Целевые атаки на банкоматы. Способы совершения и способы обнаружения

GROUP IB

Ведущий специалист по компьютерной криминалистике
Матвеева Веста

Расследование киберпреступлений

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА И РАССЛЕДОВАНИЕ

СЕТЕВЫЕ АТАКИ

- → ХИЩЕНИЕ В ИНТЕРНЕТ-БАНКИНГЕ
- → DDOS-АТАКИ
- → ВЗЛОМ IP-ТЕЛЕФОНИИ
- → НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (ВЕБ-САЙТ / БД / СЕРВЕР / ПОЧТА)
- → СЕТЕВОЙ ШАНТАЖ / ВЫМОГАТЕЛЬСТВО

САБОТАЖ И ИНСАЙД

- → УТЕЧКИ ИНФОРМАЦИИ
- → УНИЧТОЖЕНИЕ ИНФОРМАЦИИ
- → МАНИПУЛЯЦИЯ ДАННЫМИ С ЦЕЛЬЮ МОШЕННИЧЕСТВА
- → БЛОКИРОВАНИЕ ДОСТУПА

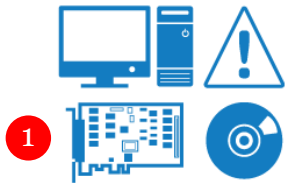
ЦЕЛЕВЫЕ АТАКИ / ПРОМЫШЛЕННЫЙ ШПИОНАЖ

- → ЦЕЛЕВЫЕ ВИРУСНЫЕ АТАКИ
- → «ПРОСЛУШКА» СЕТЕВЫХ КАНАЛОВ СВЯЗИ
- → УСТАНОВКА ПРОГРАММНЫХ ЗАКЛАДОК
- → ОРГАНИЗАЦИЯ ЦИФРОВЫХ «ЧЕРНЫХ ВХОДОВ»

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ

- → МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ВЫСОКИХ ТЕХНОЛОГИЙ
- → ВЫМОГАТЕЛЬСТВО,
- → РАЗГЛАШЕНИЕ КОММЕРЧЕСКОЙ ТАЙНЫ И КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
- → НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ТОВАРНОГО ЗНАКА И БРЕНДА

Компьютерная криминалистика и исследование вредоносного кода



→ Сбор цифровых доказательств

Сбор сведений об инциденте и определение источников хранения доказательной информации по инциденту, их сохранение и оформление в соответствии с нормами государственного законодательства

→ Проведение криминалистического исследования

Для разбора инцидента, получения и закрепления доказательств, являющихся допустимыми в судебном разбирательстве

→ Экспресс-криминалистика

Проведение криминалистических исследований в сжатые сроки

→ Участие специалистов в оперативно-розыскных мероприятиях

Минимизация рисков уничтожения доказательств в случае неквалифицированных действий, а также обеспечение должного правового статуса технических мероприятий

Компьютерная криминалистика и исследование вредоносного кода

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА И РАССЛЕДОВАНИЕ

1

→ **Исследование вредоносных программ**

Определение функциональных возможностей исполняемых файлов, установление сетевых адресов. Разбор и дешифрация файлов конфигурации и иных служебных данных

2

→ **Сравнение исходных кодов и программных продуктов**

Проведение компьютерных исследований современного плагиата в области ИТ

3

→ **Исследование мобильных устройств**

Проведение исследований мобильных устройств на логическом и физическом уровнях, а также на уровне файловой системы

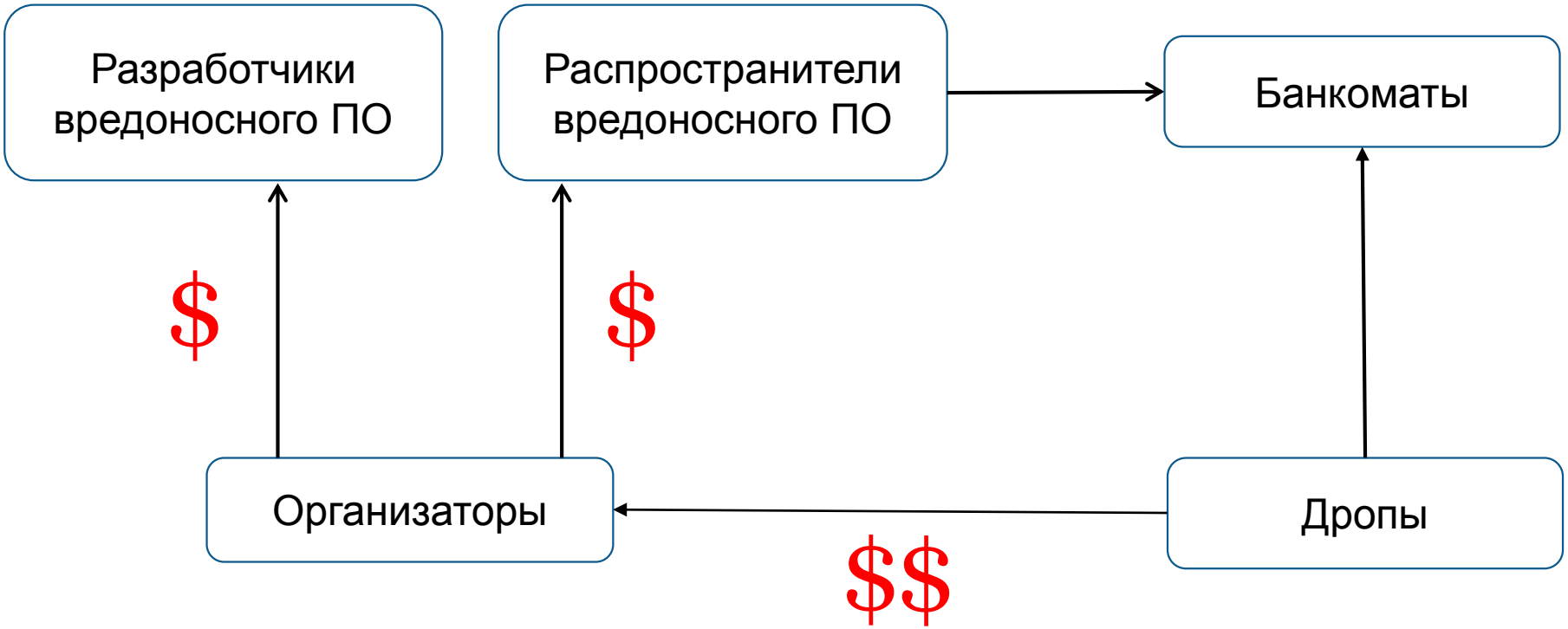
4

→ **Аутсорсинг услуг**

Объединение услуг в комплексе, что позволяет эффективно управлять инцидентами и минимизировать временные и финансовые затраты на них

ПРЕСТУПНЫЕ ГРУППЫ

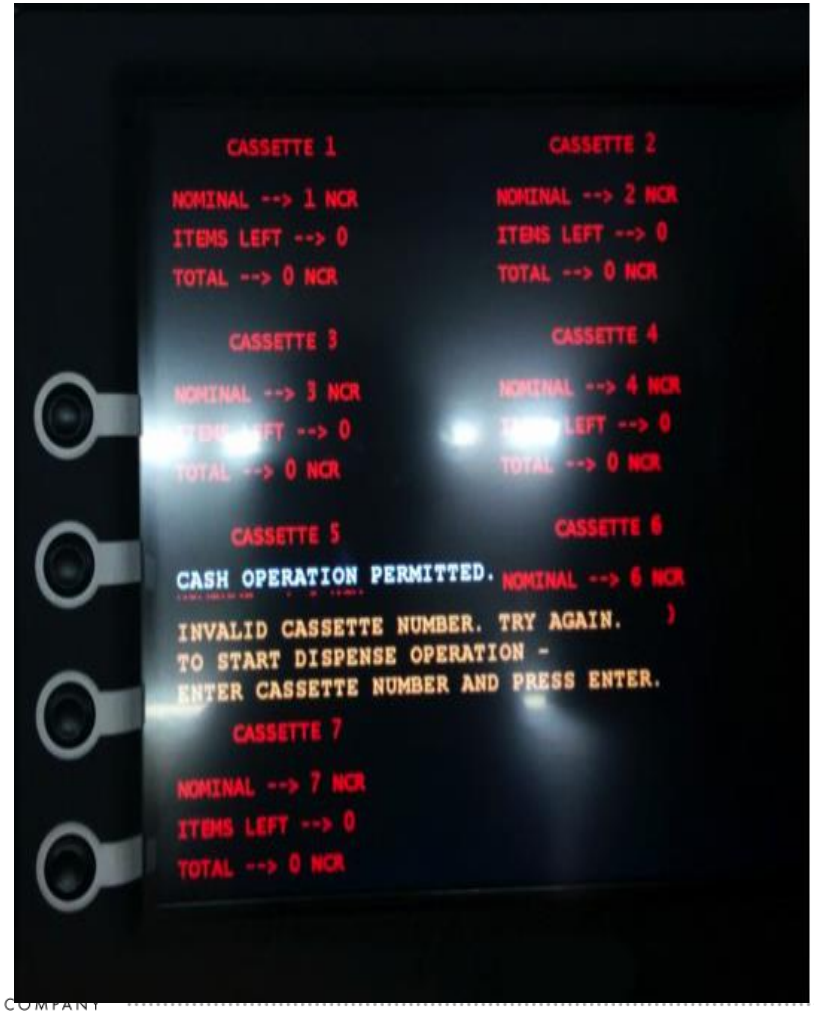
Преступная группа



- ✓ Вредоносная программа – 2000 – 5000 $
- ✓ Шифрование исполняемых файлов – 20 – 30 $
- ✓ Средний размер хищения 20 000 $

ЗАРАЖЕНИЕ БАНКОМАТОВ

Вредоносная программа диспенсер (Платформа NCR) он же Backdoor.MSIL.Tyupkin

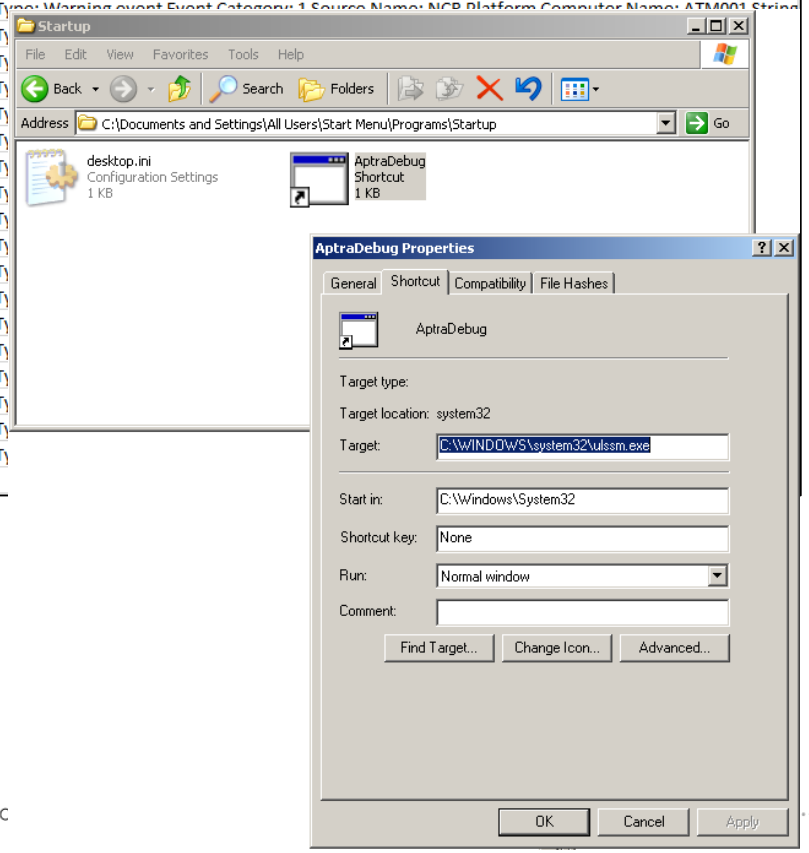


1. Заражение банкомата
2. Ожидание команд с ПИН-клавиатуры
3. Отключение локальной сети
4. Подача команд напрямую диспенсеру

Вредоносная программа диспенсер (Платформа NCR)

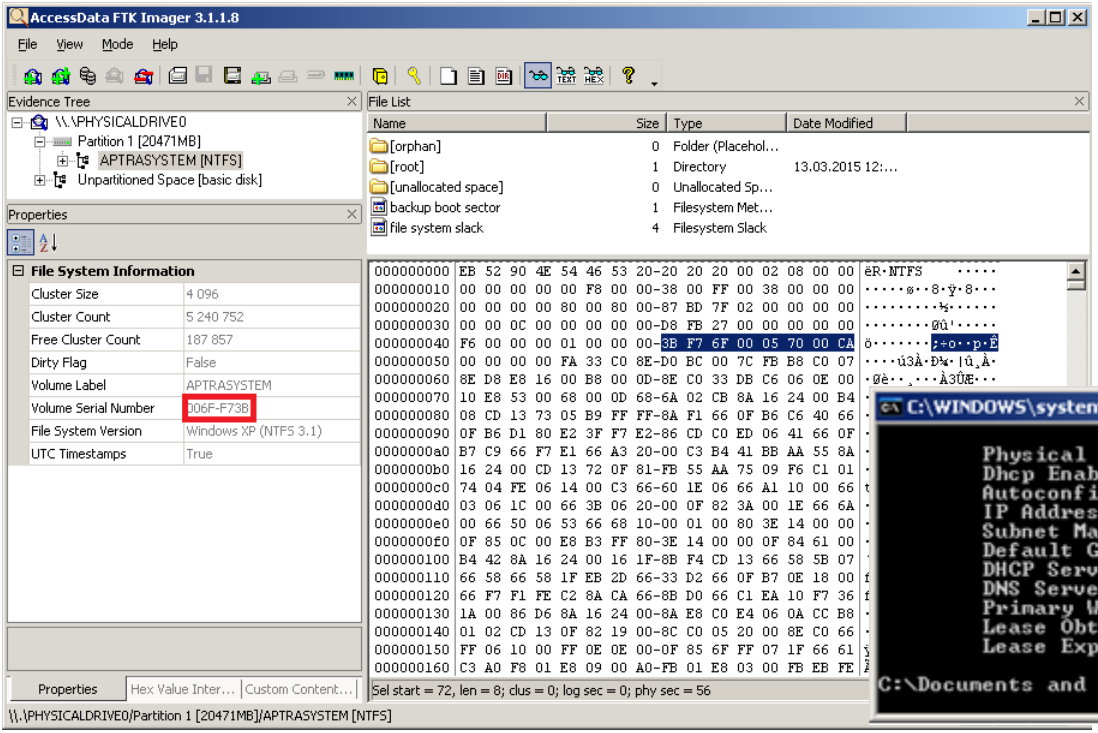
1. Копирование исполняемого файла с загрузочного компакт диска. Добавление ярлыка в автозагрузку.

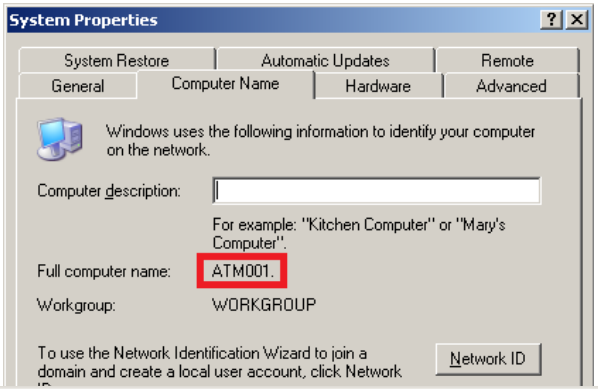
16.03.2015	10:00:03	M...	REG	NTUSER key	Content Modification Time	ATM001	[\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\D_Autorun\DefaultIcon] (default): [REG_SZ] D:\HBCD\HBCDMenu.exe
16.03.2015	10:00:03	M...	REG	NTUSER key	Content Modification Time	ATM001	[\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\D_Autorun\DefaultLabel] (default): [REG_SZ] CLAYDERMAN
16.03.2015	10:00:03	M...	REG	NTUSER key	Content Modification Time	ATM001	[\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\D_Autorun] Value: No values stored in key.
16.03.2015	10:00:04	M...	EVT	WinEVT	Content Modification Time	ATM001	[2147483917 / 0x8000010d] Record Number: 33960 Event Type: Information event Event Category: 0 Source Name: PlugPlayManager Computer Nam
16.03.2015	10:00:04	...B	EVT	WinEVT	Creation Time	ATM001	[2147483917 / 0x8000010d] Record Number: 33960 Event Type: Information event Event Category: 0 Source Name: PlugPlayManager Computer Nam
16.03.2015	10:00:08	M...	EVT	WinEVT	Content Modification Time	ATM001	[21 / 0x00000015] Record Number: 78955 Event Ty
16.03.2015	10:00:08	...B	EVT	WinEVT	Creation Time	ATM001	[21 / 0x00000015] Record Number: 78955 Event Ty
16.03.2015	10:00:09	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78958 Event Ty
16.03.2015	10:00:09	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78959 Event Ty
16.03.2015	10:00:09	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78959 Event Ty
16.03.2015	10:00:09	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78956 Event Ty
16.03.2015	10:00:09	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78957 Event Ty
16.03.2015	10:00:09	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78957 Event Ty
16.03.2015	10:00:09	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78958 Event Ty
16.03.2015	10:00:09	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78956 Event Ty
16.03.2015	10:00:13	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78963 Event Ty
16.03.2015	10:00:13	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78962 Event Ty
16.03.2015	10:00:13	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78961 Event Ty
16.03.2015	10:00:13	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78962 Event Ty
16.03.2015	10:00:13	...B	EVT	WinEVT	Creation Time	ATM001	[22 / 0x00000016] Record Number: 78960 Event Ty
16.03.2015	10:00:13	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78960 Event Ty
16.03.2015	10:00:13	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78963 Event Ty
16.03.2015	10:00:13	M...	EVT	WinEVT	Content Modification Time	ATM001	[22 / 0x00000016] Record Number: 78961 Event Ty
16.03.2015	10:01:47	...B	FILE	NTFS_DETECT	crtime	ATM001	TSK:/WINDOWS/system32/ulssm.exe

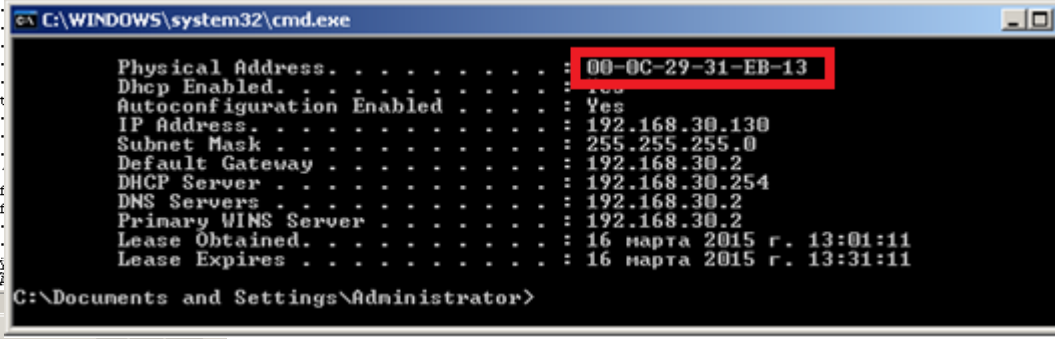


GROUP IB

Зараженная система





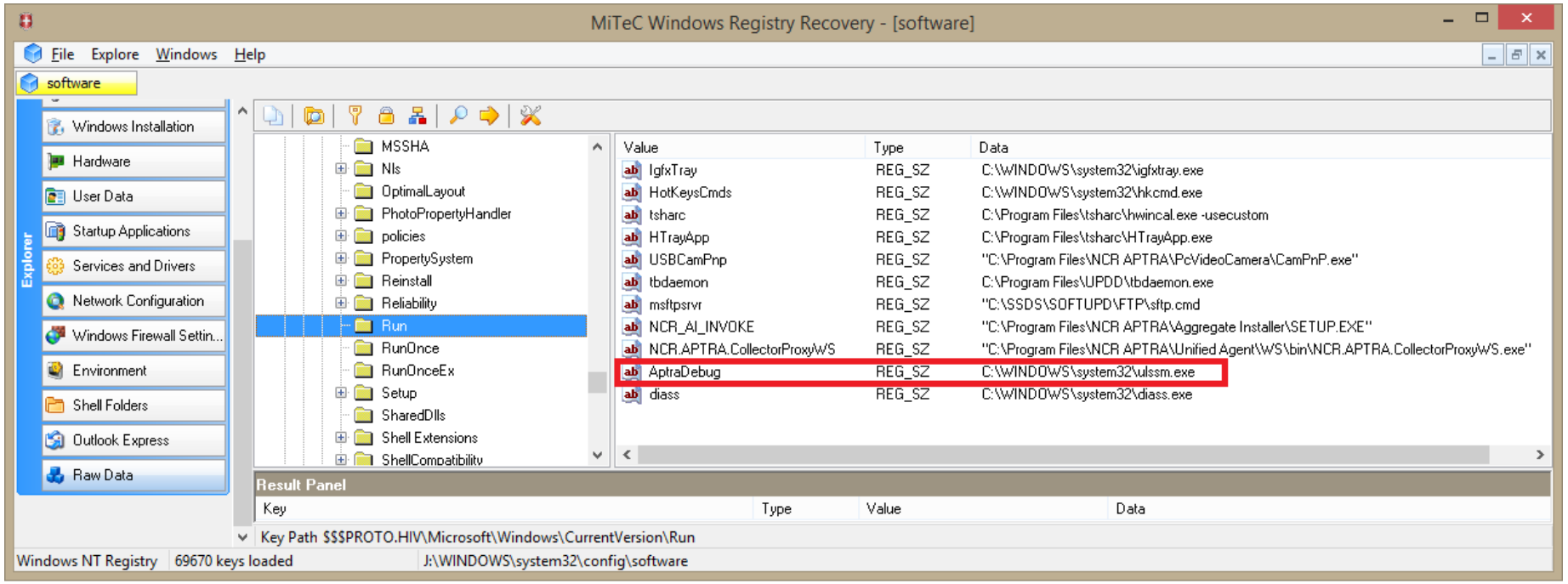


Система, в которой подготавливался ярлык

Filename	Linked path	Created	Written	Last Accessed	Size [B]	Vol Type	Vol Serial	Vol Name	NetBIOS	MAC Address
AptraDebug.lnk	C:\Windows\System32\ulssm.exe	16.03.2015 10:01:47	16.03.2014 19:26:05	16.03.2015 10:01:47	118784	Fixed	588D - 28EA		lucky	1C:6F:65:91:0D:CB
	C:\	n/a	n/a	n/a	0					
	?Windows	22.08.2013 13:36:16	15.03.2015	15.03.2015 23:55:30	0					
	?gSystem32	22.08.2013 13:36:18	16.03.2015	16.03.2015 23:55:30	0					
	?ulssm.exe	16.03.2015 10:01:48	16.03.2014 0:00:02	16.03.2015 23:55:30	118784					

2. Автозагрузка

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
AptraDebug = «<Путь к исполняемому файлу исследуемой программы>»



3. Использование XFS API для подключения к устройствам PINPAD и диспенсеру

4. Скрытие окна программы и ожидание ввода команд

CODE: <Числовой код>
ENTER SESSION KEY TO PROCEED!

DISABLING LOCAL AREA NETWORK...
PLEASE WAIT

CASH OPERATION PERMITTED.
TO START DISPENSE OPERATION -
ENTER CASSETTE NUMBER AND PRESS ENTER

CASH OPERATION FINISHED.
TAKE THE MONEY NOW!

CASH OPERATION PERMITTED
INVALID CASSETTE NUMBER. TRY AGAIN.
TO START DISPENSE OPERATION –
ENTER CASSETTE NUMBER AND PRESS ENTER.

ЦЕЛЕВЫЕ АТАКИ

Архив из вложения содержит файл с расширением «.doc.cpl» и значком файла «Microsoft Word»

Пароль на архив 11

Александр, Добрый день!

Высылаю Вам наши реквизиты для заключения договора, и документы на проверку

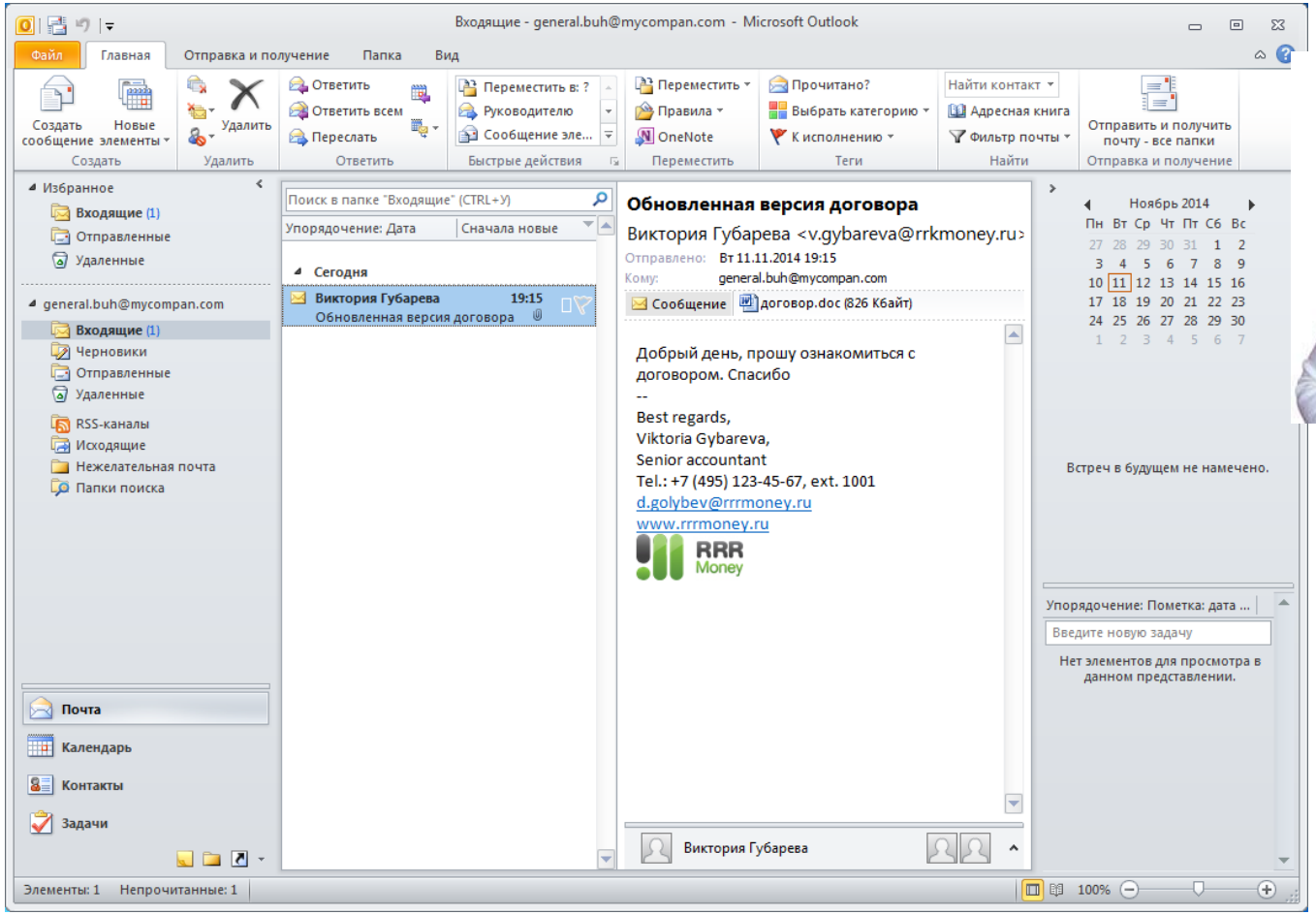
Сумма депозита 32 000 000 руб 00 коп, сроком на один год, % в конце срока

С Уважением, XX

тел. +XXXX

Email:xxx@xxx.ru

Письмо на почту



Anunak

CVE-2012-0158 + договор.doc = <3

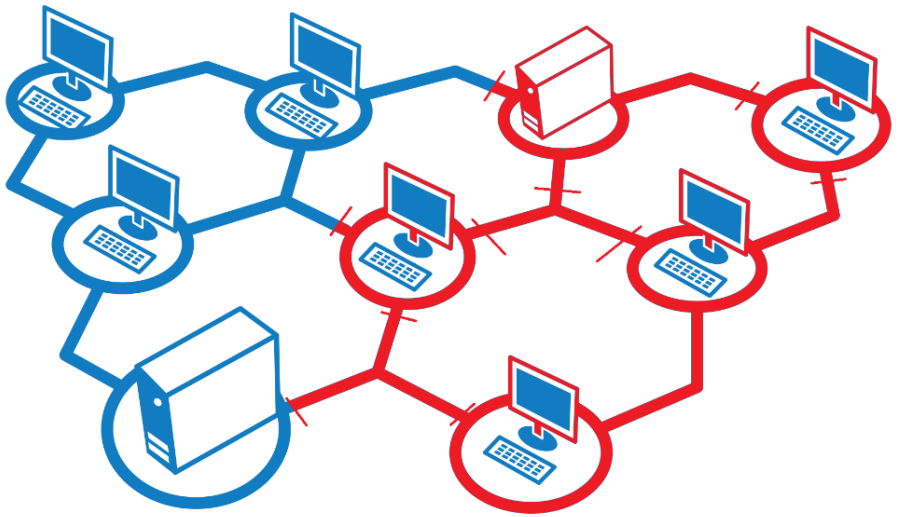
bc:31.131.17.125 + blizko.net/blizko.org

ntxobj.exe

%SYSTEM%/Com/svchost.exe

- netsh
- AmmyAdmin
- Mimikatz

%All Users%\Application Data\Mozilla\%name%.bin



Пароли

2014-11-11 17:53:32 – mimi.exe
2014-11-11 17:53:41 – /Intell/mimi/6.txt
2014-11-11 17:54:52 – /Intell/mimi/mimi32/mimikatz.log

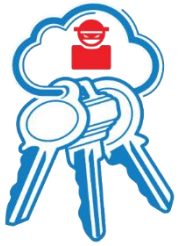
Result:
User Name : Buh
Domain : Buh-PC

Domain : INTAD *
Password : igf42er5

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```



Подмена кассет (Платформа Wincor)

1. Загрузка при удаленном или физическом доступе в банкомат. Модификация ключей реестра.

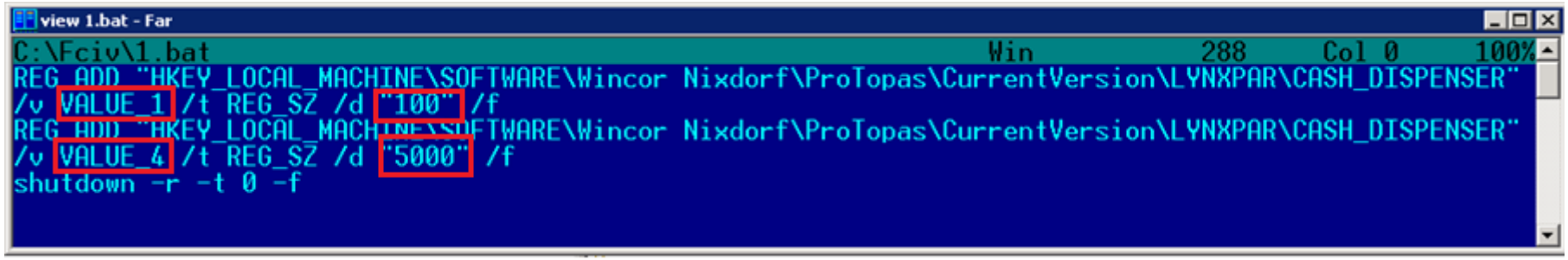
2. Выдача вместо купюр номиналом 100р купюр номиналом 5000р.

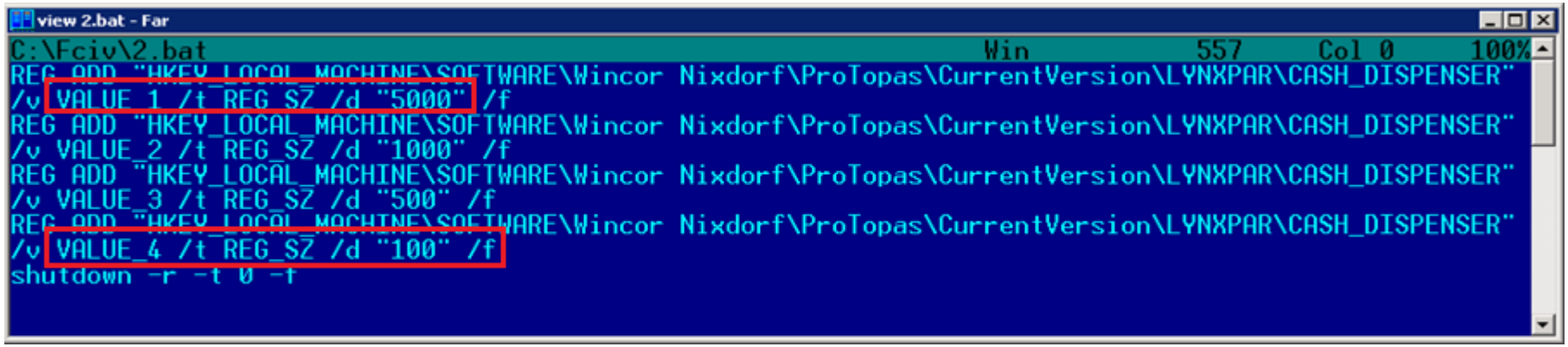
Выдать 500 рублей → Выдает 5x5000=25000 рублей

Подмена кассет (Платформа Wincor)

Модификация ключей реестра.

HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER\

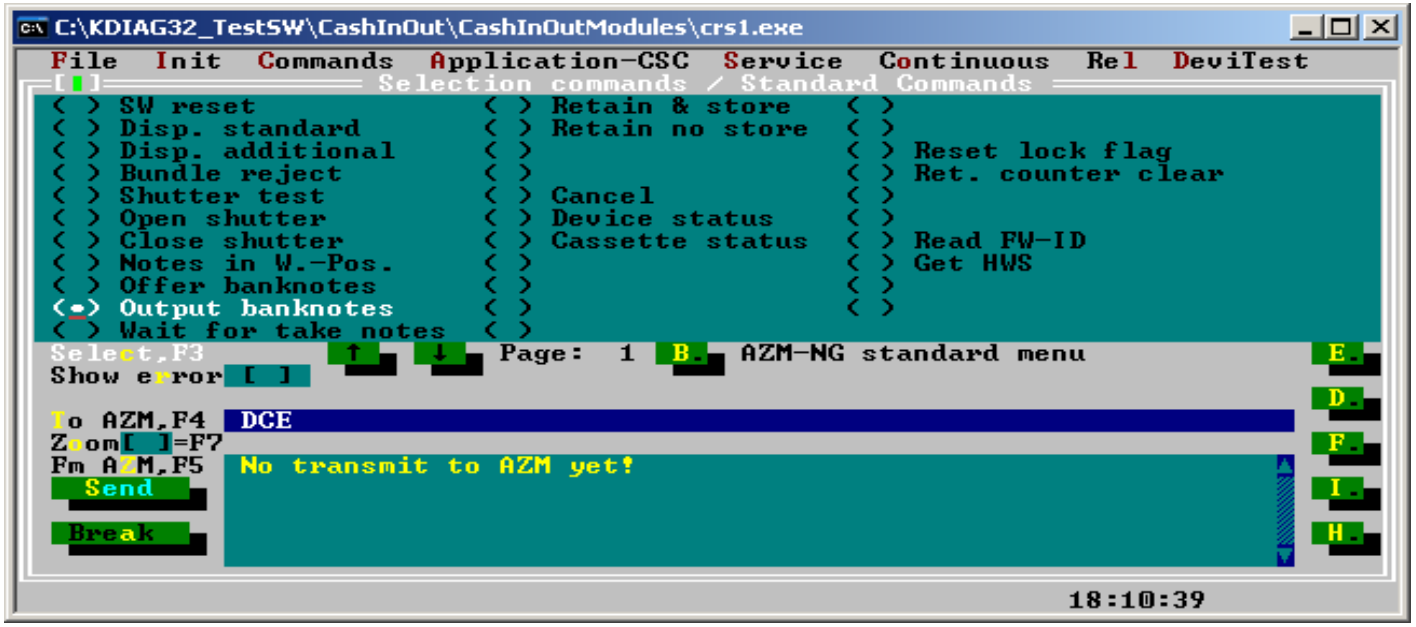




Вредоносная программа диспенсер (Платформа Wincor)

1. Загрузка при удаленном или физическом доступе в банкомат.

2. Запуск модифицированной версии диагностического ПО Test software Component Diagnostic ("KDIAG32")



3. Выдача купюр без проверки на открытие сейфа.

СОКРЫТИЕ В СИСТЕМЕ

Граббер (Платформа NCR)

1. Загрузка при доступе в банкомат. Модификация ПО банкомата (добавление функции в исполняемый файл в автозагрузке).

2. Запись тела вируса в библиотеку, в скрытый поток NTFS (ApplicationCore.exe:netncr.dll)

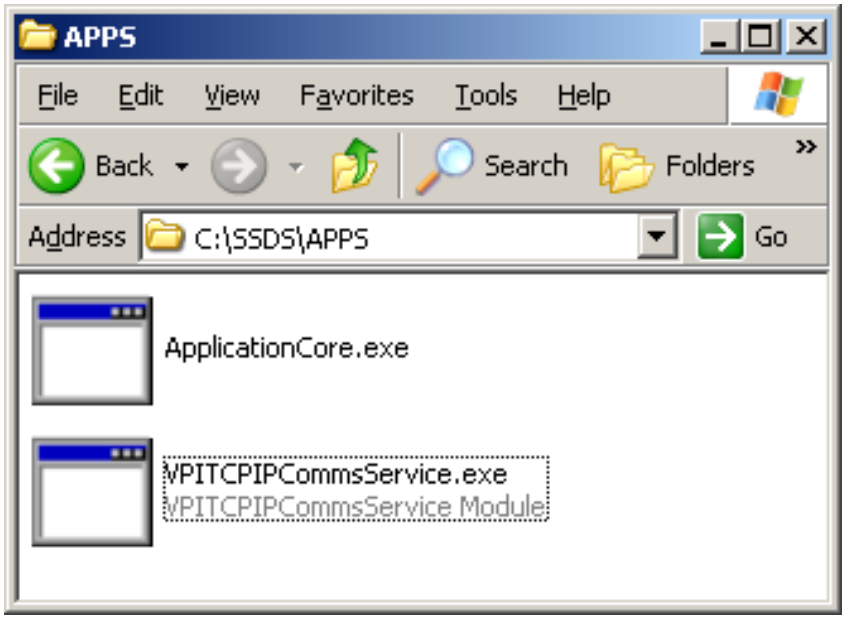
3. Перехват треков и пинов и запись их в зашифрованном виде в скрытый поток NTFS (autosave:descriptor).

4. Копирование данных на чип определенной карты, удаление вируса и следов работы после чтения определенной карты.

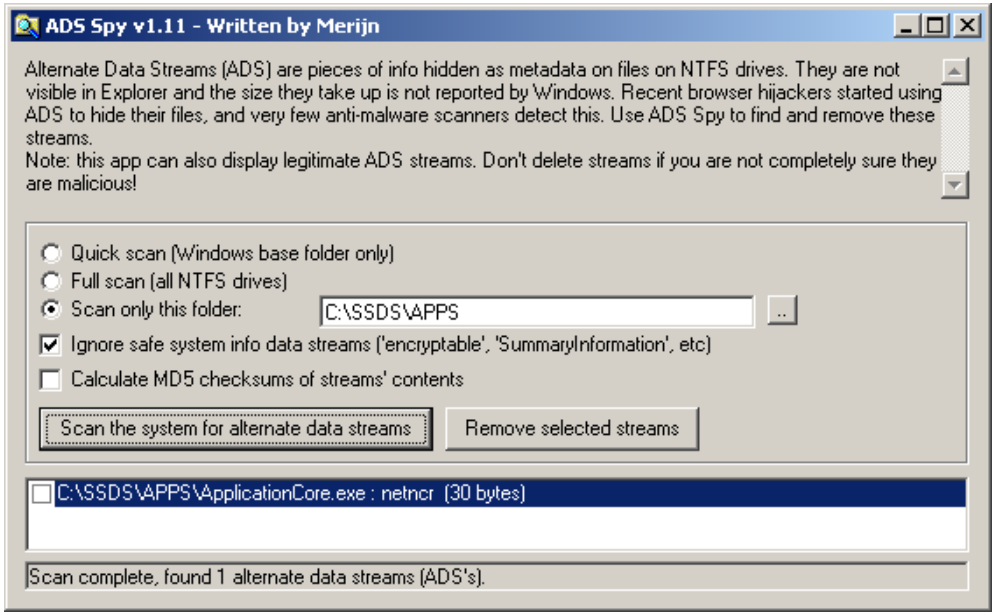
Автозагрузка
ApplicationCore.exe

```
.text:0040279C
.text:0040279C ; Attributes: bp-based frame
.text:0040279C
.text:0040279C                 public start
.text:0040279C start           proc near
.text:0040279C                 push    ebp
.text:0040279D                 mov     ebp, esp
.text:0040279F                 add     esp, 0
.text:004027A2                 pop     ebp
.text:004027A3                 push    offset loc_402038
.text:004027A8                 push    offset aCSsdsAppsAppli ; "C:\\SSDS\\APPS\\ApplicationCore.exe:netncr"...
.text:004027AD                 mov     eax, 7C801D7Bh
.text:004027B2                 call    eax
.text:004027B4                 retn
.text:004027B4 start           endp
.text:004027B4
.text:004027B4 ; ---------------------------------------------------------------------------
.text:004027B5                 align 4
.text:004027B8 aCSsdsAppsAppli db 'C:\SSDS\APPS\ApplicationCore.exe:netncr.dll',0
.text:004027B8                                         ; DATA XREF: start+C7o
.text:004027E4                 dd 7 dup(0)
.text:00402800                 dd 200h dup(?)
.text:00402800 _text           ends
```

Проводник – не отображается



ADSSpy – отображается



autosave:descriptor – данные с карты, в том числе второй трек

```
DateTime =  2013-06-11 16:29:37
track2 =
Balance =  0
PinBlock =  BD 29 B8 2A D5 22 D6 D1
PinLen =  8
Pin =  A5 75 6F 62 00 00


DateTime =  2013-06-11 16:40:13
track2 =
Balance =  0
PinBlock =  3A C4 96 79 06 13 35 A0
PinLen =  8
Pin =  45 70 FE B5 00 00


DateTime =  2013-06-11 16:41:07
track2 =
Balance =  0
PinBlock =  E2 44 7B 1B 14 D7 73 F1
PinLen =  8
Pin =  82 0F AF 3C 00 00
```

Вредоносная программа диспенсер (Платформа Diebold)

1. Загрузка при доступе в банкомат. Модификация ПО банкомата (добавление функции в исполняемый файл в автозагрузке).

2. Запись тела вируса в библиотеку, в скрытый поток NTFS (SpiService.exe:740DF3B835B.)

3. Активация от мастер-карты, удаление вируса и следов работы после чтения определенной карты.

4. Опустошение кассет диспенсера.

Автозагрузка
SpiService.exe

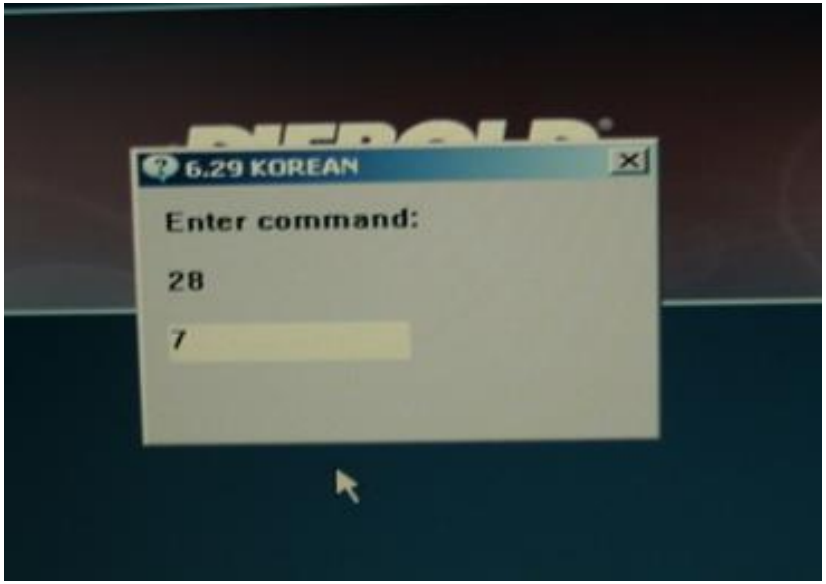
```
.text:00402751 ; Attributes: bp-based frame
.text:00402751
.text:00402751                 public start
.text:00402751 start           proc near
.text:00402751                 push    ebp
.text:00402752                 mov     ebp, esp
.text:00402754                 add     esp, 0
.text:00402757                 pop     ebp
.text:00402758                 push    offset loc_402056
.text:0040275D                 push    offset aCProgramFilesD ; "C:\\Program Files\\Diebold\\AgilisXFS\\bin\\"...
.text:00402762                 mov     eax, 7C801D7Bh
.text:00402767                 call    eax
.text:00402769                 retn
.text:00402769 start           endp
.text:00402769
.text:00402769 ; ---------------------------------------------------------------------------
.text:0040276A                 db 8Dh, 40h, 0
.text:0040276D aCProgramFilesD db 'C:\Program Files\Diebold\AgilisXFS\bin\SpiService.exe:740DF3B835B'
.text:0040276D                                         ; DATA XREF: start+C1o
.text:0040276D                 db '.exe',0
.text:004027B3                 align 4
.text:004027B4                 dd 13h dup(0)
.text:00402800                 dd 200h dup(?)
```

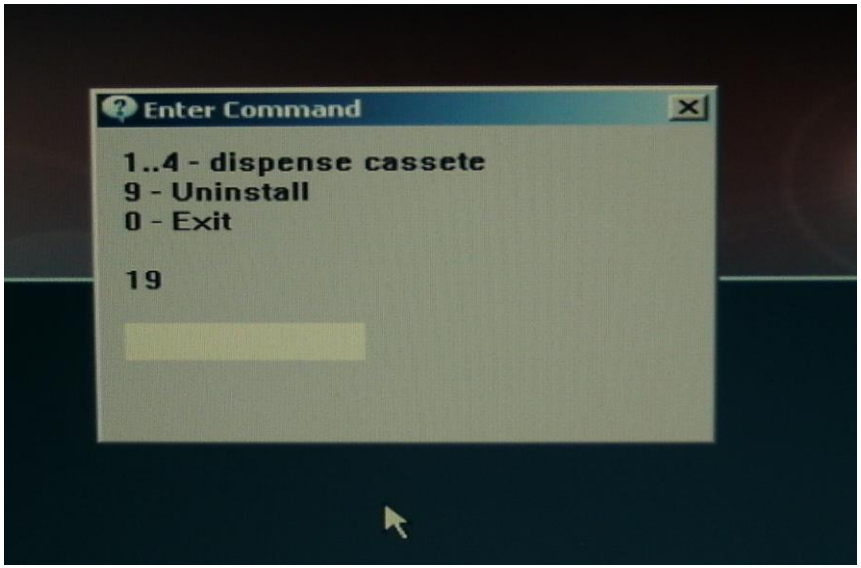
Подключение USB

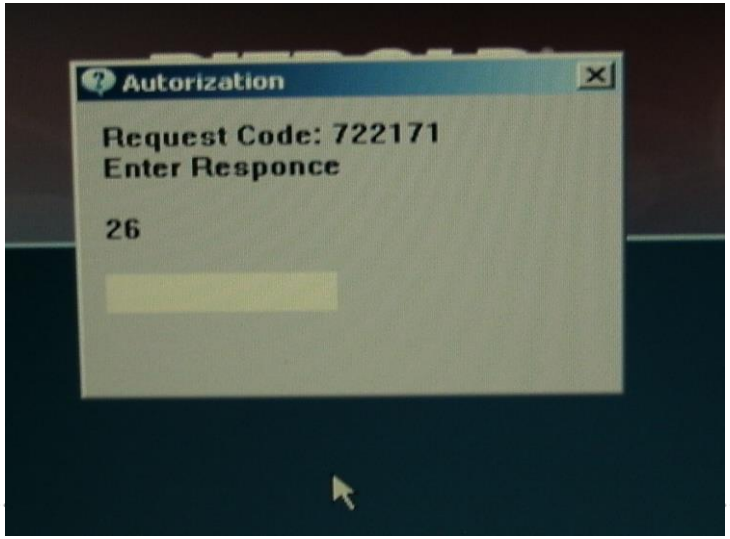
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\0033] DriverDate: [REG_SZ] 7-1-2001 DriverDateData: [REG_BINARY] DriverDesc: [REG_SZ] Generic volume DriverVersion: [REG_SZ] 5.1.2
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet001\Enum\STORAGE\RemovableMedia\7&22759ab6&0&RM] Capabilities: [REG_DWORD_LE] 96 Class: [REG_SZ] Volume ClassGUID: [REG_SZ] {71A27CDD-812A-11D0-BEC7-08002BE2092F} CompatibleID
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet002\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\0033] DriverDate: [REG_SZ] 7-1-2001 DriverDateData: [REG_BINARY] DriverDesc: [REG_SZ] Generic volume DriverVersion: [REG_SZ] 5.1.2
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&22759ab6&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#] SymbolicLink: [REG_SZ] \\?\S
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&22759ab6&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}] DeviceInstance: [REG_SZ] STOR
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet002\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&22759ab6&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\#] SymbolicLink: [REG_SZ] \\?\S
06.02.2015	22:18:41	M...	REG	SYSTEM key	Content Modification Time	[\ControlSet002\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}\##?#STORAGE#RemovableMedia#7&22759ab6&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}] DeviceInstance: [REG_SZ] STOR
06.02.2015	22:18:42	.A..	LOG	WinPrefetch	Last Time Executed	Prefetch [RUNDLL32.EXE] was executed - run count 5 path: \WINDOWS\SYSTEM32\RUNDLL32.EXE hash: 0x451FC2C0 volume: 1 [serial number: 0xFC8F532A device path: \DEVICE\HARDDISKVOLUME1]
06.02.2015	22:18:48	..C.	FILE	NTFS_DETECT	ctime	TSK:Content.IE5
06.02.2015	22:18:48	..C.	FILE	NTFS_DETECT	ctime	TSK:/Documents and Settings/Administrator/Cookies/index.dat
06.02.2015	22:18:48	..C.	FILE	NTFS_DETECT	ctime	TSK:History.IE5
06.02.2015	22:18:48	.A..	FILE	NTFS_DETECT	atime	TSK:/WINDOWS/system32/odbc32.dll
06.02.2015	22:19:01	M...	REG	NTUSER key	Content Modification Time	[\Software\Microsoft\Windows\ShellNoRoam\MUICache] @"C:\Program Files\Windows NT\Accessories\WORDPAD.EXE" -190: [REG_SZ] Rich Text Document @"C:\Program Files\Windows NT\Accessories\WORI
06.02.2015	22:19:01	M...	REG	NTUSER key	Content Modification Time	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH: [Count: 425]
06.02.2015	22:19:01	M...	REG	NTUSER key	Content Modification Time	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH:F:\E15C0740DF3B835B.exe: [Count: 1]
06.02.2015	22:19:01	M...	REG	NTUSER key	Content Modification Time	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] HRZR_EHACNGU: [REG_BINARY] HRZR_EHACNGU:(ahyy): [REG_BINARY] HRZR_EHACNGU:::
06.02.2015	22:19:01	.A..	LOG	WinPrefetch	Last Time Executed	Prefetch [E15C0740DF3B835B.EXE] was executed - run count 1 path: \E15C0740DF3B835B.EXE hash: 0x134C6192 volume: 1 [serial number: 0x7408DF34 device path: \DEVICE\HARDDISK1\DP(1)0-0+6] volume: 2 [se
06.02.2015	22:19:06	M...	EVT	WinEVT	Content Modification Time	[3221232506 / 0xc0001b7a] Record Number: 3384 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Computer Name: DIEBOLD-6EED880 Strings: [u'Diebold XFS' u'1']
06.02.2015	22:19:06	...B	EVT	WinEVT	Creation Time	[3221232506 / 0xc0001b7a] Record Number: 3384 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Computer Name: DIEBOLD-6EED880 Strings: [u'Diebold XFS' u'1']
06.02.2015	22:19:06	..C.	FILE	NTFS_DETECT	ctime	TSK:/Program Files/Diebold/AgilisXFS/bin/SpiService.exe
06.02.2015	22:19:11	...B	FILE	NTFS_DETECT	crtime;mtime;ctime;atime	TSK:/WINDOWS/Prefetch/E15C0740DF3B835B.EXE-134C6192.pf
06.02.2015	22:19:12	.A..	FILE	NTFS_DETECT	atime	TSK:/Program Files/Diebold/AgilisXFS/bin/SpiService.exe
06.02.2015	22:19:13	...B	EVT	WinEVT	Creation Time	[551 / 0x00000227] Record Number: 1175714 Event Type: Unknown 8 Event Category: 2 Source Name: Security Computer Name: DIEBOLD-6EED880 Strings: [u'Manage_ATM' u'DIEBOLD-6EED880' u'(0x0 0x459e6a)']

Запуск E15C0740DF3B835B.exe с подключенного USB

Команды


6.29 KOREAN
Enter command:
28
7


Enter Command
1..4 - dispense cassete
9 - Uninstall
0 - Exit
19


Autorization
Request Code: 722171
Enter Responce
26

ПРОБЛЕМЫ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

1. Необходимо оперативное снятие образа банкомата
2. Использование штатных утилит с модификациями
3. Использование скрытых потоков NTFS
4. Самоуничтожение программ, удаление журналов, видеофайлов.
5. Использование штатных средств удаленного управления
6. Подмена временных атрибутов файлов

ПРОБЛЕМЫ БЕЗОПАСНОСТИ БАНКОМАТОВ

1. Инсайд
2. Возможность сброса пароля на BIOS банкомата. Использование одинаковых паролей
3. Отсутствие возможности контролировать целостность ПО банкомата
4. Доступность сервисного ПО

Матвеева Веста

matveeva@group-ib.ru

+7 (495) 984-33-64 www.group-ib.ru info@group-ib.ru

facebook.com/group-ib twitter.com/group-ib