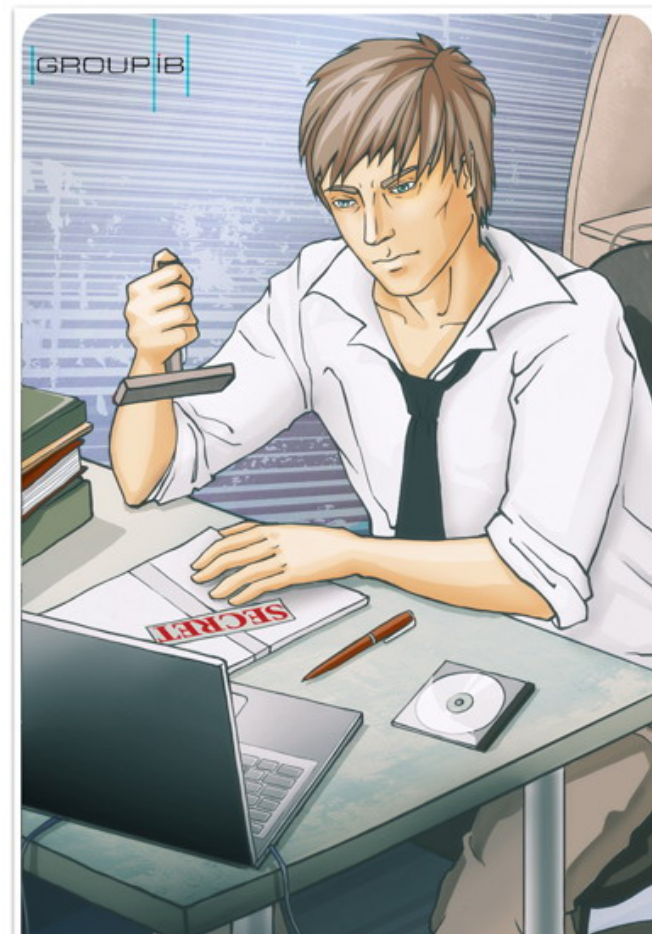


# Расследование инцидента. Пример из жизни.

Александр Писемский  
CISM, MCP  
Group-IB (Группа информационной безопасности)  
[pisemskiy@group-ib.ru](mailto:pisemskiy@group-ib.ru)



12:00 – Звонок на телефон оперативного дежурного Group-IB. Женский голос говорит, что у их компании украли деньги через Банк-клиент 10 дней назад. Обнаружили пропажу средств только через 2 дня. Написали заявление в местное отделение МВД. По делу никаких подвижений нет. Просит помочь.

12:30 – Группа по реагированию на инциденты Group-IB выезжает к пострадавшим.

13:30 – Интервью с руководителем компании-жертвы, персоналом и системным администратором. Получение информации об инциденте со слов всех так или иначе задействованных лиц. Получение информации об ИТ-инфраструктуре, процедурах работы с ДБО. Получение разрешения на проведение расследования

14:30 – Расследование началось

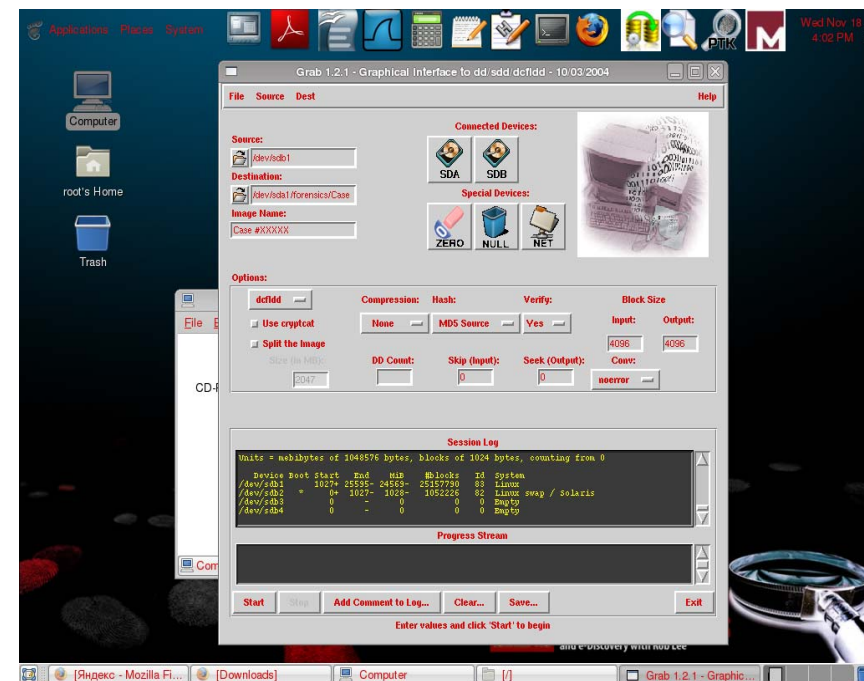
- Проведение сбора необходимых улик, их анализ, передача полученных данных в МВД



# Снимаем образ с ПК

Главная задача – сохранение доказательств **НЕИЗМЕННЫМИ**

- Изымаем жесткий диск из ПК и устанавливаем его в RECK
- Подключаем его в режиме «только чтение»
- Снимаем образ с помощью одной из многих утилит, в основе которых лежит dd или dcfldd



## Physical Evidentiary Item (Source) Information:

[Drive Geometry]

Bytes per Sector: 512

Sector Count: 234 484 672

Source data size: 114494 MB

Sector count: 234484672

[Computed Hashes]

MD5 checksum: 2afce733866231928c09a98a307d38e2

SHA1 checksum: c713a1b8e777f24b404f8ca7bee9ecc3004c64bd

## Image Information:

Acquisition started: Wed Nov 18 15:39:28 2009

Acquisition finished: Wed Nov 18 17:32:11 2009

Segment list:

## Image Verification Results:

Verification started: Wed Nov 18 17:32:11 2009

Verification finished: Wed Nov 18 17:56:01 2009

MD5 checksum: 2afce733866231928c09a98a307d38e2 : **verified**

SHA1 checksum: c713a1b8e777f24b404f8ca7bee9ecc3004c64bd : **verified**

# Снимаем логи с серверов и сетевого оборудования

---

- Прокси\Шлюзы\Программные фаерволы
  - Логи авторизации с контроллера домена
  - Логи с консоли управления антивирусными средствами
  - Таблицы маршрутизации
  - Syslog с железных МЭ и Unix-серверов
  - И т.д.
-

# Отправляем запросы на предоставление информации

- Провайдеру «жертвы»
- В банк с просьбой предоставления информации по доступу к счету «жертвы»
- В банк-получатель с просьбой предоставления информации по получающей стороне

## Анализ логов ISA-сервера с шлюза жертвы

- В ходе анализа обнаруживаем, что ПК, на котором проводились платежи заражен вредоносным ПО, которое ежедневно производит подключения к китайским и латвийским IP-адресам, где пытается скачать обновления и отправляет информацию о своем статусе.
- Определяем день заражения, ресурс с которого оно произошло и приложение, через которое вирус проник на ПК.
- Также видим, что ежедневно одновременно с включением ПК запускается приложение DynGate, которое производит подключения к серверам TeamViewer.

# Записи в логах

ISA1	08.11.2009	7:19:49	TCP	192.168.0.210:2120	X.X.X.X:80	svchost.exe:3:5.1
ISA1	08.11.2009	7:19:49	TCP	192.168.0.210:2121	X.X.X.X:80	svchost.exe:3:5.1
ISA1	08.11.2009	7:19:49	TCP	192.168.0.210:2121	X.X.X.X:80	svchost.exe:3:5.1
ISA1	08.11.2009	7:20:13	TCP	192.168.0.210:2125	X.X.X.Y:80	4E.tmp:3:5.1
ISA1	08.11.2009	7:20:13	TCP	192.168.0.210:2126	X.X.X.Y:80	4E.tmp:3:5.1
ISA1	08.11.2009	7:20:13	TCP	192.168.0.210:2127	X.X.X.Y:80	4E.tmp:3:5.1
ISA1	08.11.2009	7:20:14	TCP	192.168.0.210:2127	X.X.X.Y:80	4E.tmp:3:5.1
ISA1	08.11.2009	7:20:14	TCP	192.168.0.210:2128	X.X.X.X:80	4E.tmp:3:5.1

192.168.0.210	Opera	08.11.2009	7:37:04	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/javaw.exe	Allowed
192.168.0.210	Opera	08.11.2009	7:37:11	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/bss.exe	Allowed
192.168.0.210	Opera	08.11.2009	7:37:27	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/fak.exe	Allowed
192.168.0.210	Opera	08.11.2009	7:38:38	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/socks5.exe	Allowed
192.168.0.210	Microsoft Internet Explorer	08.11.2009	7:40:07	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/socks5.exe	Allowed
192.168.0.210	Microsoft Internet Explorer	08.11.2009	7:40:20	ISA1	213.182.197.234	80	GET	http://X.X.X.X/update/tv.exe	Allowed
192.168.0.210	Mozilla/4.0 (compatible; MSIE 6.0; DynGate)	08.11.2009	7:40:30	ISA1	87.230.73.30	80	GET	http://Y.Y.Y.Y/din.aspx?s=00000000&id=0&client=DynGate&rnd=134761120&p=10000001	Allowed

## ■ Криминалистический анализ образа

The screenshot shows the Autopsy Forensic Browser interface in Mozilla Firefox. The browser address bar displays `http://localhost:9999/autopsy`. A warning message states: "WARNING: Your browser currently has Java Script enabled. You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons." The main content area features the Autopsy logo (a dog with a hat) and the URL `http://www.sleuthkit.org/autopsy/`. At the bottom, there are buttons for "OPEN CASE", "NEW CASE", and "HELP".

The screenshot shows the Carver application interface. The "Source Image" field contains `C:\Case\Drive.imz`. Below it, a message says "Image Not Found" with a "Configure Carve List" button. The "Output Folder ( no spaces)" field contains `C:\Case\o1`. At the bottom, there is a "Start Scalpel" button and a label "# of files Carved:". The footer text reads "Interface (c) Xabersoft 2008 v 3.0 Demo Version".

The screenshot shows the AccessData FTK Imager interface. The "Evidence Tree" on the left shows a directory structure for `system32`. The "File List" on the right shows a list of files and directories. The "Properties" window at the bottom shows details for the selected file:

General	
Name	system32
File Class	Directory
File Size	512
Physical Size	512
Date Accessed	31.07.2009 21:40:46
Date Created	29.10.2003 10:26:56
Date Modified	29.07.2009 10:50:32
Encrypted	<input type="checkbox"/>
Compressed	<input type="checkbox"/>

The "Properties" window also shows "DOS Attributes" and "Properties" tabs. The footer text reads "Buhgalter.001\NONAME [NTFS][root]\WINDOWS\system32".

The screenshot shows the Registry Ripper application interface. The "Hive File:" field is empty. The "Report File:" field is empty. The "Plugin File:" dropdown menu is empty. The "Rip It" and "Close" buttons are visible at the bottom. The "Plugins List Populated" section shows a list of plugins:

Name	Size	Type	Date
1033	1 KB	Directory	29.07.2009 10:...
1049	1 KB	Directory	29.07.2009 10:...
Aktiv Co	1 KB	Directory	29.07.2009 10:...
appmgmt	1 KB	Directory	29.07.2009 10:...
bits	1 KB	Directory	29.07.2009 10:...
inf	1 KB	Directory	29.07.2009 10:...
msagent	1 KB	Directory	29.07.2009 10:...
PCHealth	1 KB	Directory	29.07.2009 10:...
peernet	1 KB	Directory	29.07.2009 10:...
Resources	1 KB	Directory	29.07.2009 10:...
SoftwareDistribution	1 KB	Directory	29.07.2009 10:...
schemas	1 KB	Directory	29.07.2009 10:...
system	1 KB	Directory	29.07.2009 10:...
system32	1 KB	Directory	29.07.2009 10:...
DRVSTORE	1 KB	Directory	29.07.2009 10:...
dt	1 KB	Directory	29.07.2009 10:...

## ■ Восстанавливаем хронологию

Date	Size	Type	Mode	UID	GID	Meta	File Name
Wed Jul 29 2009 05:08:05	127488.a..	r/rrwxrwxrwx		0	04664-128-3		C:/WINDOWS/system32/mshearts.exe (deleted)
Wed Jul 29 2009 05:08:05	1175635.a..	-/rrwxrwxrwx		0	05002-128-3		C:/Program Files/MSN Gaming Zone/Windows/Hrtzres.dll (deleted)
Wed Jul 29 2009 05:08:05	2178131.a..	-/rrwxrwxrwx		0	05005-128-3		C:/Program Files/MSN Gaming Zone/Windows/Shvlres.dll (deleted)
Wed Jul 29 2009 05:08:05	780885.a..	-/rrwxrwxrwx		0	05008-128-3		C:/Program Files/MSN Gaming Zone/Windows/chkrres.dll (deleted)
Wed Jul 29 2009 05:08:05	753236.a..	-/rrwxrwxrwx		0	05011-128-3		C:/Program Files/MSN Gaming Zone/Windows/Rvseres.dll (deleted)
Wed Jul 29 2009 05:08:05	1817687.a..	-/rrwxrwxrwx		0	05014-128-3		C:/Program Files/MSN Gaming Zone/Windows/bckgres.dll (deleted)
Wed Jul 29 2009 05:08:05	327743.a..	-/rrwxrwxrwx		0	05239-128-3		C:/Program Files/Movie Maker/wmmres.dll (deleted)
Wed Jul 29 2009 05:08:05	347136.a..	r/rrwxrwxrwx		0	089653-128-3		C:/WINDOWS/system32/tourstart.exe
Wed Jul 29 2009 05:08:05	538624.a..	r/rrwxrwxrwx		0	089777-128-3		C:/WINDOWS/system32/spider.exe
Wed Jul 29 2009 05:08:06	137216.a..	r/rrwxrwxrwx		0	089701-128-3		C:/WINDOWS/system32/sti_ci.dll
Wed Jul 29 2009 05:08:06	388608.a..	-/rrwxrwxrwx		0	090924-128-3		C:/WINDOWS/system32/Restore/rstrui.exe (deleted)
Wed Jul 29 2009 05:08:09	244224.a..	r/rrwxrwxrwx		0	090614-128-3		C:/WINDOWS/system32/usmt/migwiz.exe
Wed Jul 29 2009 05:08:30	252928.a..	-/rrwxrwxrwx		0	090508-128-3		C:/WINDOWS/system32/compatui.dll (deleted)
Wed Jul 29 2009 05:08:42	331264.a..	-/rrwxrwxrwx		0	090346-128-3		C:/WINDOWS/system32/hnetwiz.dll (deleted)
Wed Jul 29 2009 05:08:43	29184.a..	-/rrwxrwxrwx		0	0125989-128-3		C:/WINDOWS/system32/oobe/msoobe.exe (deleted)
Wed Jul 29 2009 05:09:03	886m...	r/rrwxrwxrwx		0	0220-128-4		C:/WINDOWS/win.ini

Извлекаем с HDD необходимые для дальнейшего анализа файлы

С помощью криминалистического браузера образов извлекаем интересующие нас файлы:

- Журналы Windows
- Hives Реестра
- Обнаруженное вредоносное ПО
- Историю работы в Интернете
- Логи другого ПО
- Удаленные файлы, имеющие отношение к инциденту

# Что получили в ходе анализа?

## ■ Теперь мы знаем кто украд ключи и как!

\*К слову, ключи были обнаружены на рабочем столе вместе с файлом-памяткой для работы со всеми ДБО, использующимися в компании, включая пароли.

### Лог TeamViewer:

```
10/29 14:24:58.315 00252 T Connection incoming, threadid = 13 (..\Server\Server.cpp, 255)
10/29 14:24:58.361 02696 T CLogin::run() (.Login.cpp, 135)
10/29 14:24:58.361 02696 T CLogin::NegotiateVersionServer() (.Login.cpp, 364)
10/29 14:24:58.361 02328 D S10 0.0.0.0 - CT13 CT.Run
10/29 14:24:58.377 02328 D CT13 TM.TM_TVout
10/29 14:24:58.377 02224 D S9 88.198.141.34 - CT12 CT.Run
10/29 14:24:58.377 02224 D ! S9 88.198.141.34 - CT12 CT.Send.CMD_IDENTIFY
From=*VICTIM_TV_ID* To=0 L=32
10/29 14:24:58.424 02224 D CT12 TM.TM_GWout
10/29 14:24:58.486 02224 D S9 88.198.141.34 - CT12 CT.Receive.CMD_SESSIONMODE
From=*BAD_GUY_TV_ID* To=*VICTIM_TV_ID* L=20
10/29 14:24:58.549 02224 D S9 88.198.141.34 - CT12 CT.Receive.CMD_IDENTIFY From=0
To=341495665 L=32
10/29 14:24:58.596 02224 D Received encrypted and signed AES 256Bit session key
.....
10/29 14:25:06.299 01136 T ConnectionAccessSettings: RemoteControl: Denied FileTransfer:
Allowed ControlRemoteTV: Denied SwitchSides: Denied AllowDisableRemoteInput: Denied AllowVPN:
Denied AllowPartnerViewDekstop: Denied (..\Server\ServerThread.cpp, 2229)
07/29 14:25:06.502 03948 F The Serverthread started.
```

## Ответы на запросы

- От Банка жертвы получена информация по подключениям злоумышленников к серверу ДБО, все адреса принадлежат сети *Yota*.
- На банк после отправки платежки совершалась *DDoS-атака*.
- Деньги были переведены на счет физического лица, а затем обналичены в банкоматах в г. Екатеринбурге
- *TeamViewer* предоставил внешний IP-адрес, зарегистрированный за ПК с уникальным идентификатором TeamViewer  
\*BAD\_GUY\_TV\_ID\* - след ведет в одну из домашних сетей Москвы

Проведя анализ вредоносного ПО мы получили

- 1) Сигнатуру для включение в базу вредоносного ПО;
- 2) IP-адреса управляющих центров;
- 3) Поняли принципы функционирования и распространения.

- Оформив соответствующим образом отчет по криминалистической экспертизе ПК, анализу логов и вредоносного ПО, мы передаем данную информацию вместе с заявлением в правоохранительные органы для проведения дальнейшего расследования.

# Почему расследованием должна заниматься третья сторона?

Вывод Вы сможете сделать сами, ответив на следующие вопросы:

- Доверяете ли Вы своей Службе Безопасности?
- Уверены ли Вы, что инцидент произошел не по их прямой или косвенной вине, что помешает СБ быть объективными при расследовании?
- Достаточно ли мотивирована СБ, чтобы найти виновного в инциденте?
- Имеют ли специалисты СБ необходимую компетенцию и опыт в проведении расследований, криминалистической экспертизы, анализа программного обеспечения? Сколько будет стоить их обучение и дополнительное оборудование? На сколько возможен их отрыв от основной работы?
- Имеют ли Ваши специалисты возможность взаимодействия с правоохранительными органами и международными CERT для проведения расследований, выходящих за рамки Вашей компании?

# Проблемы, с которыми мы сталкиваемся ежедневно при расследовании

- Практически полное отсутствие заинтересованности со стороны провайдеров в снижении уровня преступности у них в сети
- Нет единых стандартов по осуществлению протоколирования в информационных системах
- Менталитет и недоверие к правоохранительным органам
- Нет единой судебной практики и слабость законодательной базы
- Неприменимость многих западных методик к Российской действительности
- Дефицит специалистов по расследованию ИТ-преступлений
- ИТ - преступность глобальна
- Отсутствие единой схемы обмена информации об инцидентах как между коммерческими организациями, так и правоохранительными органами

Мы призываем к сотрудничеству все организации, которые так или иначе используют ИТ в своей работе. Уже сегодня уровень преступности в Рунете сопоставим с уровнем Китая и Африки. Если не предпринять коллективных мер сейчас, то потом будет поздно. С каждым последующим преступлением дерзость и размах злоумышленников только возрастают.

Только совместные усилия и ответственность всех участников: организаций, государства и физических лиц, способны стабилизировать и улучшить ситуацию.

Спасибо за внимание

GROUP IB



Александр Писемский  
CISM, MCP  
Группа информационной безопасности

[pisemskiy@group-ib.ru](mailto:pisemskiy@group-ib.ru)  
[www.group-ib.ru](http://www.group-ib.ru)

