Carbanak gang is back and packing new guns

www.welivesecurity.com/2015/09/08/carbanak-gang-is-back-and-packing-new-guns/

By Anton Cherepanov posted 8 Sep 2015 - 10:49AM

The Carbanak *financial APT* group made the headlines when Group-IB and Fox-IT broke the news in December 2014, followed by the Kaspersky report in February 2015. The two reports describe the same cybercriminal gang which stole up to several hundreds of millions of dollars from various financial institutions.

However, the story is interesting not only because of the large amount of money stolen but also from a technical point of view. The Carbanak team does not just blindly compromise large numbers of computers and try to 'milk the cow' as other actors do, instead they act like a mature APT-group. They only compromise specific high-value targets and once inside the company networks, move laterally to hosts that can be monetized.

A few days ago CSIS published details about new Carbanak samples found in the wild.

In this blog we will describe the latest developments in the Carbanak story.

Casino hotel hack

At the end of August, we detected an attempt to compromise the network of a casino hotel in the USA. The infection vector used in this attack may have been a spearphishing e-mail with a malicious attachment using an RTF-exploit or .SCR file. The attackers' aim was to compromise PoS servers used in payment processing.

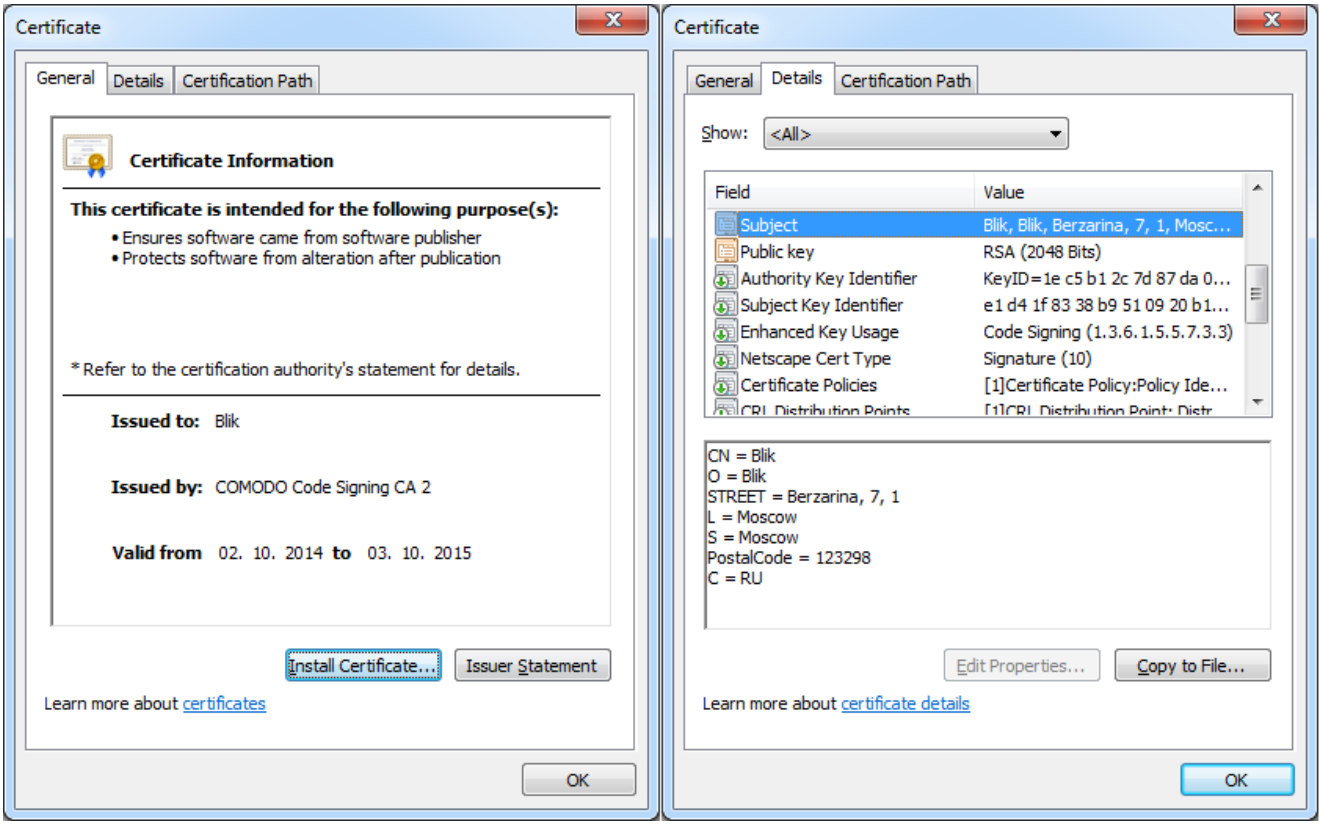
The main backdoor used by attackers was the open-source Tiny Meterpreter. In this case, however, the source was modified – the process injection to svchost.exe was added to its functionality.

This Tiny Meterpreter backdoor dropped two different malware families:

- Win32/Spy.Sekur – well known malware used by the Carbanak gang
- Win32/Wemosis – a PoS RAM Scraper backdoor

As mentioned here by our colleagues from TrendMicro, Carbanak malware is capable of targeting Epicor/NSB PoS systems, while Win32/Wemosis is a general-purpose PoS RAM Scraper which targets any PoS that stores card data in the memory. The Wemosis backdoor is written in Delphi and allows the attacker to control an infected computer remotely.

Both executables were digitally signed with the same certificate:



The certificate details:

Company name: Blik
Validity: from 02 October 2014 to 03 October 2015
Thumbprint: 0d0971b6735265b28f39c1f015518768e375e2a3
Serial number: 00d95d2caa093bf43a029f7e2916eae7fb
Subject: CN = Blik
O = Blik
STREET = Berzarina, 7, 1
L = Moscow
S = Moscow
PostalCode = 123298
C = RU

This certificate was also used in the digital signature of a third malware family used by the same gang: Win32/Spy.Agent.ORM.

Win32/Spy.Agent.ORM – overview

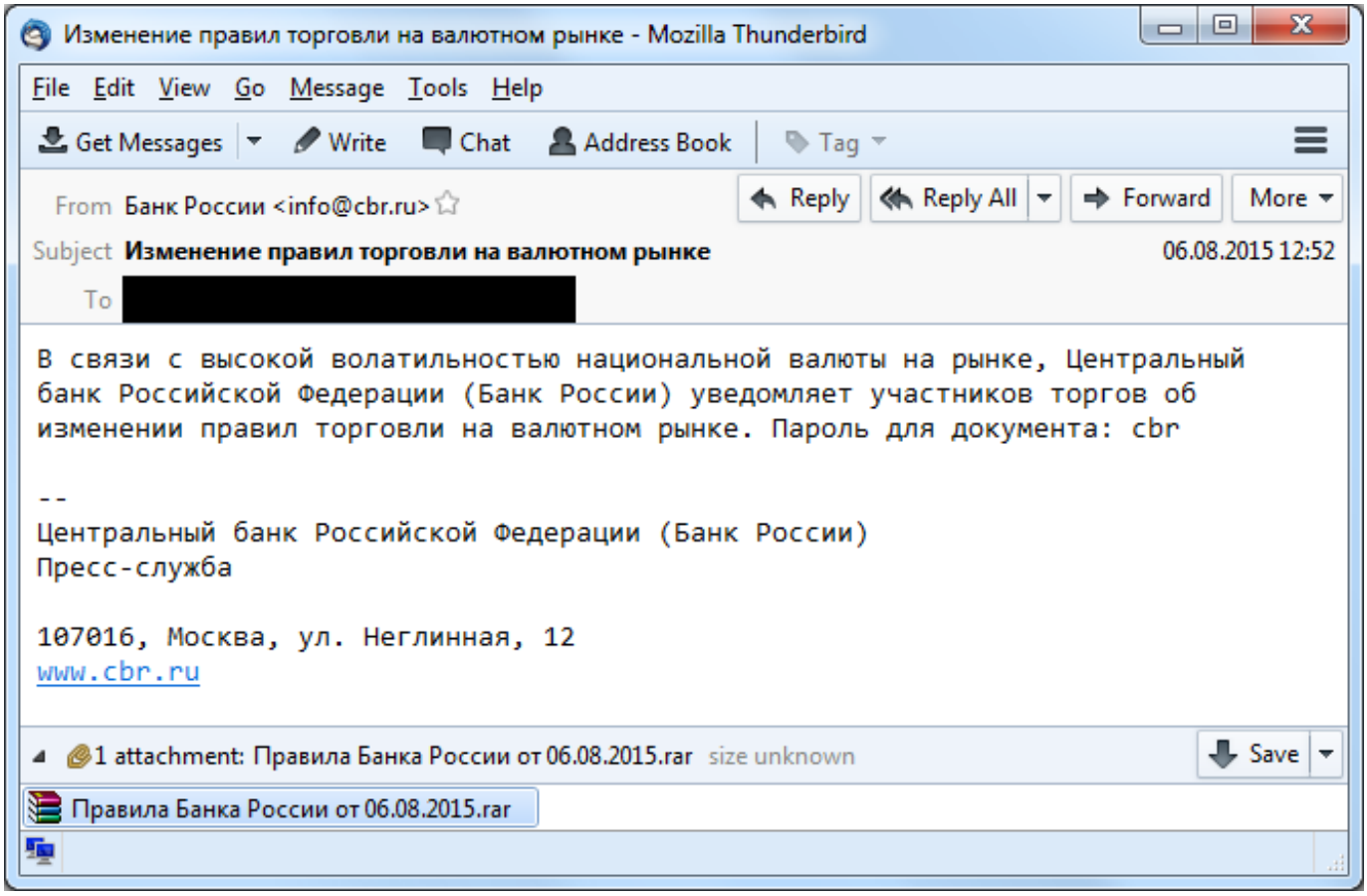
Win32/Spy.Agent.ORM (also known as *Win32/Toshliph*) is a trojan used as one of their first-stage payloads by the Carbanak gang. The binary of the testing version was signed with a **Blik** certificate: moreover, *Spy.Agent.ORM* shares some similarities in the code with “the regular” Carbanak malware.

The *Win32/Spy.Agent.ORM* malware family is already known in the industry because of two blogposts. In July 2015 security company Cyphort reported the compromise of a news portal and a banking site – rbc.ua and unicredit.ua. It turns out that the compromised sites served *Win32/Spy.Agent.ORM*. After that, Blue Coat reported a spearphishing attempt targeting Central Bank of Armenia employees, the payload being the same.

This malware appeared on our radar at the beginning of summer 2015, and afterwards we started to track it.

We have seen attempts to attack various companies in Russia and Ukraine using spearphishing e-mails that have malicious attachments consisting of .SCR files or .RTF exploits.

Here is an example of a spearphishing email sent to one of the biggest Forex-trading companies:



Roughly translated from Russian to English, it says:

“Due to the high volatility of the ruble exchange rate the Bank of Russia sends rules of trading on the currency market. Password the attached document: cbr”

Here is another example of a spear phishing attempt. Email with this text was sent to the largest electronic payment service in Russia:

Постановлением Роскомнадзора от 04.08.2015г. Вам необходимо заблокировать материалы попадающие под Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) “О персональных данных”. Перечень материалов в документе.

Пароль roscomnadzor

Another rough translation from Russian to English:

“According to Roscomnadzor prescript you should block the materials, which you can find in the attachment. Password is roscomnadzor”

We have seen similar .SCR files with following filenames:

- АО «АЛЬФА-БАНК» ДОГОВОР.scr (Alfabank contract)
- Перечень материалов для блокировки от 04.08.2015г.scr (List to block)
- Postanovlene_ob_ustranenii_18.08.2015.pdf %LOTS_OF_SPACES% ..scr
- Правила Банка России от 06.08.2015.pdf %LOTS_OF_SPACES% .scr (Rules of Bank of Russia)

All these attachments contained a password protected archive with .SCR file. The files had Adobe Acrobat reader icon or MS Word icons.

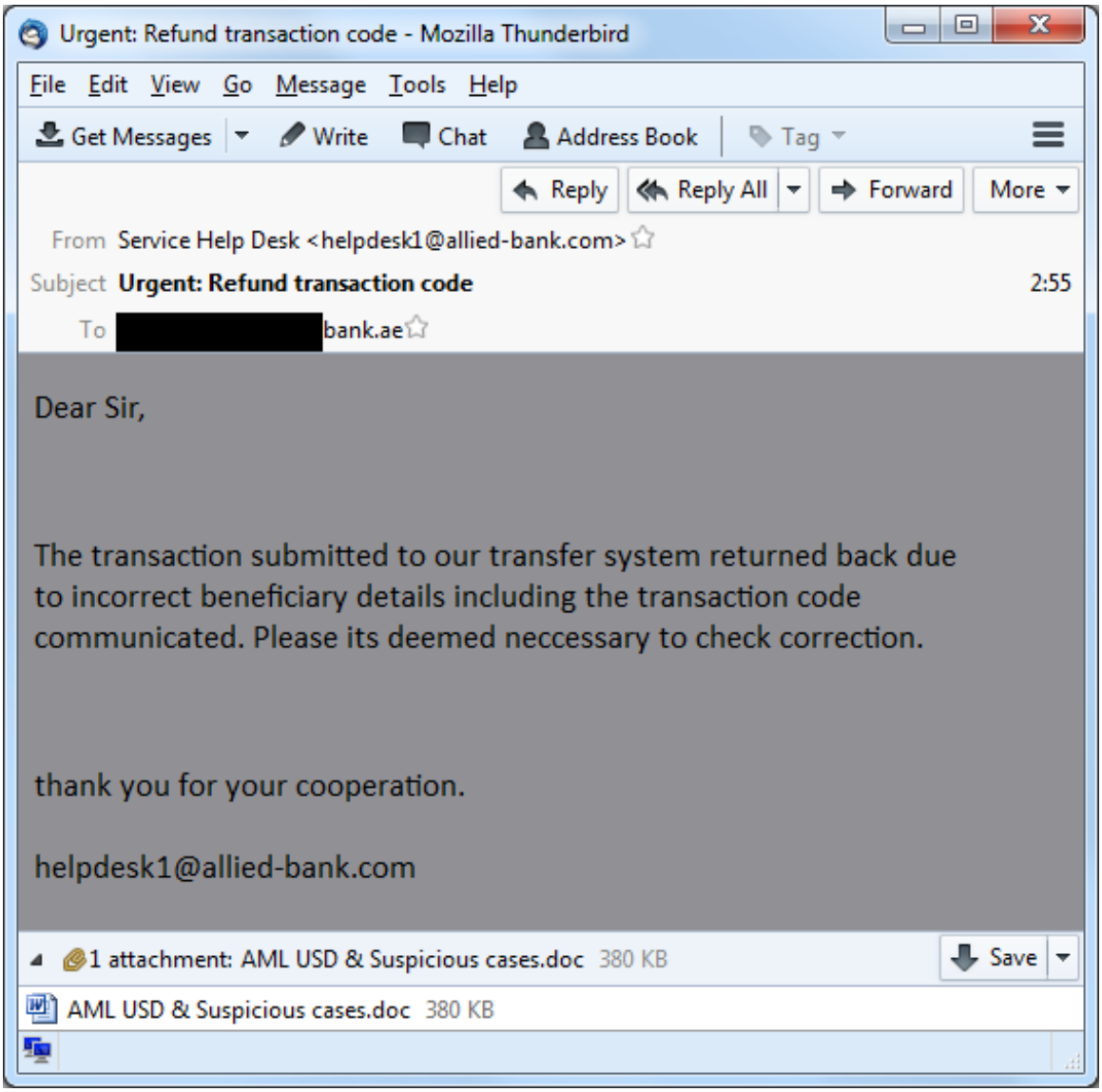
In other cases attackers used RTF files with different exploits, including an exploit for one of the latest Microsoft Office vulnerabilities, CVE-2015-1770, which was patched by Microsoft in June 2015 in MS15-059.

We have seen RTF files with the following names used in attacks:

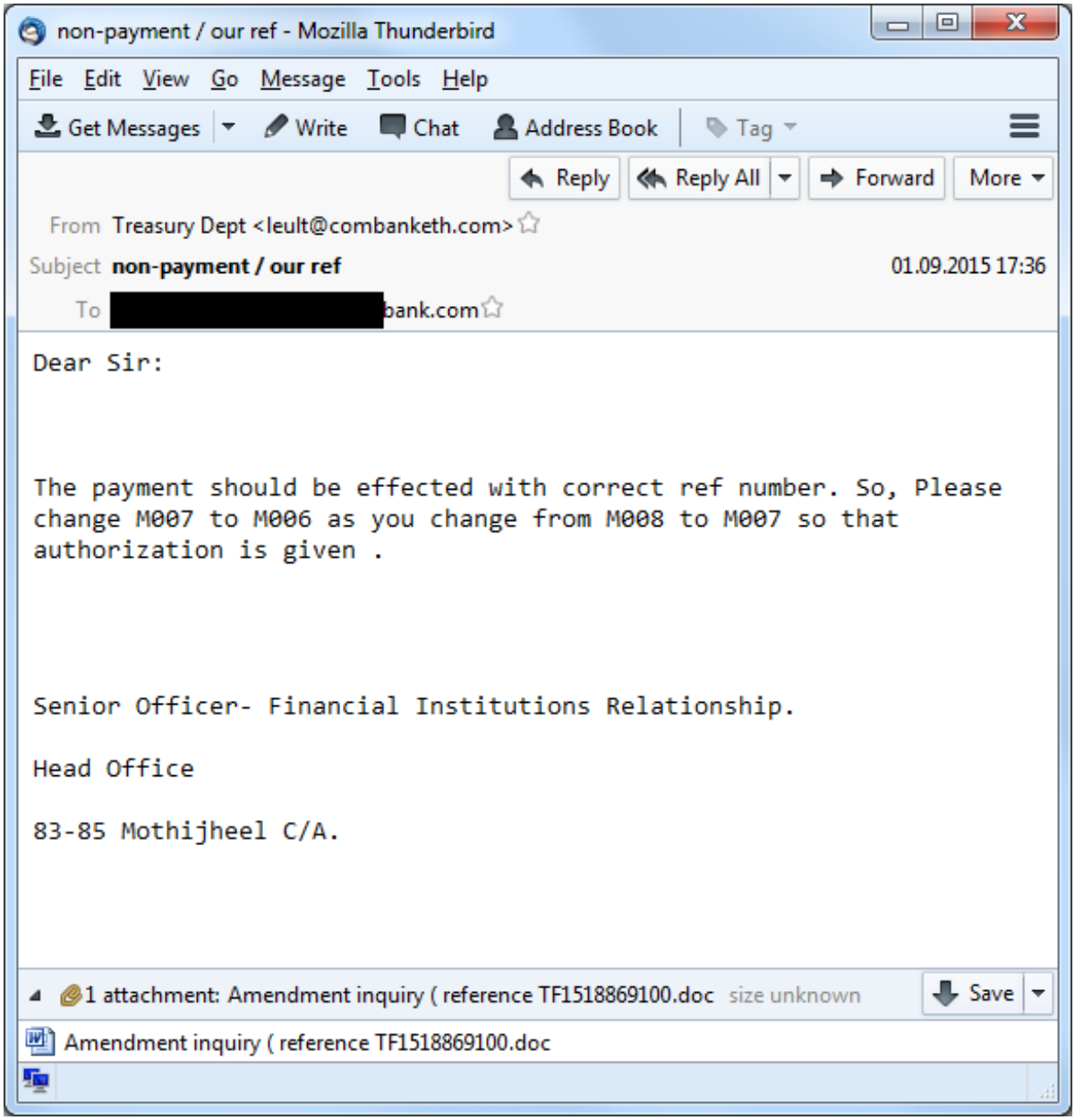
- prikaz-451.doc
- REMITTANCE ADVICE ON REJECTION.doc
- PROOF OF REMITTANCE ADVICE .doc
- HDHS739_230715_010711_A17C7148_INTERNAL.doc
- Բանկերի և բանկային գործունեության մասին ՀՀ օրենք 27.07.2015.doc (Armenian: The Law on Banks and Banking 27.07.2015)
- PAYMENT DETAILS.doc

- АО «АЛЬФА-БАНК» ДОГОВОР.doc (Russian: Alpha-bank contract)
- AML REPORTS_20082015_APPLICATION FORM-USD-MR VYDIAR.doc
- Anti-Money Laudering & Suspicious cases.doc
- ApplicationXformXUSDXduplicateXpayment.doc
- AML USD & Suspicious cases.doc
- Amendment inquiry (reference TF1518869100.doc
- Information 2.doc

Here is example of a spearphishing message that was sent to a bank in the United Arab Emirates:



Here is example of a spearphishing email that was sent to a German bank:



Win32/Spy.Agent.ORM – Technical details

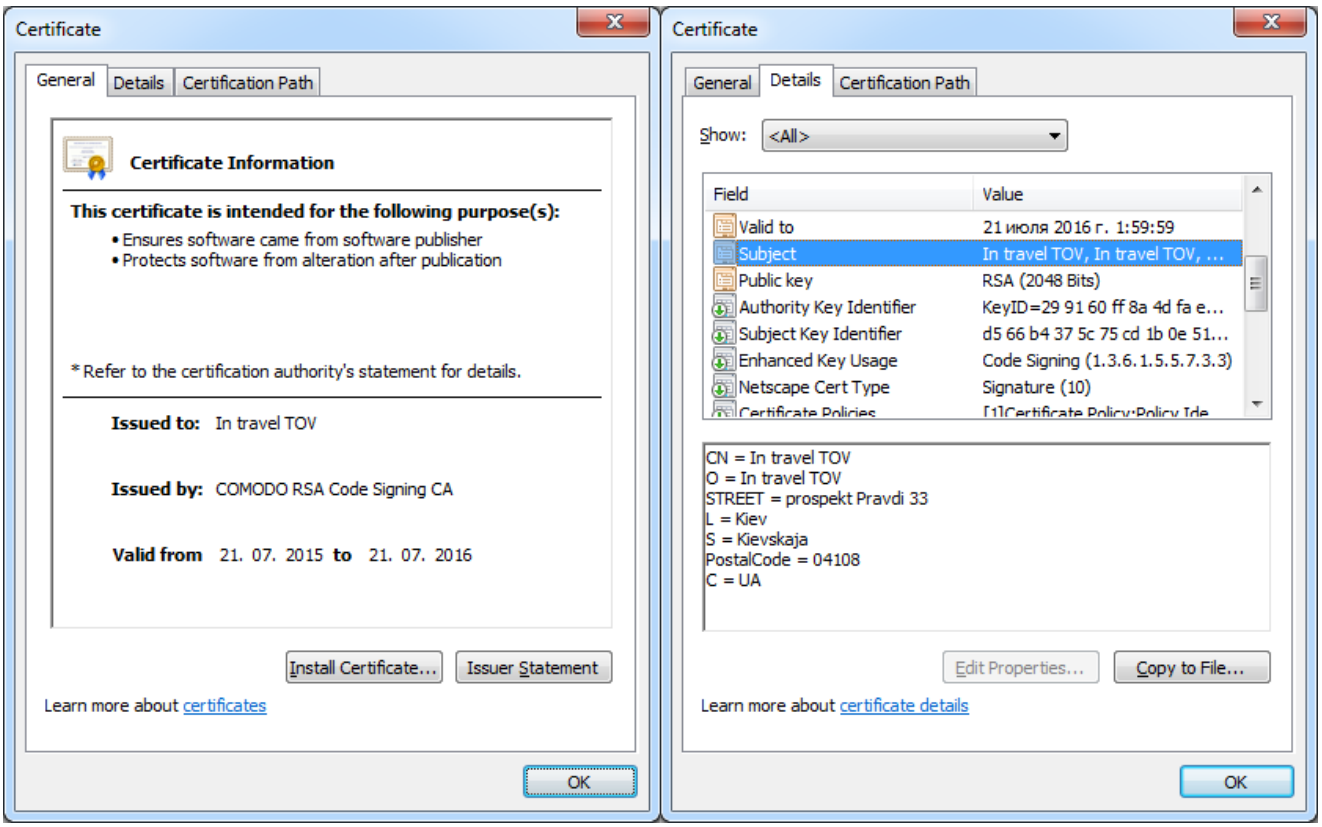
Win32/Spy.Agent.ORM is a small and simple backdoor that enables the attackers to assess the victim. When executed the trojan connects to a C&C server and receives commands to grab screenshots, enumerate running processes and get information about the system and campaign ID. Based on that information malware operator decides whether the infected computer is useful: that is, whether it's the intended target or just a system that was accidentally infected.

Here is list of commands that it can receive from C&C server:

Command	Purpose

0x02	Collects information about computer: Computer Name, User Name, Windows Version, Architecture (32/64 bit) and campaign ID
0x03	Collects list of running processes
0x04	Downloads binary to %TEMP% and executes
0x05	Updates itself
0x06	Deletes itself
0x07	Makes screenshot
0x08	Loads binary in the memory, without dropping to the disk

The latest sample of this malware family found in the wild is also digitally signed with a different certificate:



The certificate details:

Company name: In travel TOV

Validity: from 21 July 2015 to 21 July 2016
Thumbprint: 7809fbd8d24949124283b9ff14d12da497d9c724
Serial number: 00dfd915e32c5f3181a0cdf0aff50f8052
Subject: CN = In travel TOV
O = In travel TOV
STREET = prospekt Pravdi 33
L = Kiev
S = Kievskaja
PostalCode = 04108
C = UA

Also, the latest sample is able to gain system privileges via an exploit and install itself as a system service. The trojan attempts to exploit a vulnerability – CVE-2015-2426 in the OpenType manager module (ATMFD.dll) – which was patched by Microsoft in MS15-078. The exploit for this vulnerability was leaked in a Hacking Team dump.

```
.text:00401461 loc_401461:
.text:00401461      push    250Ah
.text:00401466      push    offset aAtmfd_dll       ; "atmfd.dll"
.text:0040146B      push    ebx
.text:0040146C      call    [ebp+gdi32_NamedEscape]
.text:0040146F      cmp     eax, 0FFFFFF21h
.text:00401474      jz      short loc_4014AC
.text:00401476      mov     eax, [ebp+var_30]
.text:00401479      cmp     [ebp+var_4], ebx
.text:0040147C      jz      short loc_401483
.text:0040147E      add     eax, 8
.text:00401481      jmp     short loc_401486
```

The digital certificate for **Blik** used in this case is not the only link between Win32/Spy.Agent.ORM and Win32/Spy.Sekur (Carbanak malware). They share similarities in code – take a look at the function that generates the BOTID-value, for example:

```
1  char generate_botid()
2  {
3    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5    mac_size = get_mac_address(&mac_buffer);
6    v1 = 0;
7    if ( mac_size > 0 )
8      v1 = mac_buffer ^ BYTE2(mac_buffer);
9    v11 = 128 - mac_size;
10   pGetComputerNameA = get_api_by_hash(0, kernel32_GetComputerNameA_hash);
11   pGetComputerNameA(v3, &mac_buffer + mac_size, &v11);
12   calc_hash(&mac_buffer, mac_size + v11);
13   format_string = string_decrypt("%08x%08x");
14   call_wvsprintf(&buffer, format_string, v1);
15   free(format_string);
16   str_init(&v10, 32, 0, -1);
```

```
  v5 = string_decrypt(aHollyda1);
  str_append(v5, -1);
  free(v5);
  str_append_char(0x30);
  str_append(&buffer, -1);
  str_copy(&g_botid, generated_botid, v9);
  str_free(&generated_botid);
  return 1;
}
```

Win32/Spy.Sekur (Carbanak)

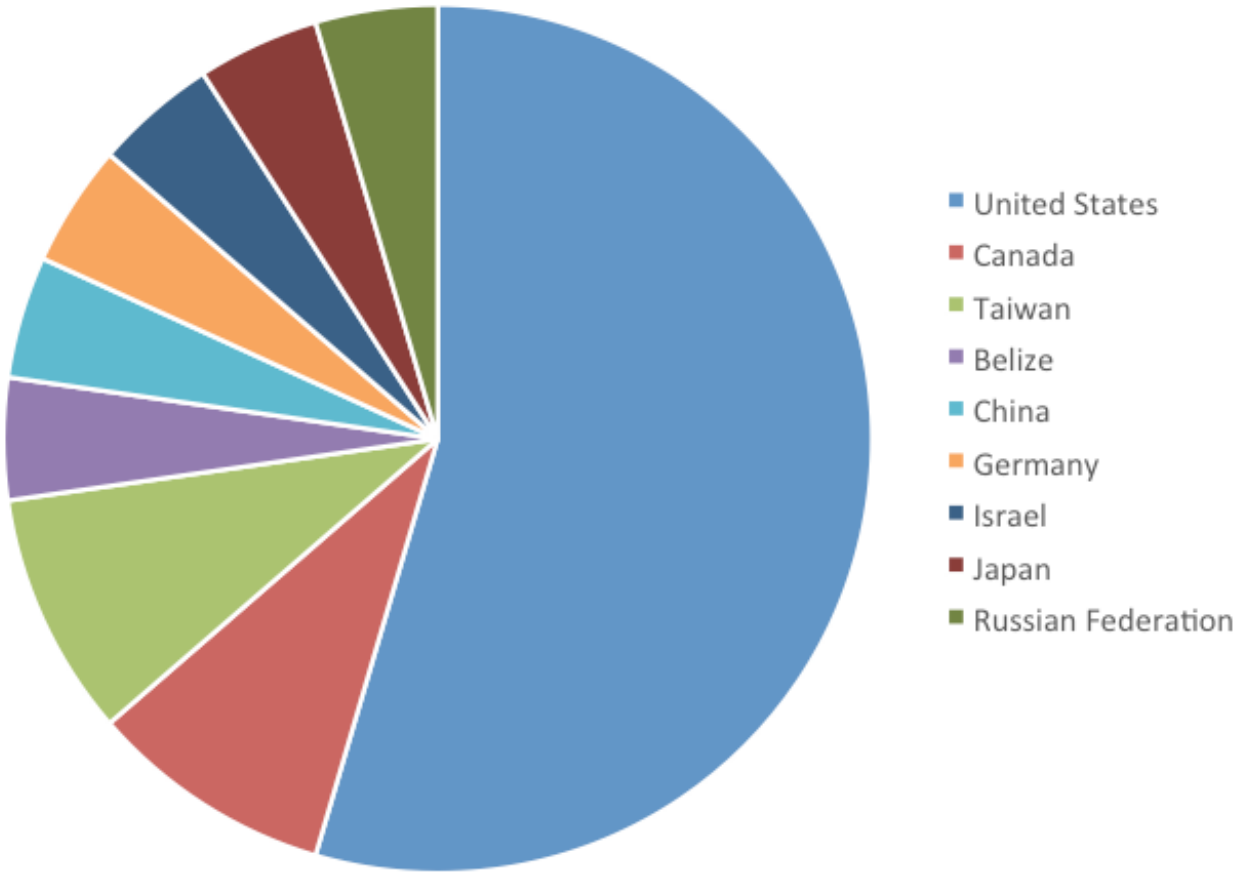
```
int generate_botid()
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v0 = 0;
  SizePointer = 0;
  GetAdaptersInfo(0, &SizePointer);
  adapter_info = mem_alloc(SizePointer);
  if ( !GetAdaptersInfo(adapter_info, &SizePointer) )
  {
    for ( i = adapter_info; i; i = i->Next )
    {
      if ( i != adapter_info )
      {
        v3 = i->Type;
        if ( v3 != 71 && v3 != 6 )
          continue;
      }
      mem_copy(&xor_buffer, i->Address, 8);
      if ( i->Type == 6 )
        break;
    }
  }
  mem_free(adapter_info);
  nSize = 64;
  GetComputerNameA(Buffer, &nSize);
  x = 0;
  do
  {
    *(&xor_buffer + x) ^= Buffer[v0];
    v0 = v0 + 1 < nSize ? v0 + 1 : 0;
    ++x;
  }
  while ( x < 8 );
  word_id = xor_buffer;
  dword_id = *(&xor_buffer + 1);
  v7 = string_decrypt(&v11, "%04x%08x");
  wsprintfA(g_botid, *v7, word_id, dword_id);
  return mem_free(v11);
}
```

Win32/Spy.Agent.ORM

The BOTID-value is a unique value generated on the basis of the hardware parameters of infected computer, and it's used by attackers for computer identification. In both cases generation is based on the MAC-address and computer name and the resulting value is formatted using the **wsprintf** –function.

Sinkhole statistics

Our sinkhole of some C&C domains used by the Win32/Wemosis has resulted in hits from bots in the following countries.



As the attacks are highly targeted, the total number of victims is low in absolute numbers. Victims in the USA are situated in several states, including Nevada (Las Vegas), California, and New York, and include casinos and hotels.

Conclusions

Even after it has reportedly stolen hundreds of millions of dollars, the infamous Carbanak APT group isn't resting on its laurels. On the contrary, it is very active and keeps attacking specific targets related to the finance industry, including banks, Forex-trading companies, and even an American casino hotel. Recently, we have detected malware used by the Carbanak group in the following countries, among others:

- United States of America
- Germany
- United Arab Emirates

As described in this blog post, the gang doesn't use just one malware family to carry out its operations but several. While the code in the different families – Carbanak (Win32/Spy.Sekur), Win32/Spy.Agent.ORM, and Win32/Wemosis – is different it does contain similar traits, including the same digital certificate.

Furthermore, the attackers are updating their arsenal with the latest exploits, such as the Microsoft Office remote code execution vulnerability, CVE-2015-1770, or the zero-day exploit leaked in the Hacking Team dumps, CVE-2015-2426.

We continue to monitor the Carbanak threats. For any enquiries or sample submissions related to the subject, contact as at: threatintel@eset.com.

Indicators of Compromise (IoC)

Trojan.Win32/Spy.Sekur (Carbanak malware) SHA-1:

A048C093C5DA06AF148CA75299960F618F878B3A
3552338D471B7A406D8F7E264E93B848075235C0
3A9A23C01393A4046A5F38FDBAC371D5D4A282F1
8D5F2BF805A9047D58309788A3C9E8DE395469A8
BCF9E4DCE910E94739728158C98578A8D145BE56
8330BC5A3DCC52A22E50187080A60D6DBF23E7E6
E838004A216E58C44553A168760100B497E514E8
CF1F97879A6EB26FEDC7207D6679DFA221DD2D45
726779134020402072792 3CC7C8D65AFC18F6F5B
F8CBF647A64028CAE835A750EF3F8D1AA216E46C
33870482BA7DE041587D4B809574B458C0673E94
3927835C620058EFCADF76642489FC13AACE305B
D678BD90257CF859C055A82B4A082F9182EB3437
0B8605D0293D04BBF610103039768CBE62E2FAAE
7A9BE31078BC9B5FECE94BC1A9F45B7DBF0FCE12

RTF-exploits SHA-1:

D71E310ADF183F02E36B06D166F8E3AD54FDBCC9
5B6ABA51215A9662987F59AEF6CAE0A9E3A720B8
1AD84A244B7D4FBB4D89D023B21715B346027E49
E8514BF4C4E1F35FB1737C2F28A4A4CED07AA649
68EA12CDCCEE01D50C23EBC29CAA96BF40925DC6
AC95F01487B4F179A1F10684B1E0A5656940A005

B4A94A214FC664B8D184154431E1C5A73CA0AE63

Trojan.Win32/Spy.Sekur C2 servers:

weekend-service.com:80
seven-sky.org:80
comixed.org:80
91.207.60.68:80
89.144.14.65:80
87.98.217.9:443
82.163.78.188:443
50.62.171.62:700
31.3.155.123:443
216.170.116.120:80
216.170.116.120:700
216.170.116.120:443
194.146.180.58:80
193.203.48.41:700
185.29.9.28:443
178.209.50.245:443
162.221.183.11:80
162.221.183.11:443
162.221.183.109:443
141.255.167.28:443
104.232.32.62:443
104.232.32.61:443

Trojan.Win32/Spy.Agent.ORM SHA-1:

2DD485729E0402FD652CF613E172EA834B5C9077
5E8B566095FD6A98949EF5C479CE290F520DD9E2
8C2C08111F76C84C7573CF07C3D319A43180E734
36093A6004A9502079B054041BADC43C69A0BDEB
6F452C76F7AC00FE1463314F5AA0A80EC4F7360C
850E9A10E6D20D33C8D2C765E22771E8919FC3EE
A09F520DDED0D5292A5FA48E80DE02F9AF718D06
3707029DC5CBBE17FD4DE34134847F92E7324C45
905D0842CC246A772C595B8CF4A4E9E517683EB7
237784574AFB8868213C900C18A114D3FA528B95
6090853934833D0814F9239E6746161491CCCB44

3672C9F4E7F647F2AF9AE6D5EA8D9C7FF16FAF40
EC5DADAACAE763D0E55CE6A78C9A5F57B01A5135
4E8EE08FF4F8DC06AFF8DE2E476AFAFBA58BDC11
A734193F550DDA5C1FFD9FEC3A0186A0A793449C
EFC0555418A6ED641047D29178D0DA3AEFA7ADEB
B79E6A21D8C2813EC2279727746BDB685180751A
4DB58E7D0FCA8D6748E17087EB34E562B78E1FDE
567749B4F2330F02DD181C6C0840191CEE2186D9
3ACEA9477B219FC6B8C0A734E67339AE2EB2AA5B
2896814E5F8860E620AC633AF53A55D9AA21F8C0
84CC02B3C10306BFCECE8BF274B57475B056C6D6
207FF65543DAC6D1D9F86DFFD891C507AD24018B
D627DD4E3850CBD571AFC4799A331054C7080B0D
DCC932B878B374D47540D43A2DEE97F37D68267F
983D33F547588A59B53D7F794768B264454446D5
19E7C7A78C5D58945B615D98FF0990389485933F
DED83A1E3B6630D69077976CC01321FBC946DCE2
170142C042BF32FF86AF680EAD86CD1AF075B0CB
A77336620DF96642691C1E5B6C91511BFA76A5BE
3CEF1CA36A78CBA308FB29A46B20E5CA22D03289
DD01331ABFF03525506CDCBAC4D76CB4EFD602A4

RTF-exploits SHA-1:

1F9462AA39645376C74566D55866F7921BD848F7
81E43D653ACD2B55C8D3107E5B50007870D84D76
AC68AD2E5F5802A6AB9E7E1C1EC7FAB3C6BDBAA4
F869C7EA683337A2249908C21B9D3283CC2DD780
7162BB61CD36ED8B7EE98CBD0BFFEC33D34DD3E7
5943ABCF662DC9634B714B1358164B65E5651D15
A40BDF005B4B469D2C7BED1766C9DA9823E1CFB7
833A8D88BE11807BAE966D56B28AF7B3CC34DBCD
AF7564EE7959142C3B0D9EB8129605C2AE582CB7
DCC932B878B374D47540D43A2DEE97F37D68267F
6FF3AE5BA4E9A312602CBD44A398A02AB0437378
32AA4911BC6AB8098E496CD88790FF7147EC6AC3

Trojan.Win32/Spy.Agent.ORM – C2 Servers:

192.52.166.66

84.200.4.226
78.128.92.117
176.31.157.62
clients4-google.com (192.169.82.86)
adobe-dns-3-adobe.com (78.128.92.112)
img.in-travelusa.com (192.169.82.86)

Tiny meterpreter SHA-1:

28D514FE46D8B5720FE27C40C3889F3B45967CC7
0B0884992F28A3C1439DBA60007076B22831CE51

Win32/Wemosis (PoS RAM Scraper) SHA-1:

5E31DB305A97736C0F419A3F2F8F093FF6A1F56F

Win32/Wemosis – C2 server:

198.100.119.14

Author Anton Cherepanov, ESET