



Customer Login

News

Blog

Press

SWEPT

Career

Contact

About CSIS

Home > CSIS > Blog >

Blog

Carbanak returns

2015-09-02 21:32:52 | Peter Kruse

Short background

Just recently, CSIS carried out a forensic analysis involving a Microsoft Windows client that was compromised in an attempt to conduct fraudulent online banking transactions. As part of the forensic task, we managed to isolate a signed binary, which we later identified as a new Carbanak sample.

The \$1bn heist

Carbanak (aka Anunak) has been around for several years and it was highlighted in a report released by researchers at Kaspersky in February 2015 with the headline "*The Great Bank Robbery: Carbanak cybergang steals \$1bn from 100 financial institutions worldwide*" (ref 1). As expected, such a colorful title would quickly draw the attention of international press and a few days later the story was headlining the media.

At the time when the Carbanak story broke into the media, several researchers from CSIS were attending the *Kaspersky Security Analyst Summit* (TheSAS2015) hosted in Mexico. We soon got very busy answering questions from concerned customers. As our investigation at that time progressed, it turned out, that none of our customers was affected by Carbanak. Unfortunately, this would not last forever. As stated earlier, during the last week, we uncovered a new variant of Carbanak. From our analysis, it comes clear that Carbanak has returned and has been confirmed targeting large corporations in Europe and in the USA. Attack methods are spear phishing.

The first new variant

As already mentioned, the new variant of Carbanak is digitally signed (more details on that follow later in the blog post). It was found on the compromised Windows 7 host at this location:
C://Program/DataMozilla/svchost.exe. On Windows XP, the location would be: *C://Documents and Settings/All Users/Application Data/Mozilla/svchost.exe*. At the same time, it adds a runkey to registry, so that the code would be executed upon reboot of the system.

After having reversed the code, we are now able to confirm that the folder and the filename are both static and thus can be used as an IoC (Indicator of Compromise). Carbanak injects itself into the svchost.exe process. In this way, it manages to hide its presence in memory.

As several other advanced data stealing threats, Carbanak utilizes plugins. The plugins are installed using Carbanak's own protocol and communicating with a hardcoded IP address over TCP port 443. The two plugins downloaded during our analysis were "wi.exe" and "klgconfig.plugin". Both of them have already been mentioned in the Kaspersky report (ref. 2).

When communicating with the C&C, the sample in question registers the BOT with a predefined string: *yamota0* – followed by a 16 bytes randomly generated string used as BOTID e.g.: "*yamota0832ebfe80090bd64*". See screenshot below:

```
00000000 28 01 00 00 00 00 00 00 00 00 02 00 00 00 00 00 (. . . . .
00000010 00 00 00 00 18 fc 40 00 00 00 02 00 00 00 00 00 ' . . . . @.
00000018 27 01 17 00 00 00 17 00 00 00 02 00 00 00 00 00 ' . . . . @.
00000028 00 00 00 00 18 fc 40 00 79 61 6d 6f 74 61 30 38 ' . . . . @. yamota08
00000038 33 32 65 62 66 65 38 30 30 39 30 62 64 36 34 32ebfe80 090bd64
00000047 20 0f 00 00 00 0f 00 00 00 02 02 00 00 00 00 ' . . . . G.
00000057 00 00 00 00 10 cc 47 00 69 67 2e 70 6c 75 67 ' . . . . G.
0000005f 0e 6b 6c 67 63 6f 6e 66 ' . . . . klgconf ig.plugin
0000006e 20 01 07 00 00 00 07 00 00 02 03 00 00 00 00 ' . . . . G.
0000007e 00 00 00 00 10 cc 47 00 ' . . . . G.
00000086 06 77 69 2e 65 78 65 ' . . . . wi.exe
00000000 20 01 04 00 00 00 04 00 00 00 02 02 00 00 00 00 ' . . . .
00000010 00 00 00 00 00 00 00 00 01 00 00 10 00 00 00 03 ' . . . .
00000018 00 00 00 00 20 01 04 00 00 00 00 00 00 00 00 00 ' . . . .
00000028 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 ' . . . .
00000038 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ . . . .
00000048 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ' . . . . @.
00000058 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ' . . . .
00000068 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 ' . . . .
00000078 0e 0f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ' . . . . !.!.!Th
00000088 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f ' . . . . is progr am canno
00000098 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
000000a8 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 mode . . . $.
000000b8 26 38 33 7d 62 59 5d 2e 62 59 5d 2e 62 59 5d 2e &83}by]. by]. by].
000000c8 a1 56 00 2e 60 59 5d 2e 62 59 5c 2e 59 59 5d 2e .V. \y]. by\ .yy].
000000d8 9e 2e e4 2e 73 59 5d 2e a0 b5 92 2e 70 59 5d 2e . . . . sy]. . . . py].
000000e8 a0 b5 91 2e 63 59 5d 2e 52 69 63 68 62 59 5d 2e . . . . cy]. Richby].
000000f8 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 ' . . . . PE..L..
00000108 64 af ba 55 00 00 00 00 00 00 00 e0 00 02 01 d..U..
00000118 0b 01 0b 00 00 40 00 00 00 c0 00 00 00 00 00 00 ' . . . . @.
00000128 20 13 00 00 00 10 00 00 00 50 00 00 00 00 40 00 ' . . . . .P. . . @.
00000138 00 10 00 00 02 00 00 05 00 01 00 00 00 00 00 ' . . . .
00000148 05 00 01 00 00 00 00 00 00 20 01 00 00 04 00 00 ' . . . .
00000158 00 00 00 02 00 40 81 00 00 00 10 00 00 00 00 ' . . . . @.
00000168 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 ' . . . .
00000178 00 00 00 00 00 00 00 00 ac 51 00 00 c8 00 00 00 ' . . . .
00000188 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ' . . . . Q.
```

There are several differences between these new variants and the previously observed Carbanak specimen (ref 2). These include:

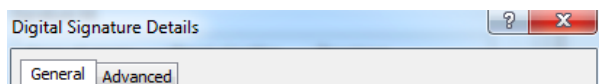
- new geographical targets
- a new proprietary protocol
- the use of random files (i. e. main component is static) and mutexes
- predefined IP address (previous variants were using domains)

Besides these, the binaries are almost identical with the previous Carbanak samples.

For one of the new samples, the C&C server can be tied to a well-known bulletproof hosting company.

Signed Carbanak malware

As shown below, this new variant of Carbanak was digitally signed using Comodo:




Heimdal Security protects against banker trojan malware.

Press Contact

Peter Kruse
Partner & Security Specialist
pkr@csis.dk
PGP Key ID: 0x49006F37



**Digital Signature Information**
This digital signature is OK.

Signer information

Name:

Blik

E-mail:

Not available

Signing time:

Thursday, 23 July, 2015 10:28:47

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
COMODO Time S...	Not available	Thursday, 23 July, 2...

Details

OK

CN = Blik
O = Blik
STREET = Berzarina, 7, 1
L = Moscow
S = Moscow
PostalCode = 123298
C = RU

Certificate

General

Details

Certification Path

Show: <All>

Field	Value
Serial number	00 d9 5d 2c aa 09 3b f4 3a 02 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	COMODO Code Signing CA 2, ...
Valid from	Thursday, 02 October, 2014 0...
Valid to	Saturday, 03 October, 2015 0...
Subject	Blik, Blik, Berzarina, 7, 1, Mosc...
Public key	RSA (2048 Bits)

CN = Blik

O = Blik

STREET = Berzarina, 7, 1

L = Moscow

S = Moscow

PostalCode = 123298

C = RU

Edit Properties...

Copy to File...


Learn more about [certificate details](#)

OK

Certificate valid from 02-Oct-2014 till 03-Oct-2015

After some investigations, we located additional information related to the company "Blik".

Компания ООО "БЛИК" - краткая справка



Компания зарегистрирована 3 апреля 2014 года регистратором Межрайонная инспекция Федеральной налоговой службы № 46 по г. Москве. ГЕНЕРАЛЬНЫЙ ДИРЕКТОР организации - ЧУНЯЕВА СВЕТЛАНА АЛЕКСАНДРОВНА. Компания ООО "БЛИК" находится по адресу 123298, ГОРОД МОСКВА, УЛИЦА БЕРЗАРИНА, 7, 1, основным видом деятельности является «Прочая оптовая торговля». Организация также осуществляет деятельность по следующим неосновным направлениям: «Деятельность агентов по оптовой торговле лесоматериалами и строительными материалами», «Деятельность агентов по оптовой торговле пищевыми продуктами, включая напитки, и табачными изделиями», «Оптовая торговля фруктами, овощами и картофелем», «Оптовая торговля мясом, мясом птицы, продуктами и консервами из мяса и мяса птицы», «Оптовая торговля молочными продуктами, яйцами, пищевыми маслами и жирами», «Оптовая торговля алкогольными и другими напитками», «Неспециализированная оптовая торговля пищевыми продуктами, включая напитки, и табачными изделиями», «Оптовая торговля одеждой, включая нательное белье, и обувью», «Оптовая торговля бытовыми электротоварами, радио- и телеаппаратурой», «Оптовая торговля изделиями из керамики и стекла, обоями, чистящими средствами», «Оптовая торговля прочими непродовольственными потребительскими товарами», «Оптовая торговля лесоматериалами, строительными материалами и санитарно-техническим

торговлей сельскохозяйственными, строительными материалами и строительным оборудованием», «Оптовая торговля скляными изделиями, ручными инструментами, водопроводным и отопительным оборудованием», «Прочая розничная торговля в неспециализированных магазинах», «Розничная торговля фруктами, овощами и картофелем», «Розничная торговля мясом, мясом птицы, продуктами и консервами из мяса и мяса птицы», «Розничная торговля алкогольными и другими напитками», «Прочая розничная торговля пищевыми продуктами в специализированных магазинах», «Розничная торговля одеждой». Организации присвоен ИНН 7734721873, ОГРН 1147746359530.

Company registration date: April 3, 2014.

Director: Chunyaeva Svetlana Alexandrova.

Company address: 123298, Moscow, street. Berzarina, 7, 1.

The registration information of the company states "Other wholesale" as the primary business activity of "Blik". The organization also operates the following non-core activities:

- wholesale trade of timber and building materials
- wholesale trade of food, beverages and tobacco
- wholesale of fruit and vegetables
- wholesale of meat, poultry, products and canned meat and poultry meat
- wholesale of dairy products, eggs and edible oils and fats
- wholesale of alcoholic and other beverages

When searching further, we only managed to find the following domain related to this company: blikSCO.com

Updated Date: 2015-04-01 17:55:18.274469

Creation Date: 2014-10-01

Registrant Name: Svetlana Chunyaeva

Registrant Organization: Blik

Registrant Street: Berzarina, 7, 1

Registrant City: Moscow

Registrant Postal Code: 123298

Registrant Country: Russian Federation

Registrant Phone: +7.4997030345

Registrant Email: admin@blikSCO.com

One interesting question arises, as it sometimes does in cases like this: "why would a company working within this kind of business area ever need a code-signing certificate?"

This brings us to several observations:

- The timeline between the dates of company registration and certificate issue could indicate that criminals have probably registered their own company using fake identity or a stolen passport
- This time, the criminals have obviously registered a real company instead of using a stolen certificate for code signing as they did previously as report by Kaspersky.
- We speculate that the main purpose of this company is to receive money from fraudulent transactions. As stated in the Kaspersky report, Carbanak-related transfers are rather huge. Possibly, they have registered a company and opened bank accounts in order to receive their stolen money while having full control of the transferring process.

Conclusions:

Carbanak is what we define as a financial APT. In its nature, it is very targeted and it is being deployed in small numbers. In this way, it tends to slide under the radar. We have observed at least four different new variants of Carbanak targeting key financial personal in large international corporations.

It is our intention to release a technical write-up on our analysis of Carbanak. Meanwhile samples have been shared with trusted entities to ensure that detection is deployed in order to eradicate the threat through various security solutions.

References

Ref 1:

<http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide>

Ref 2:

https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

// Yurii Khvyi and Peter Kruse, CSIS