АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET: кибергруппа Lazarus переключилась на Центральную Америку

25 апреля 2018 года

Группа Lazarus получила известность после кибератаки на Sony Pictures Entertainment в 2014 году. В 2017 году группа сохраняет активность, используя широкий спектр вредоносных инструментов, включая вайпер KillDisk.

Наше исследование показало, что Lazarus с большой долей вероятности стоят за атакой на онлайн-казино в Центральной Америке и некоторые другие цели в конце 2017 года. В этих инцидентах атакующие использовали одни и те же инструменты, в том числе KillDisk, который запускался на скомпрометированных устройствах.

Инструменты Lazarus

Хакеры Lazarus были впервые идентифицированы в отчете Novetta Operation Blockbuster в феврале 2016 года; US CERT и ФБР назвали эту кибергруппу Hidden Cobra. Группа получила широкую известность после атаки на Sony Pictures Entertainment.

Последующие атаки, связанные с Lazarus, привлекли внимание специалистов по информационной безопасности, в работе опиравшихся на материалы Novetta и другие исследования – сотни страниц описаний инструментов атакующих: атаки на польские и мексиканские банки, эпидемия WannaCry, фишинговые атаки на подрядчиков Министерства обороны США и др. Все эти исследования позволяют определить Lazarus в качестве источника атак.
Обратите внимание, что список инструментов Lazarus (все файлы, которые специалисты по информационной безопасности связывают с активностью группы) достаточно широк, и мы считаем,

что существует множество их подсемейств. В отличие от наборов инструментов, используемых другими кибергруппами, исходный код инструментов Lazarus никогда не раскрывался в результате публичной утечки.

Помимо специальных программ, Lazarus используют проекты, доступные на GitHub или предоставляемые на коммерческой основе.

Инструменты Lazarus для атаки на онлайн-казино

В этом разделе мы рассмотрим некоторые инструменты, обнаруженные на серверах и рабочих станциях сети онлайн-казино в Центральной Америке, и объясним, как установили их связь с Lazarus. Антивирусные продукты ESET детектируют вредоносные программы группы как Win32/NukeSped и Win64/NukeSped. Они использовались в сочетании с образцами деструктивного ПО KillDisk.

Почти все эти инструменты предназначены для запуска в качестве службы Windows. Для этого нужны права администратора, а это означает, что атакующие должны иметь эти права во время разработки или компиляции.

TCP-бэкдор

Win64/NukeSped.W – консольное приложение, установленное в системе как служба. Одним из первых этапов выполнения является динамическая загрузка требуемых имен DLL в стек:

```
mov     dword ptr [rbp+57h+LibFileName_0], 'nrek'
mov     [rbp+57h+var_64], '23le'
mov     [rbp+57h+var_60], 'lld.'          kernel32.dll
mov     [rbp+57h+var_5C], 0
mov     dword ptr [rbp+57h+LibFileName_1], 'avda'
mov     [rbp+57h+var_44], '23ip'
mov     [rbp+57h+var_40], 'lld.'          advapi32.dll
mov     [rbp+57h+var_3C], 0
mov     dword ptr [rbp+57h+LibFileName_2], 'lhpi'
mov     [rbp+57h+var_54], 'ipap'
mov     [rbp+57h+var_50], 'lld.'          iphlpapi.dll
mov     [rbp+57h+var_4C], 0
mov     dword ptr [rbp+57h+LibFileName_3], 'astw'
mov     [rbp+57h+var_34], '23ip'
mov     [rbp+57h+var_30], 'lld.'          wtsapi32.dll
mov     [rbp+57h+var_2C], 0
mov     dword ptr [rbp+57h+LibFileName_4], 'uces'
mov     [rbp+57h+var_84], '.23r'          secur32.dll
mov     [rbp+57h+var_80], 'lld'
mov     dword ptr [rbp+57h+LibFileName_5], 'ldtn'
mov     [rbp+57h+var_A4], 'ld.l'          ntdll.dll
mov     [rbp+57h+var_A0], 6Ch
mov     dword ptr [rbp+57h+LibFileName_6], 'resu'
mov     [rbp+57h+var_94], '.vne'          userenv.dll
mov     [rbp+57h+var_90], 'lld'
mov     dword ptr [rbp+57h+LibFileName_7], 'wlhs'
mov     [rbp+57h+var_74], '.ipa'          shlwapi.dll
mov     [rbp+57h+var_70], 'lld'
lea     rcx, [rbp+57h+LibFileName_0]    ; lpLibFileName
call    cs:LoadLibraryA
```

Аналогично, имена процедур для API Windows строятся динамически. В этом конкретном образце они видны в виде открытого текста; в других прошлых образцах, которые мы проанализировали, они были закодированы в base64, зашифрованы или размещены в стеке посимвольно:

```
lea     rdx, aWtsenumeratese            ; "WTSEnumerateSessionsA"
mov     rcx, r13                        ; hModule
call    cs:GetProcAddress
mov     cs:WTSEnumerateSessionsA, rax
lea     rdx, aWtsfreememory             ; "WTSFreeMemory"
mov     rcx, r13                        ; hModule
call    cs:GetProcAddress
mov     cs:WTSFreeMemory, rax
lea     rdx, aWtsqueryuserto            ; "WTSQueryUserToken"
mov     rcx, r13                        ; hModule
call    cs:GetProcAddress
mov     cs:WTSQueryUserToken, rax

loc_13F6BA818:                          ; CODE XREF: resolve_WINAPIs 5E1↑j
test    r12, r12
jz      short loc_13F6BA862
lea     rdx, aLsaenumeratelo            ; "LsaEnumerateLogonSessions"
mov     rcx, r12                        ; hModule
call    cs:GetProcAddress
mov     cs:LsaEnumerateLogonSessions, rax
```

Эти признаки являются типичными чертами вредоносного ПО Lazarus. Другая типичная характеристика бэкдора Lazarus также видна в этом бэкдоре: он слушает определенный порт, который является индикатором блокировки брандмауэром:

```
1  void __fastcall TCP::PortOpening(__int64 a1, unsigned __int16 a2, int bSwitch)
2  {

13   l_bSwitch = bSwitch;
14   v4 = a2;
15   szCommand = 0;
16   memset(&Dst, 0, 0x103ui64);
17   szFmt = "netsh firewall add portopening TCP %d Assistance";
18   if ( !l_bSwitch )
19     szFmt = "netsh firewall delete portopening TCP %d";
20   sprintf(&szCommand, szFmt, v4);

28   if ( CreateProcessA_1(0i64, &szCommand, 0i64, 0i64, 0, 0, 0i64, 0i64, &Start
29   {
30     WaitForSingleObject(hHandle, 0x3A98u);
31     CloseHandle_1(hHandle);
32     CloseHandle_1(hObject);
33     Sleep(0x7D0u);
34   }
35 }
```

Бэкдор поддерживает 20 команд, функциональность которых аналогична ранее проанализированным образцам Lazarus (обратите внимание, что имена команд здесь не заданы злоумышленниками, а были созданы вирусным аналитиком ESET):

```
switch ( CommandId )
{
  case 1:
    v10 = cmd__GetCurrentDir(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 2:
    v10 = cmd__ListDisksInfo(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 3:
    v10 = cmd__FileSearch(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 4:
    v10 = cmd__CreateProcessSimple(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 5:
    v10 = cmd__ChangeRealFileTime(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 6:
    v10 = cmd__DropFile(MainObject, (__int64)Param1, (__int64)Param2, Param3);
    goto LABEL_59;
    :
  case 17:
    v10 = cmd__CreateProcessAsLoggedUser(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 18:
    v10 = cmd__InjectIntoExplorer(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
  case 19:
    v10 = cmd__InjectIntoProcIDLoggedUser(MainObject, (__int64)Param1, (__int64)Param2, (__int64)Param3);
    goto LABEL_59;
}
if ( CommandId == 20 )
  break;
```

Бэкдор создает несколько файлов в файловой системе. Порт прослушивания хранится в текстовом файле с именем %WINDOWS%\Temp\p. Файл %WINDOWS%\Temp\perflog.evt содержит список путей бинарных файлов, предназначенных для инжекта, исполнения или записи в реестр в зависимости от начального символа строки:

```
"*" = выполнение через инжект в процесс (executed via process
injection)
"+" = выполнение через cmd.exe
" " = запись в реестр
HKLM\SYSTEM\CurrentControlSet\Services\<ServiceName>\Instance
```

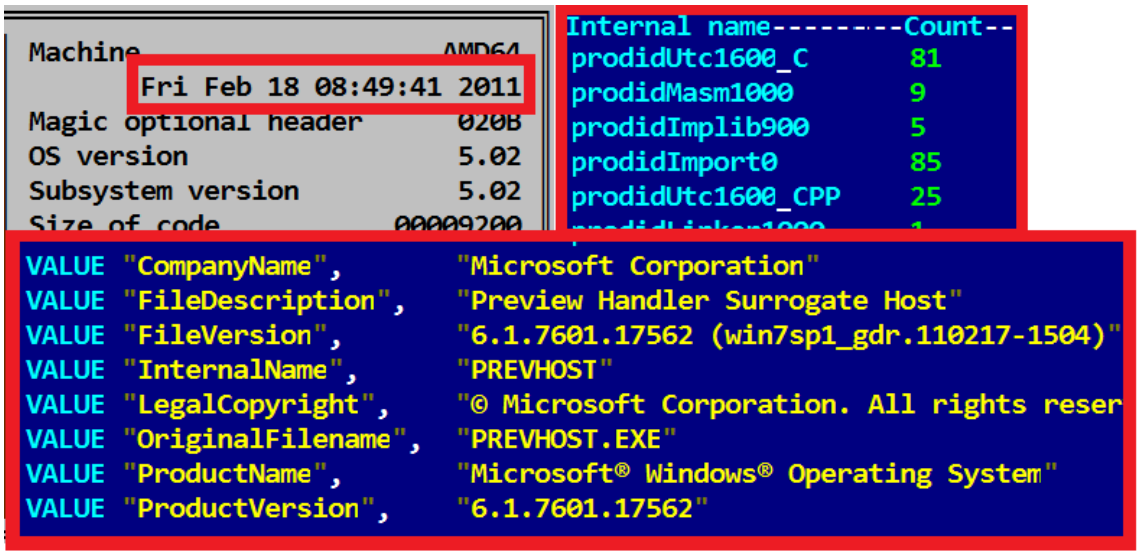
В случае опции «+» выходные данные cmd.exe / c «% s 2 »% s» (или cmd.exe / c «% s »% s 2> и 1») записываются в % WINDOWS% \ Temp \ perflog.dat.

Взломщик сеансов

Консольное приложение Win64/NukeSped.AB создает процесс от имени другого пользователя, зарегистрированного в настоящее время в системе жертвы (аналогично команде номер 17 из ранее описанного бэкдора TCP).

Это защищенный с помощью Themida вариант описанного Лабораторией Касперского. В нашем случае он был установлен как C:\ Users\public\ps.exe. Он имеет три параметра.

Статичный просмотр показывает одинаковые свойства файла в обоих этих выборках: одна и та же временная метка компиляции PE, идентичные данные компоновщика Rich Header (указывающие на компоновщик Visual Studio 2010 (10.00)), а часть информации о версии ресурсов совпадает:



Хотя временная метка PE и ресурсы украдены из законного файла Microsoft PREVHOST.EXE из Windows 7 SP1, данные по линковке файла отсутствуют: исходный же файл Microsoft был скомпилирован и связан с Visual Studio 2008 (9.00).

Наш последовательный динамический анализ подтвердил, что этот файл, найденный в скомпрометированной сети онлайн-казино, связан с взломщиком сеанса, используемым в атаках на польские и мексиканские объекты.

Загрузчик/установщик

Это простой инструмент для работы из командной строки, принимающий несколько параметров. Он предназначен для работы с процессами (инжект/удаление процесса с помощью PID или имени), службами (завершение/переустановка службы) или файлами (сброс /удаление). Функциональность определяют параметры.

Версии KillDisk

KillDisk – общее название, под которым продукты ESET детектируют деструктивное вредоносное ПО с функцией стирания диска – повреждение загрузочных секторов и перезапись, а затем удаление (системных) файлов, с последующей перезагрузкой, позволяющую сделать устройство непригодным к использованию.

Несмотря на то, что все версии KillDisk имеют схожие функции, кодовая база образцов не всегда совпадает. У KillDisk много подсемейств, названия которых отличаются суффиксами (в нашем случае, Win32/KillDisk.NBO). Варианты подсемейств с общими фрагментами кода иногда используются в разных киберкампаниях, что может указывать на общий источник атак, как в данном кейсе.

Другие версии KillDisk использовались в целевых атаках на украинские объекты в декабре 2015 и декабре 2016 года, но эти образцы относятся к другим подсемействам и, скорее всего, не имеют отношения к новым атакам.

Изучая инцидент в Центральной Америке, мы обнаружили два варианта Win32/KillDisk.NBO в скомпрометированной сети. Вредоносным ПО было заражено больше ста машин в организации. Есть несколько возможных объяснений его появления: атакующие могли скрывать следы после атаки, либо использовать KillDisk для вымогательства или киберсаботажа. В любом случае, это масштабное заражение в рамках одной организации.

Данные нашей телеметрии, а также одновременное использование версий Win32/KillDisk.NBO и других известных инструментов Lazarus в скомпрометированной сети указывают на то, что KillDisk развернули именно хакеры Lazarus, а не какая-либо другая кибергруппа.

Анализ двух образцов показал, что у них много общих фрагментов кода. Кроме того, они почти идентичны версии KillDisk, которая использовалась в атаках на финансовые организации Латинской Америки, изученных Trend Micro.

В образцах KillDisk, обнаруженных в сети онлайн-казино, используется следующий путь: C:\Windows\Temp\dimens.exe

Фактическая встроенная полезная нагрузка инжектирована в системный процесс werfault.exe:

```
1  BOOL WinMainEx()
2  {
15   if ( *(_WORD *)au8EmbeddedPayload == IMAGE_DOS_SIGNATURE )
16   {
17     do
18     {
19       v0 = &au8EmbeddedPayload[e_lfanew];
20       if ( *(_DWORD *)&au8EmbeddedPayload[e_lfanew] != IMAGE_NT_SIGNATURE )
21         break;
27       if ( !CreateProcessA( "C:\\Windows\\system32\\werfault.exe",
51       Mem = (char *)VirtualAllocEx(ProcessInformation.hProcess, *((LPVOID *)v0 + 13),
                                      *((_DWORD *)v0 + 20), 0x3000u, 0x40u);
58       if ( Mem )
59       {
60         WriteProcessMemory(ProcessInformation.hProcess, Mem, au8EmbeddedPayload,
81         SetThreadContext(ProcessInformation.hThread, v1);
82         ResumeThread(ProcessInformation.hThread);
88     }
```

Один из вариантов защищен с помощью коммерческого VMProtect третьего поколения, что затрудняет распаковку. Скорее всего, атакующие не покупали лицензию VMProtect, а использовали доступные пиратские или утекшие в интернет копии. Использование инструментов для защиты ПО характерно для группы Lazarus: в атаках на польские и мексиканские банки в феврале 2017 года они использовали Enigma Protector; некоторые образцы Operation Blockbuster, о которых сообщали Palo Alto Networks, использовали более старую версию VMProtect.

Типичный формат строк Lazarus

Среди многочисленных характеристик, которые позволяют нам приписывать авторство образцов и происхождение атак группе Lazarus, необходимо отметить формат строк. В таблице ниже представлены форматированные строки, найденные в вышеупомянутых образцах, а также в других TCP бэкдорах, связанных с Lazarus:

Строки формата	Атака Lazarus / Отчет
cmd.exe /c "%s 2>> %s"	Данный кейс: онлайн-казино в Центральной Америке
cmd.exe /c "%s >> %s 2>&1"	
cm%sx%s"%s%s %s" 2>%s	Operation Blockbuster и эпидемия WannaCry
c%s.e%sc "%s > %s 2>&1"	Operation Blockbuster - The Sequel
%sd.e%sc "%s > %s 2>&1"	
%s%s%s "%s > %s 2>&1"	Operation Blockbuster - The Saga
md.e	
xe /c	
%sd.e%sc "%s > %s" 2>&1	Operation Blockbuster
%sd.e%sc n%ssh%srewa%s ad%s po%sop%sing T%s %d "%s"	
%s /c "%s" >%s 2>&1	Operation Blockbuster
cmd.exe /c "%s" > %s 2>&1	Атаки на польские и мексиканские банки

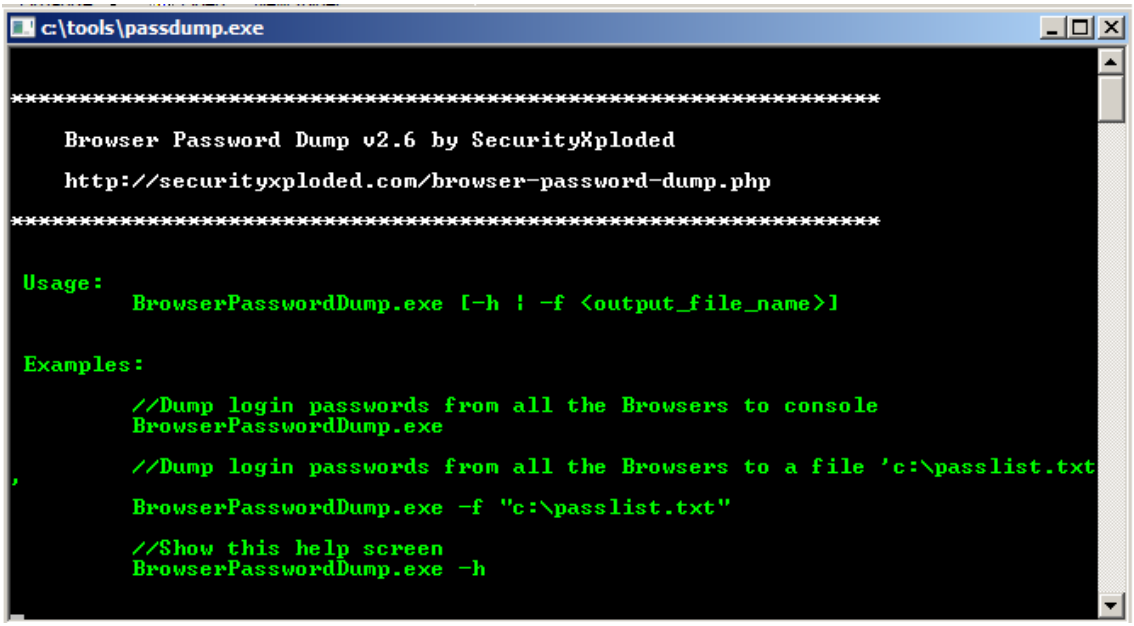
Сам по себе этот факт не может быть доказательством, но, поискав схожее форматирование строк во всех образцах вредоносного ПО, собранного ESET, мы обнаружили их только в образцах, предположительно относящихся к Lazarus. Следовательно, мы можем предположить, что наличие этих строк указывает на авторство Lazarus.

Дополнительные инструменты

Существует минимум два доступных инструмента, которые использовали атакующие.

Browser Password Dump

Этот инструмент предназначен для восстановления паролей из популярных веб-браузеров. С декабря 2014 года он использует старые, хорошо известные методы. Его можно использовать в последних версиях Google Chrome (64.0.3282.186), Chromium (67.0.3364.0), Microsoft Edge (41.16299.15.0) и Microsoft Internet Explorer (11.0.9600.17843). Он не совместим с последними версиями Firefox или Opera.



Mimikatz

Атакующие использовали также модифицированную версию инструмента Mimikatz, предназначенного для извлечения учетных данных Windows. Он принимает один параметр – имя файла для хранения вывода. Если параметр не задан, выходной файл под названием ~Temp1212.tmp хранится в том же каталоге, что и Mimikatz. Вывод содержит хеши учетных данных Windows авторизованных пользователей. Инструмент часто используется в целевых атаках, в частности, группой Telebots в эпидемии Petya, а также в Операции Buhtrap.

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
12   l_argc = argc;
13   l_argv = argv;
14   mimikatz_initOrClean(1);
15   if ( l_argc >= 2 )
16     g_logFileName = (char *)l_argv[1];          ~Temp1212.tmp
17   err = RtlAdjustPrivilege(SE_DEBUG_PRIVILEGE, TRUE, FALSE, &bEnabled);
18   if ( (err & 0x80000000) != 0 )
19     FS::writeFile(
20       (__int64)L"ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (%u) %08x\n",
21       SE_DEBUG_PRIVILEGE,
22       err,
23       v7);
24   v10 = 4;
25   pOptionalData = g_pOptionalData;
26   kuhl_m_sekurlsa_enum(pData, (__int64)&pOptionalData);
27   (*(void (**)(void))(qword_13F2992F0 + 8))();
28   CoUninitialize();
29   return 0;
30 }
```

Вектор заражения

Большинство инструментов, описанных выше, загружалось и устанавливалось на рабочих станциях с помощью вредоносных дропперов и загрузчиков, используемых на начальной стадии атаки. Кроме того, мы видели индикаторы, указывающие на использование средств удаленного доступа, включая Radmin 3 и LogMeIn для контроля целевых устройств.

Выводы

Недавняя атака на онлайн-казино в Центральной Америке позволяет предположить, что хакеры Lazarus перекомпилируют инструменты перед каждой новой кампанией (мы не видели идентичные образцы где-либо еще). Это была сложная многоэтапная атака, в рамках которой использовались десятки защищенных инструментов, которые, будучи автономными, вряд ли продемонстрировали такую динамику.

Использование KillDisk, скорее всего, служило одной из двух целей: атакующие скрывали следы после операции шпионажа, либо использовали деструктивное ПО для вымогательства или саботажа. В любом случае, обнаружение вредоносного ПО более чем на 100 рабочих станциях и серверов организации указывает на значительные ресурсы, затраченные атакующими.

Образцы

429B750D7B1E3B8DFC2264B8143E97E5C32803FF	Win32/KillDisk.NBO
7DFE5F779E46855B32612D168B9CC5334F25B5F6	Win32/KillDisk.NBO
5042C16076AE6346AF8CF2B40553EEEEA98D5321	Win64/NukeSped.W trojan (VMProtect-ed)
7C55572E8573D08F3A69FB15B7FEF10DF1A8CB33	Win64/NukeSped.W trojan (Themida-protected)
E7FDEAB60AA4203EA0FF24506B3FC666FBFF759F	Win64/NukeSped.Z trojan (Themida-protected)
18EA298684308E50E3AE6BB66D7321A5CE664C8E	Win64/NukeSped.Z trojan (VMProtect-ed)
8826D4EDBB00F0A45C23567B16BEED2CE18B1B6A	Win64/NukeSped.AB trojan (Themida-protected)
325E27077B4A71E6946735D32224CA0421140EF4	Win64/Riskware.Mimikatz.A application
D39311C74DEB60C736982C1AB74D6684DD1E1264	Win32/SecurityXploded.T (VMProtect-ed)
E4B763B4E74DE3EF24DB6F19108E70C494CD18C9	Win32/SecurityXploded.T (Themida-protected)