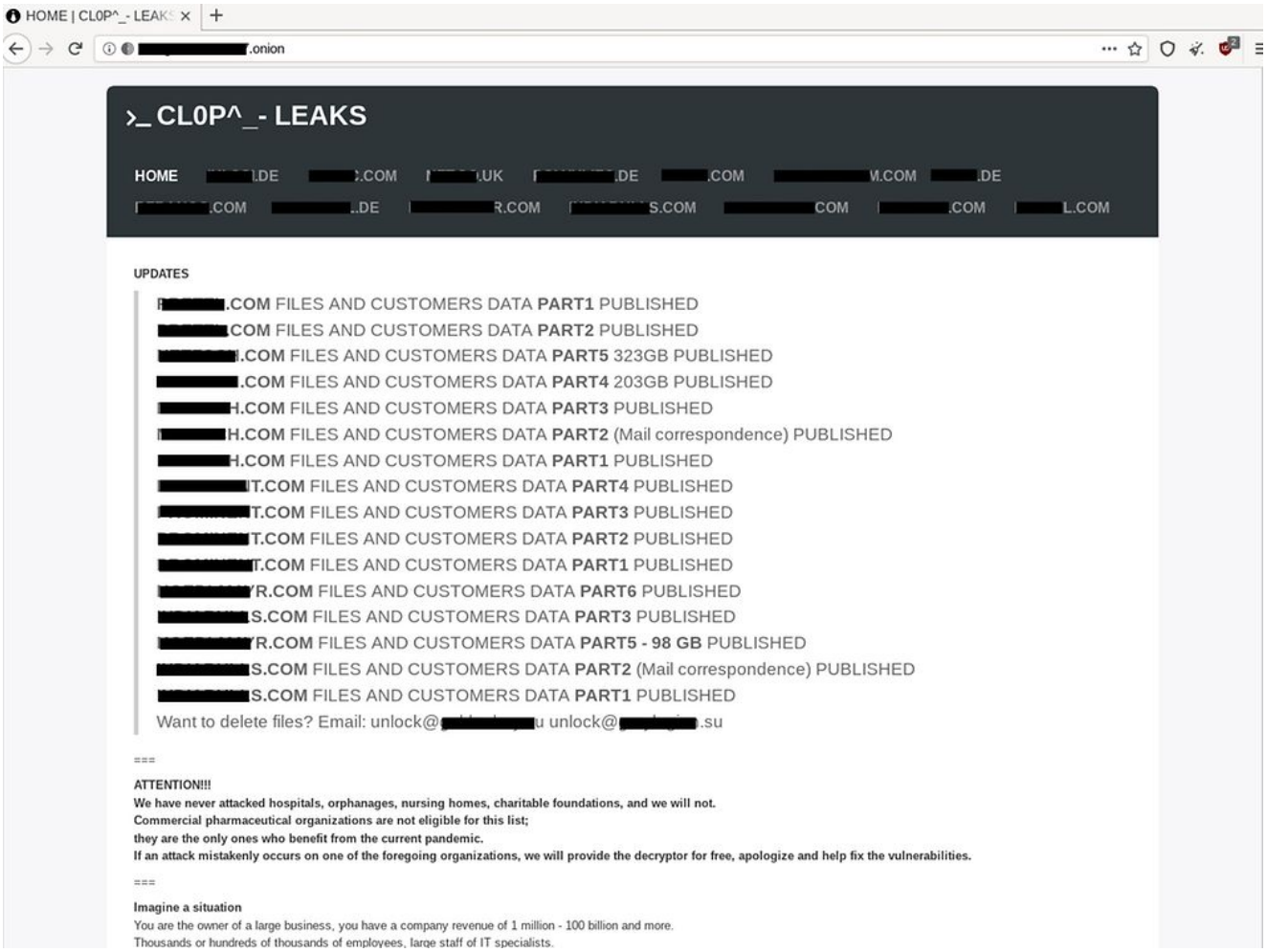
На момент написания статьи Жертва C не указана на портале утечек CLoP. Следовательно, мы можем предположить только две вещи: либо это было неудачное атака, и программа-вымогатель не была развернута, потому что что-то пошло не так во время развертывания Образца 1 или Образца 2. Либо операторы CLoP успешно развернули Образец 2, жертва C заплатила выкуп , и поэтому не указан на портале утечек.

В случае жертвы D я обнаружил два образца. Оба образца были собраны в один день, но в течение шести часов. Оба образца содержат логику программы-вымогателя. Семантические возможности обоих образцов практически равны. Однако разница между Образцом 3 и Образцом 4 не так очевидна, как в случаях с жертвой A и жертвой B.

В отличие от жертвы C, у нас есть четкие признаки, позволяющие предположить, что CLoP достиг своей цели по успешному шифрованию инфраструктуры жертвы D.
Присутствие CLoP в Интернете

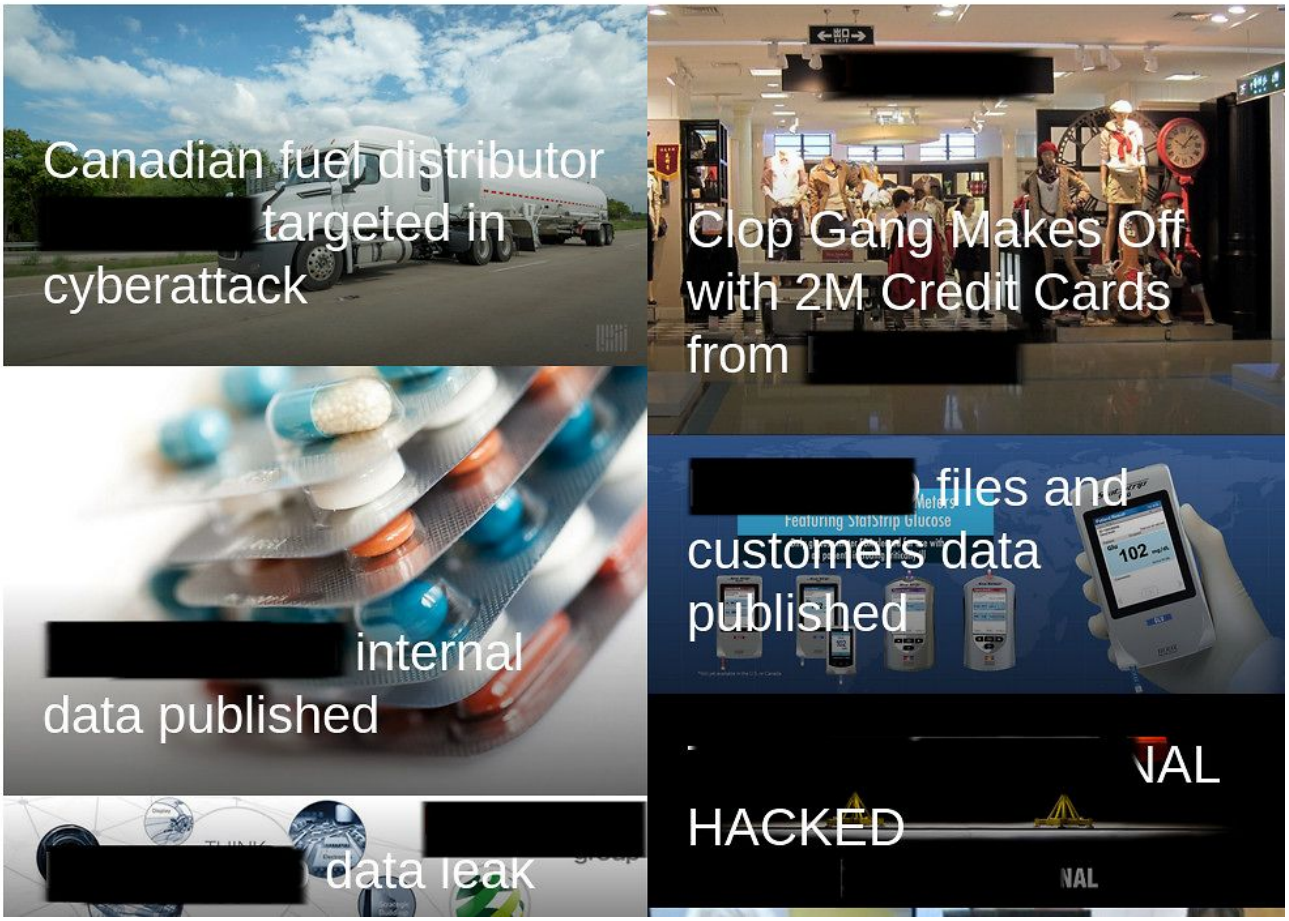
CLoP поддерживает два онлайн-присутствия для поддержки своих операций по охоте на крупную дичь. Первое присутствие - это их портал утечек под названием «CLoP ^ -LEAKS». Его цель - запугать будущих жертв, размещая конфиденциальные данные прошлых жертв, которые не заплатили выкуп. Второе присутствие - это их переговорный портал. Это служит «поддержкой клиентов» для жертв, которые готовы прийти к соглашению и заплатить выкуп.
Запугивание жертвы: портал утечек CLoP

CLoP - одна из банд вымогателей, применившая технику двойного вымогательства. Прежде чем развернуть программу-вымогатель, они извлекают до терабайта конфиденциальных данных из сети жертвы. В случае, если жертва правильно настроила резервное копирование и не желает платить выкуп, она все равно может пригрозить опубликовать эти данные на своем портале утечек «CLoP ^ -LEAKS». Портал перечисляет 19 жертв в январе 2021 года. Большинство из них проживают в Германии. На следующем снимке экрана показан их портал утечек, размещенный в сети TOR:



Сервисы сайта:

Чат: чат поддержки, в котором киберпреступники направляют жертв через переговорный процесс.
Demo decrypt: инструмент дешифрования, который жертвы могут использовать для расшифровки до пяти файлов по своему выбору.
Купить биткойны: информация о том, как покупать биткойны
Новости: красочные скриншоты новостей о последних кибератаках CLoP.
О нас: дальнейшие ссылки о них.
Операторы CLoP пытаются убедить своих жертв заплатить, красочно демонстрируя свою историю взломов (раздел «Новости»). Ссылки на сторонние веб-сайты (раздел «О нас») предоставляют дополнительную справочную информацию о них.



Процесс переговоров проходит по той же схеме, что и с другими бандами вымогателей. Тон разговора полезный и прямой, но никогда не враждебный. Сначала они спрашивают, уполномочен ли их собеседник вести переговоры, и упоминают, что их просто интересуют деньги.

Если обе стороны придут к соглашению, операторы CLoP предоставят дешифратор и доказательство того, что они удалили все эксфильтрованные файлы. Взамен они хотят денег в биткойнах. Они предлагают бесплатное дешифрование до пяти некритических файлов, чтобы доказать, что они могут расшифровать сеть жертвы, и продемонстрировать ей свою добрую волю.
Они требуют от 5% до 10% годового дохода, но говорят жертвам, что возможны скидки до 30%, если они придут к соглашению менее чем за полнедели. Тем не менее, они открыты для дальнейших переговоров, чтобы окончательный выкуп был намного меньше первоначального требования в размере 5–10% от годового дохода.
После того, как обе стороны согласовали цену, операторы CLoP предлагают дополнительную поддержку и предложения о том, как осуществлять переводы в биткойнах. Они готовы мириться с небольшими колебаниями из-за биткойнов. Хотя

они знают, что биткойн сильно колеблется, и они фиксируют выкуп только за 24 часа. После того, как они получили выкуп на свой биткойн-кошелек, они продолжают оказывать поддержку. Жертв обычно очень беспокоят три вещи. Во-первых, какие данные CLOP удалось эксфильтровать и что они получили отчет об удалении файлов. Во-вторых, им требуется дополнительная поддержка для расшифровки их инфраструктуры. В-третьих, им нужен отчет о том, как произошло нарушение сети. Операторы CLOP, похоже, помогают жертвам решить эти проблемы даже после того, как им уже заплатили.

Заключение:
CLOP была одной из самых активных операций по охоте на крупную дичь в 2020 году. Им удалось взломать несколько крупных предприятий. Их вторжения связаны с TA505. Я ожидаю, что эти вторжения продолжатся с той же скоростью и частотой в 2021 году.
Образцы CLOP содержат персонализированные записки о выкупе, в которых упоминается жертва и раскрываются важные детали переговорного процесса. Операторы CLOP предлагают собственный портал для переговоров, в том числе службу поддержки через чат.
В случаях, когда жертвы не платят выкуп, они загружают большие объемы конфиденциальных данных на свой портал «CLOP ^ -LEAKS». На момент написания они продолжают хранить эти данные там, в некоторых случаях более девяти месяцев.
Я задокументировал поведение метода проб и ошибок, наблюдаемое при развертывании CLOP: в нескольких развертываниях имеется более одного образца, связанного с жертвой. В некоторых случаях кажется, что первая выборка была начальной проверкой того, блокирует ли обнаружение конечной точки выборку. В других случаях первый образец не содержит возможности дешифрования, поскольку операторы, вероятно, закомментировали его для этой сборки.

Это показывает, что операторы CLOP имеют доступ к исходному коду CLOP. Они способны компилировать и быстро исправлять в нем проблемы во время текущего развертывания. Это подчеркивает предположение о том, что эта банда вымогателей представляет собой закрытую группу людей, которые совместно используют общие ресурсы и работают в тесном сотрудничестве.