welivesecurity by (eser)

Award-winning news, views, and insight from the ESET security community

English

TIPS & ADVICE BUSINESS SECURITY ESET RESEARCH >

WeLiveScience

FEATURED ▼ TOPICS ▼ ABOUT US ▼



ESET RESEARCH

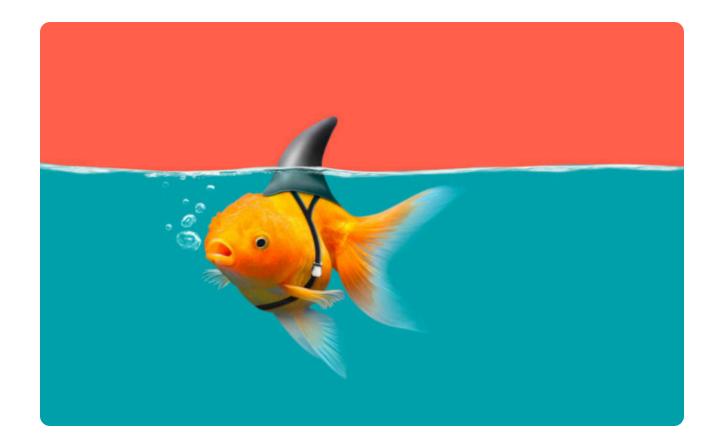
Fake or Fake: Keeping up with OceanLotus decoys

ESET researchers detail the latest tricks and techniques OceanLotus uses to deliver its backdoor while staying under the radar



Romain Dumont

20 Mar 2019 • 15 min. read



Share Article











Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

Accept all and close

Manage cookies

This article will first describe how the OceanLotus group (also known as APT32 and APT-C-00) recently used one of the publicly available exploits for CVE-2017-11882, a memory corruption vulnerability present in Microsoft Office software, and how OceanLotus malware achieves persistence on compromised systems without leaving any traces. Then the article describes how, since the beginning of 2019, the group has been leveraging self-extracting archives to run code.

Context

Following OceanLotus' activities is taking a tour in the world of deception. This group is known to lure victims by forging appealing documents to entice potential victims into executing the group's backdoor, and keeps coming up with new ideas to diversify its toolset. The techniques employed for the decoys range from files with so-called double extensions, self-extracting archives and macro-enabled documents, to reusing known exploits. On top of that, they are very active and relentlessly continue to raid their favourite victims, South East Asian countries.

Summing up the Equation Editor exploit

In mid-2018, OceanLotus carried out a campaign using documents abusing the weakness exposed by the CVE-2017-11882 vulnerability. Indeed, several Proofs-of-Concept were made available. The vulnerability resides in the component responsible for rendering and editing mathematical equations. One of the malicious documents used by OceanLotus was analysed by 360 Threat Intelligence Center (in Chinese) and includes details about the exploit. Let's take a look at a similar document.

First stage

This document FW Report on demonstration of former CNRP in Republic of Korea.doc (SHA-1: D1357B284C951470066AAA7A8228190B88A5C7C3) is similar to the one mentioned in the article above, and also interesting as it really targets people interested in Cambodian politics (the CNRP – Cambodia National Rescue Party – political party was dissolved in late 2017). Despite its .doc extension, the document is actually in RTF format (see Figure 1), contains many garbage groups, and is also malformed.

Your account, your cookies choice We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and

serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

6F {\rtBuddyMeowMeo 6F wMeowMeowMeowMeo 6F wMeowMeowMeowMeo 66 wPussyCatf1\adef

sfully opens this RTF _EFILEHDR structure, ;ure 3) for a font.



00000C50

0 00-E9 70 10 00-00 55 8B **E**0

Figure 2 -- FONT record values

```
FONT record (8):

Consists of:

tag (8)

[tface] typeface number

[style] 1 for italic and/or 2 for bold

[name] font name (null-terminated)

Figure 3 -- FONT record format
```

An overflow in the *name* field is possible because its size isn't checked before being copied. A name that is too long triggers the vulnerability. As seen in the RTF file content (offset 0xC26 in Figure 2), the buffer is filled with shellcode followed by a NOP (0x90) sled and the return address 0x402114. That address is a gadget in EQNEDT32. exe pointing to a RET instruction. This results in EIP pointing at the beginning of the *name* field which contains the shellcode.

```
public shellcode_start
  000:00000C26
eg000:00000C26
                                    shellcode_start proc near
eg000:00000C26 B8 44 EB 71 12
                                                             edx, 12345678h
eg000:00000C2B BA 78 56 34 12
eg000:00000C30 31 D0
                                                                             ; 0x45bd3c
eg000:00000C32 8B 08
                                                             ecx, [eax]
                      welivesecu
eg000:00000C34 8B 09
                                                             ecx, [ecx]
eg000:00000C36 8B 09
                                                             ecx, [ecx]
                                                             cx, 3Ch ; '<'
eg000:00000C38 66 83 C1 3C
                                                    add
eg000:00000C3C FF E1
                                                                             ; jump to 0xc58
eg000:00000C3C
                                    shellcode_start
eg000:00000C3C
eg000:00000C3C
                                                    db 14h dup(90h)
dd 402114h
         00C3E 90 90 90 90 90 90+nop_sled
    0:00000C52 14 21 40 00
                                    ret_gadget
                         Figure 4 -- Start of the exploit shellcode
```

The address 0x45BD3C stores a variable that is dereferenced until it reaches a pointer to the currently loaded MTEFData structure. That is where the rest of the

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

shellcode, embedded find the handle of the hdles

of a WinWord process
mask: 0x12019F. To
ther open document,
ping function and the
yyyy"; this technique is
copied to a temporary
the document are

```
00675F3F: 5D C2 04 00-50 FF 55 B0-8B 4D F4 E9-EC EB FF FF ]<sub>T</sub> → P U∭IM 0∞δ 00675F4F: AA BB CC DD-28 01 1D 00-79 79 79- welivesecurity (⊕↔ yyyy
```

Figure 5 -- Markers at the end of the document

The 32-bit value between the AABBCCDD and yyyy markers is the offset to the next shellcode. It is invoked using the CreateThread function. The extracted shellcode is the same that the OceanLotus group has been using for a while now. The Python emulator script we released in March 2018 still works to dump the next stage.

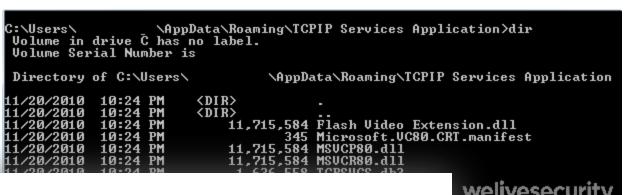
Second stage

Extracting the components

The filenames and directories are chosen dynamically. The code randomly selects the filename of an executable or DLL file located in C:\Windows\system32. It will then query its resources and extract the FileDescription field to use as a folder name. If this does not work, the code randomly chooses a folder name from the %ProgramFiles% or C:\Windows (from GetWindowsDirectoryW) directories. It avoids using a name that may clash with existing files by making sure it does not contain: windows, Microsoft, desktop, system, system32 or syswow64. If the directory already exists, the directory name is appended with "NLS_{6 digits}".

The stage's 0x102 resource is parsed and the files are dropped in either %ProgramFiles% or %AppData% in the randomly chosen folder. The creation times are changed to have the same values as kernel32.dll.

For example, here is a folder and a list of files created by picking the C:\Windows\system32\TCPSVCS.exe executable as a source of data.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

welivesecurity

nents

complex. In a nutshell, it

function)

The first file is dropped as TCPSVCS.exe which is in fact Adobe's legitimate AcroTranscoder.exe (according to its FileDescription, SHA-1: 2896738693A8F36CC7AD83EF1FA46F82F32BE5A3).

You may have noticed that the file size of some DLLs exceeds 11MB. This is because a large contiguous buffer of random data is placed inside the executable. It is possibly a way to evade detection by some security products.

Achieving persistence

The resource 0×101 of the dropper contains two 32-bit integers that dictate how the persistence should be implemented. The value of the first one specifies how the malware will achieve persistence without administrator privileges.

First integer value	Persistence mechanism
0	Do not achieve persistence
1	Scheduled task as current user
2	(HKLM HKCU)\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
3	Creation of a shortcut file (with a .lnk extension) in the subdirectory Microsoft\Windows\Start Menu\Programs\Startup under one of the environment variables: %ALLUSERSPROFILE%, %APPDATA% or %USERPROFILE%

The value of the second integer specifies how the malware should try to achieve persistence if it runs with elevated privileges.

Your account, your cookies choice We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all

optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

play name is the folder appended (the operators made sure ervice failure, the e WOW64 of the new

nne seneduled task is ereated via several eolvi interiaces. ¡FaskScheduler,

ITask, ITaskTrigger, IPersistFile and ITaskScheduler. Essentially, the malware creates a hidden task, sets the account information with the current user or the administrator information and sets the trigger.

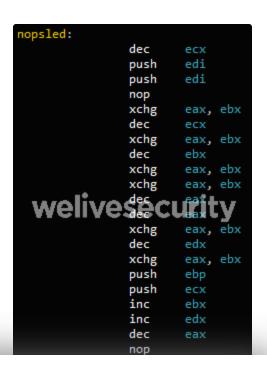
This is a daily task with a duration of 24 hours and the interval between two executions is set to 10 minutes, which means it will run all the time.

The malicious bit

In our example, the executable TCPSVCS.exe (AcroTranscoder.exe) is legitimate software side-loading the DLLs that were dropped with it. In this case, the Flash Video Extension.dll is the interesting one.

Its DLLMain function just calls a single function. Some opaque predicates are present:

After these deceptive checks, the code gets the .text section of TCPSVCS.exe, changes its protection to PAGE_EXECUTE_READWRITE and overwrites it with donothing instructions that have no side effects:



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

e effects

o Extension.dll is when the runtime point to the NOP sled, the next stage.

80-A975-411C-AB0An, it reads the dropped endent code, and uses

Creaternread to execute its content.

The content of the .db3 file is shellcode commonly used by OceanLotus. Again, we successfully unpacked its payload using the emulator script we published on GitHub.

The script extracts the final stage. This component is the backdoor that we already analysed in this white paper: OceanLotus: Old techniques, new backdoor. It is recognizable as such from the GUID {A96B020F-0000-466F-A96D-A91BBF8EAC96} that is present in the binary. The configuration of the malware is still encrypted in a PE resource. It contains almost the same configuration but the C&C servers are different from the ones that were already published:

- andreagahuvrauvin[.]com
- byronorenstein[.]com
- stienollmache[.]xyz

Once again OceanLotus showcases a large combination of techniques to stay under the radar. They came back with a "better" version of the infection process. By choosing random names and filling executables with random data, they reduce the number of reliable IoCs (hash-based and filename-based). Moreover, since they're using DLL side-loading, the attackers only have to drop the legitimate AcroTranscoder binary as-is.

Self-Extracting archives

After using RTF files, the group started using self-extracting (SFX) archives that use common document icons in an attempt to further mislead their victims. It was briefly documented by Threatbook (in Chinese). When run, these self-extracting RAR files drop and execute DLL files (with a .ocx extension) with the final payload being the previously documented {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll. Since the middle of January 2019, OceanLotus began reusing the technique but changed some configuration over time. This section will describe the technique and what they have altered to achieve their goal.

Falling for the decoy

The document THICH-THONG-LAC-HANH-THAP-THIEN-VIET-NAM (1).EXE

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

FORMANCE"

st seen in 2018. This ates it's a "JPEG Image".

1892ed0c3}.ocx 1892ed0c3}.ocx The malware drops {9ec60ada-a200-4159-b310-8071892ed0c3}.ocx (SHA-1: EFAC23B0E6395B1178BCF7086F72344B24C04DCC) as well as the image 2018 thich thong lac.jpg.

The decoy image is the following:

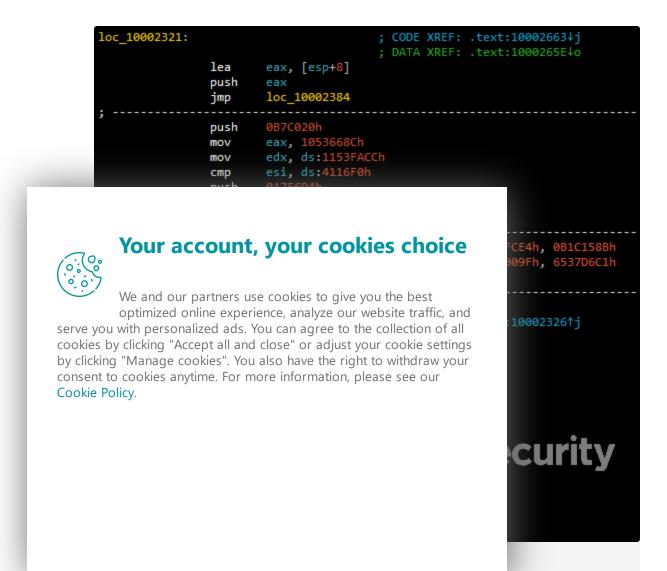


Figure 10 -- Decoy image

You may have noticed the first two lines in the SFX script invoke the OCX file twice, but it is not a mistake...

{9ec60ada-a200-4159-b310-8071892ed0c3}.ocx (ShLd.dll)

The OCX file's control flow is very similar to other OceanLotus components: there are a lot of JZ/JNZ and PUSH/RET instruction sequences interleaved with junk code.



After filtering the junk code, the export DllRegisterServer called by regsvr32.exe looks like this:

```
STATUS sub_10001F70()
 LSTATUS result; // eax
 LSTATUS v1; // edi
 int DllBaseAddress; // esi
 BYTE Data[4]; // [esp+7962h] [ebp-10h]
HKEY phkResult; // [esp+7966h] [ebp-Ch]
DWORD cbData; // [esp+796Ah] [ebp-8h]
DWORD Type; // [esp+796Eh] [ebp-4h]
 phkResult = 0;
 result = RegCreateKeyExW(
               HKEY_CURRENT USER,
               L"SOFTWARE\\Classes\\CLSID\\{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}'
               0,
               0,
               KEY ALL ACCESS,
                                          welivesecurity
               0,
               &phkResult,
               0);
 if ( phkResult )
   DllBaseAddress = f_GetDllBaseAddress();
   Type = 0;
*(_DWORD *)Data = 0;
   cbData = 4;
   v1 = RegQueryValueExW(phkResult, L"Model", 0, &Type, Data, &cbData);
   Sleep(0x3E8u);
   if ( v1 || !*(_DWORD *)Data || cbData < 4 || Type != 4 )</pre>
      *(_DWORD *)Data = 0x125211 - DllBaseAddress + f_Ret_10RegSetValueExW(phkResult, L"Model", 0, 4u, Data, 4u);
      result = RegCloseKey(phkResult);
   else
      RegDeleteValueW(phkResult, L"Model");
*(_DWORD *)Data = *(_DWORD *)Data + DllBaseAddress - 0x125211;
(*(void (__stdcall **)(int))Data)(DllBaseAddress);
result = RegCloseKey(phkResult);
 return result;
```

Figure 12 -- Main code of the installer

Basically, the first time the DllRegisterServer is called, it sets the registry value HKCU\SOFTWARE\Classes\CLSID\{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}\Model to an encoded offset in the DLL (0x10001DE0).

The second time the function is called, it reads this very same value and executes the function at that address. From there, the resource is read and executed and

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

nLotus campaigns. It ly, it drops memory and executes

-256-CBC) and that is quite easy to

The configuration is explicit: depending on the privilege level, the binary data will be written to either %appdata%\Intel\logs\BackgroundUploadTask.cpl or %windir%\System32\BackgroundUploadTask.cpl (or SysWOW64 for 64-bit systems).

Next, persistence is achieved by creating a task named

BackgroundUploadTask[junk].job where a [junk] is a collection of 0x9D and

0xA0 bytes.

The application name of the task is <code>%windir%\System32\control.exe</code> and the parameter value is the path of the dumped binary. The hidden task is set to run every day.

Structurally, the CPL file is a DLL whose internal name is ac8e06de0a6c4483af9837d96504127e.dll and that exports a CPlApplet function. This file decrypts its only resource {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll, then loads that DLL and calls its only export, DllEntry.

Backdoor configuration file

The backdoor has an encrypted configuration embedded in its resources. The structure of the configuration file is quite similar to the previous one.

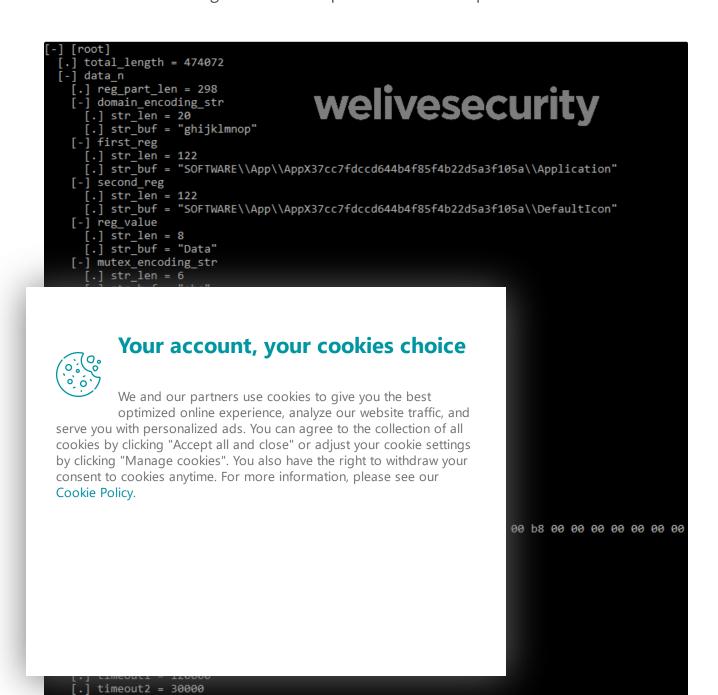


Figure 14 -- Structure of the backdoor configuration (KaitaiStruct Visualizer)

Despite the structural similarity, of the values in many of these fields have been updated comparing this to that in our white paper from March 2018. The first element of the binaries array contains a DLL (HttpProv.dll MD5: 2559738D1BD4A999126F900C7357B759) identified by Tencent but as the export name has been removed from the binary, the hashes don't match.

Going the extra mile

While hunting for samples, a few characteristics stood out. The sample just analysed appeared around July 2018 and other similar were found very recently in mid-January through early-February 2019. The infection vector used was an SFX archive dumping a legitimate, decoy document and a malicious OCX file.

Even though OceanLotus uses fake timestamps, it has been observed that the timestamp of the SFX and OCX files are always the same (0x57B0C36A (08/14/2016 @ 7:15pm UTC) and 0x498BE80F (02/06/2009 @ 7:34am UTC) respectively). This probably means that they have some kind of "builder" that reuses the same templates and just changes some characteristics.

Among the documents we analysed since early-2018, we saw different document names suggesting country-related targeting:

- The New Contact Information Of Cambodia Media(New).xls.exe
- 李建香 (个人简历).exe (fake pdf document of a CV)
- feedback, Rally in USA from July 28-29, 2018.exe

Since the discovery of the {A96B020F-0000-466F-A96D-A91BBF8EAC96}.dll backdoor and its public analysis by multiple researchers, we observed some changes in the malware's configuration data.

First, the authors started removing the names from the helper DLLs (DNSprov.dll and the two versions of HttpProv.dll).

Then the operators stopped packaging the third DLL (second version of

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

changed, perhaps to

, which are listed in the

Conclusion

OceanLotus is very active and keeps evolving. The group really focuses on varying their toolsets and decoys. They cleverly wrap their payloads with attractive documents based on current events that are likely to be of interest to their intended victims. They keep coming up with different techniques and even reuse and readapt publicly available exploit code such as for the Equation Editor exploit. Moreover, they keep improving their techniques to reduce the number of artefacts left on their victims' machines, thereby reducing the odds of detection by security products. As we have shown, a lot of in-memory operations are involved, filenames are randomly generated and the OceanLotus operators have modified their binaries to avoid being detected. Another very interesting point is that some domain names seem to be derived from a dictionary. OceanLotus is making the extra effort to continue carrying out their campaigns, but don't hold your breath...

Indicators of Compromise (IoCs)

The IoCs in this blogpost, as well as the MITRE ATT&CK attributes, are also available from our GitHub repository.

Registry keys/values:

- HKCU\SOFTWARE\Classes\CLSID\{E08A0F4B-1F65-4D4D-9A09-BD4625B9C5A1}\Model
- [HKCU|HKLM]\SOFTWARE\App\
 - AppXbf13d4ea2945444d8b13e2121cb6b663
 - Application
 - O DefaultIcon
 - AppX70162486c7554f7f80f481985d67586d
 - Application
 - O DefaultIcon

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

aliexpresscn[.]net
andreagahuvrauvin[.]com
andreagbridge[.]com
aol.straliaenollma[.]xyz
beaudrysang[.]xyz
becreybour[.]com
byronorenstein[.]com
chinaport[.]org
christienoll[.]xyz
christienollmache[.]xyz
cloud.360cn[.]info
dieordaunt[.]com
dns.chinanews[.]network
illagedrivestralia[.]xyz
karelbecker[.]com
karolinblair[.]com
lauradesnoyers[.]com
ntop.dieordaunt[.]com
Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

Files:

Documents exploiting CVE-2017-11882:			
SHA-1 hashes			
D1357B284C951470066AAA7A8228190B88A5C7C3			
49DFF13500116B6C085C5CE3DE3C233C28669678			
9DF3F0D8525EDF2B88C4A150134C7699A85A1508			
50A755B30E8F3646F9476080F2C3AE1347F8F556			
BB060E5E7F7E946613A3497D58FBF026AE7C369A			
E2D949CF06842B5F7AE6B2DFFAA49771A93A00D9			
ESET detection names			
Win32/Exploit.CVE-2017-11882.BU			
Win32/Exploit.CVE-2017-11882.A			
Win32/Exploit.Agent.KT			
Win32/Exploit.Agent.LT			
Win32/Exploit.CVE-2017-11882.EI			
SFX archives and OCX droppers:			
SHA-1 hashes			
We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.			

CC918F0DA51794F0174437D336E6F3EDFDD3CBE4
83D520E8C3FDAEFB5C8B180187B45C65590DB21A
EFAC23B0E6395B1178BCF7086F72344B24C04DCC
8B991D4F2C108FD572C9C2059685FC574591E0BE
B744878E150A2C254C867BAD610778852C66D50A
3DFC3D81572E16CEAAE3D07922255EB88068B91D
77C42F66DADF5B579F6BCD0771030ADC7AEFA97C
ESET detection names
Win32/Agent.ZUR

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	Т1193	Spearphishing Attachment	Deceitful RTF documents and self-extracting archives are sent to potential victims.
	T1204	User Execution	The user needs to execute the self-extracting archive or open the RTF document.

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

The self-extracting archives

ecute regsvr32 to run the eanLotus' backdoor.

e second stage of the ploit tries to run eanLotus' backdoor as a vice.

e second stage of the ploit tries to achieve rsistence by creating a vice.

e second stage of the

Persistence	T1060	Registry Run Keys / Start Folder	exploit tries to achieve persistence by adding a value in the Run registry key.
	T1053	Scheduled Task	The second stage of the exploit tries to achieve persistence by creating a schedule task.
	T1009	Binary Padding	The second stage of the exploit fills dropped executables with random data.
Defense Evasion	T1073	DLL Side-Loading	OceanLotus' backdoor is side-loaded by dropping a library and a legitimate, signed executable (AcroTranscoder).
	Т1112	Modify Registry	OceanLotus' backdoor stores its configuration in a registry key.
	T1027	Obfuscated Files or Information	The second stage of the exploit drops an encrypted shellcode.
	T1099	Timestomp	The creation time of the files dropped by the second stage of the exploit is set to match the creation time of kernel32.dll.
	T1083	File and Directory Discovery	OceanLotus' backdoor can list files and directories.

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

eanLotus' backdoor can ery the Windows Registry gather system ormation.

eanLotus' backdoor otures system ormation and sends it to C&C server.

eanLotus' backdoor uses

MA compression before

filtration.

Exfiltration	T1022	Data Encrypted	OceanLotus' backdoor uses RC4 encryption before exfiltration.
	T1041	Exfiltration Over Command and Control Channel	Data exfiltration is done using the already opened channel with the C&C server
	T1203	Exploitation for Client Execution	The RTF document includes an exploit to execute malicious code. (CVE-2017-11882)
Command And Control	T1094	Custom Command and Control Protocol	OceanLotus' backdoor can exfiltrate data by encoding it in the subdomain field of DNS packets.
T1065	Uncommonly Used Port	OceanLotus' backdoor use HTTP over an uncommon TCP port (14146). Port is specified in the backdoor configuration.	

Let us keep you up to date

Sign up for our newsletters

Your Fmail Address

Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.

ESET RESEARCH

CloudScout: Evasive Panda scouting cloud services

ESET RESEARCH

ESET Research Podcast:

CosmicBeetle

Embargo ransomware: Rock'n'Rust

ESET RESEARCH

Discussion

What do you think?

9 Responses















0 Comments

1 Login ▼

Start the discussion...

LOG IN WITH















Name

OR SIGN UP WITH DISQUS (?)

Share

Newest Oldest



Award-winning news, views, and insight from the ESET security community

About us

Contact us **Legal Information**

RSS Feed

ESET

Privacy Policy Manage Cookies











Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our Cookie Policy.