

ESET RESEARCH

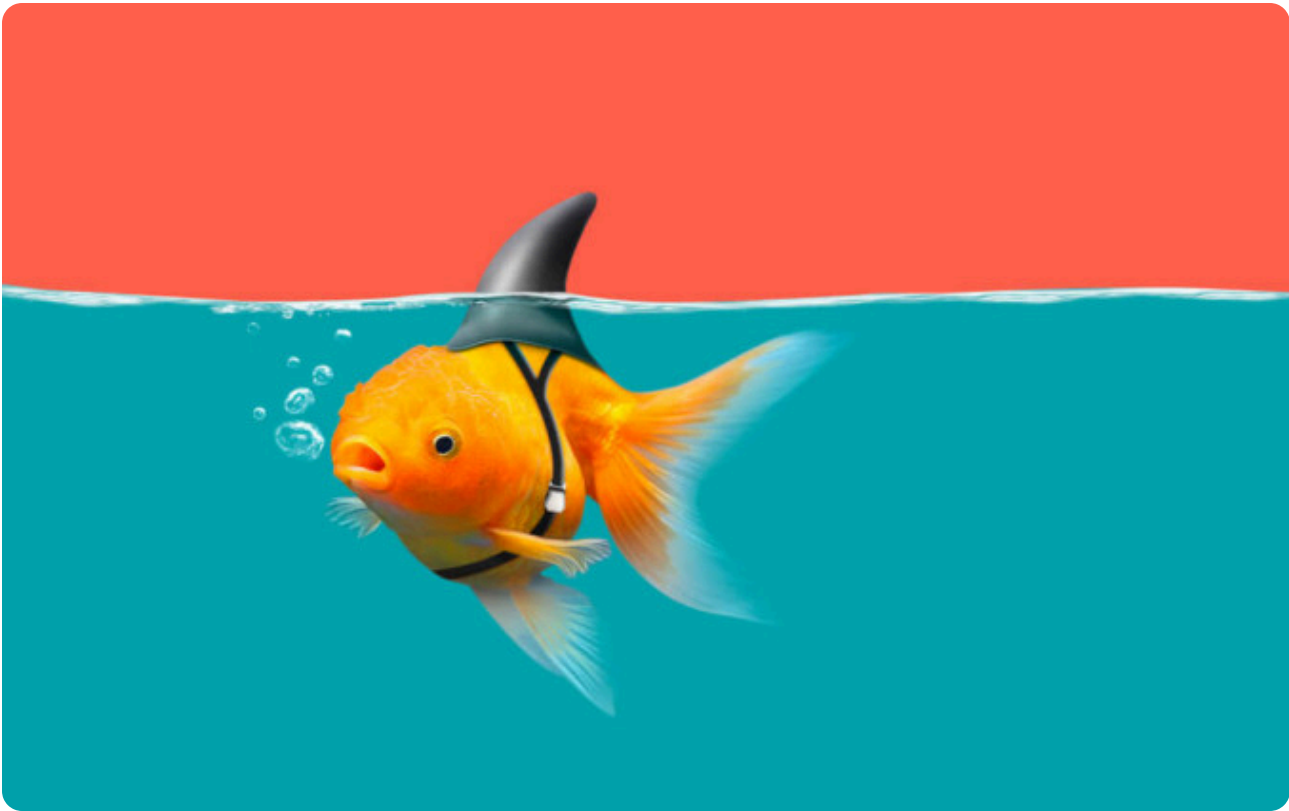
# Fake or Fake: Keeping up with OceanLotus decoys

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











 Digital Security  
Progress. Protected.

## APT Activity Report

IRAN-ALIGNED CYBERATTACKS:  
RISE IN DISRUPTIVE OPERATIONS

(eset):research

[READ NOW](#)



### 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](#)



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.

```
seg000:00000C26
seg000:00000C26
seg000:00000C26
seg000:00000C26 B8 44 EB 71 12
seg000:00000C2B BA 78 56 34 12
seg000:00000C30 31 D0
seg000:00000C32 8B 08
seg000:00000C34 8B 09
seg000:00000C36 8B 09
seg000:00000C38 66 83 C1 3C
seg000:00000C3C FF E1
seg000:00000C3C
seg000:00000C3C
seg000:00000C3C
seg000:00000C3E 90 90 90 90 90 90 90+nop_sled
seg000:00000C52 14 21 40 00 ret_gadget
```

```
public shellcode_start
shellcode_start proc near
mov     eax, 1271EB44h
mov     edx, 12345678h
xor     eax, edx           ; 0x45bd3c
mov     ecx, [eax]
mov     ecx, [ecx]
mov     ecx, [ecx]
add     cx, 3Ch           ; '<'
jmp     ecx               ; jump to 0xc58
shellcode_start endp
```

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

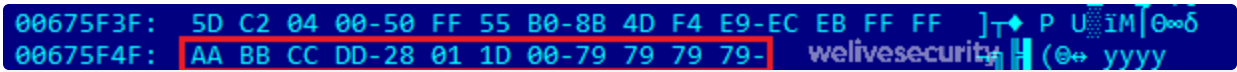


Figure 5 -- Markers at the end of the document

The 32-bit value between the AABBCDD 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.

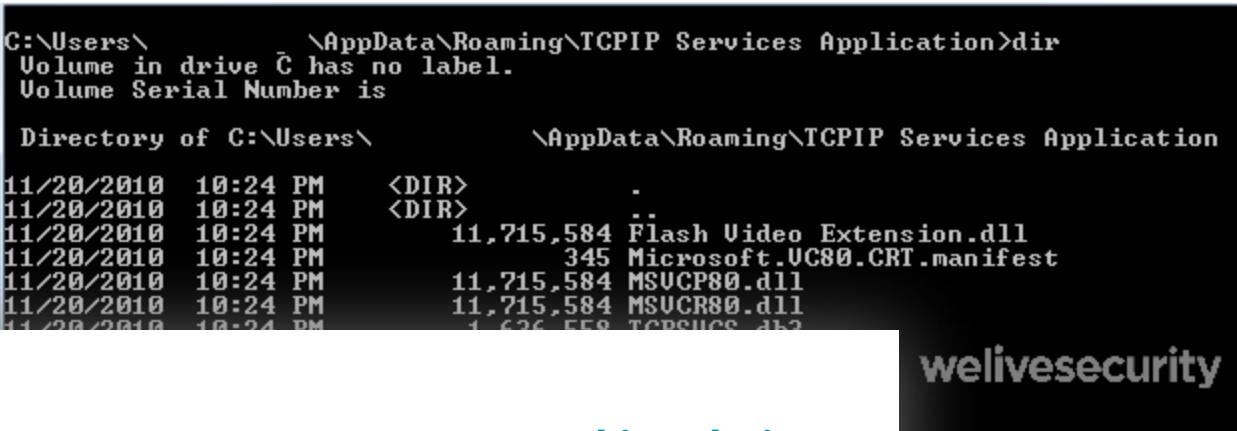
## Second stage

### 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](#).



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:

```
result = 0;
if ( "0E8j2kP9zUe9VdsFEfg2H1BV3EZAbhSKZjI52IH2pvAGji18Bi7abkTQf0ebqLPbL3erPszpTar68uA" )
{
    result = StrStrIA((LPCSTR)"0E8j2kP9zUe9VdsFEfg2H1BV3EZAbhSKZjI52IH2pvAGji18Bi7abkTQf0ebqLPbL3erPszpTar68uA", "0");
    if ( result )
    {
        if ( result <= (LPSTR)"2kP9zUe9VdsFEfg2H1BV3EZAbhSKZjI52IH2pvAGji18Bi7abkTQf0ebqLPbL3erPszpTar68uA" )
```

Figure 7 -- Opaque predicates

After these deceptive checks, the code gets the `.text` section of `TCPSVCS.exe`, changes its protection to `PAGE_EXECUTE_READWRITE` and overwrites it with do-nothing instructions that have no side effects:

```
nopsled:
    dec    ecx
    push   edi
    push   edi
    nop
    xchg    eax, ebx
    dec    ecx
    xchg    eax, ebx
    dec    ebx
    xchg    eax, ebx
    xchg    eax, ebx
    dec    eax
    dec    ebx
    xchg    eax, ebx
    dec    edx
    xchg    eax, ebx
    push   ebp
    push   ecx
    inc    ebx
    inc    edx
    dec    eax
    nop
```



### 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](#).

no side effects

Flash Video Extension.dll is then loaded when the runtime starts. It then points to the NOP sled, which is a series of no-operation instructions, the next stage.

The code then reads the dropped DLLs, finds the `Flash Video Extension.dll`, it reads the dropped DLL's metadata, finds the entry point of the dependent code, and uses

CreateThread 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

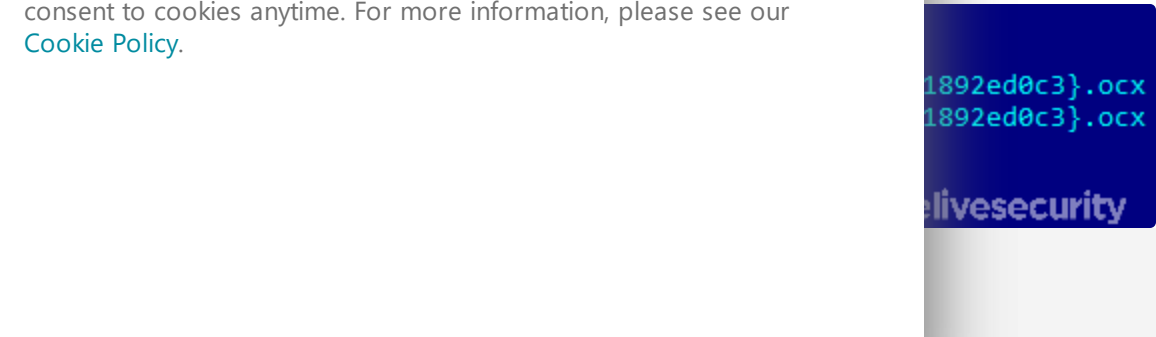
After using RTF files, the group started using self-extracting (SFX) archives that use common document icons in an attempt to further mislead their victims. It was briefly documented by [Threatbook \(in Chinese\)](#). When run, these self-extracting RAR files drop and execute DLL files (with a .ocx extension) 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  
PERFORMANCE"

**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](#).

...st seen in 2018. This  
...ates it’s a “JPEG Image”.









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

```
LSTATUS 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,
        0,
        KEY_ALL_ACCESS,
        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 )
        {
            *(_DWORD *)Data = 0x125211 - DllBaseAddress + f_Ret_10001DE0();
            RegSetValueExW(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



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\ul>  - AppXbf13d4ea2945444d8b13e2121cb6b663\ul>  - Application
  - DefaultIcon
- AppX70162486c7554f7f80f481985d67586d\ul>- Application
- 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



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](#).



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

## MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	<b>T1193</b>	Spearphishing Attachment	Deceitful RTF documents and self-extracting archives are sent to potential victims.
	<b>T1204</b>	User Execution	The user needs to execute the self-extracting archive or open the RTF document.
Execution	<b>T1059</b>	Process Execution	The self-extracting archives execute <b>regsvr32</b> to run the OceanLotus' backdoor.
	<b>T1055</b>	Process Injection	In the second stage of the exploit tries to run OceanLotus' backdoor as a service.
Persistence	<b>T1059</b>	Process Execution	In the second stage of the exploit tries to achieve persistence by creating a service.
	<b>T1055</b>	Process Injection	In the second stage of the exploit tries to achieve persistence by creating a service.



### 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](#).

Persistence	<b>T1060</b>	Registry Run Keys / Start Folder	exploit tries to achieve persistence by adding a value in the Run registry key.
	<b>T1053</b>	Scheduled Task	The second stage of the exploit tries to achieve persistence by creating a schedule task.
	<b>T1009</b>	Binary Padding	The second stage of the exploit fills dropped executables with random data.
	<b>T1073</b>	DLL Side-Loading	OceanLotus' backdoor is side-loaded by dropping a library and a legitimate, signed executable (AcroTranscoder).
	<b>T1112</b>	Modify Registry	OceanLotus' backdoor stores its configuration in a registry key.
Defense Evasion	<b>T1027</b>	Obfuscated Files or Information	The second stage of the exploit drops an encrypted shellcode.
	<b>T1099</b>	Timestomp	The creation time of the files dropped by the second stage of the exploit is set to match the creation time of <b>kerne132.dll</b> .
	<b>T1083</b>	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](#).

OceanLotus' backdoor can query the Windows Registry to gather system information.

OceanLotus' backdoor captures system information and sends it to the C&C server.

OceanLotus' backdoor uses GZIP compression before transmission.

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 Email 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

ESET RESEARCH  
Embargo  
ransomware:  
Rock’n’Rust

Discussion

What do you think?  
9 Responses

  
Upvote

  
Funny

  
Love


  
Surprised

  
Angry

  
Sad







0 Comments

1 Login ▼




Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS



Name



• Share

Best

Newest

Oldest

welivesecurity™

BY



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](#).