

ИСТОРИЯ О СОХРАНЕННЫХ
ДЕНЬГАХ, РЕПУТАЦИИ И
ОДНОМ ИНТЕРЕСНОМ
ПРОДУКТЕ



В жизни всегда
есть место открытию
open.ru



В НАЧАЛЕ ПУТИ ИЛИ ВТОРАЯ ЖИЗНЬ ТРОЯНЦА «CARBERP»

- ❑ «Двое организаторов хакерской группы Carberp, укравшей деньги со счетов более 1000 российских граждан компаний, приговорены к пяти и восьми годам лишения свободы. В общей сложности злоумышленники с помощью вредоноса похитили денежных средств на сумму **\$250 млн.**», источник «Ведомости»
- ❑ «Хакеры использовали известнейший банковский троян Carberp, на который приходится **72% заражений финансово-кредитных учреждений в мире**», исполнительный директор InfoWatch Всеволод Иванов



- ❑ «Вредоносные программы, разработанные этой хакерской группой, были сделаны так, что **антивирусы не замечали заражения**, а вирусы имели очень богатый функционал, в том числе умели перехватывать передаваемую банком информацию об изменении баланса, что позволяло похищать деньги незаметно», технический директор компании Cezurity Андрей Воронов

- ❑ «Исходники известного банковского трояна Carberp утекли в открытый доступ. Исходные коды Carberp в RAR-архиве размером **1,88 ГБ** сейчас легко находятся Google'ом. В распакованном виде проект содержит около **5 ГБ** файлов с подробным листингом. Очевидно, теперь можно ожидать новой волны креатива со стороны начинающих, так и продолжающих вирусописателей. Кто-то даже пошутил: **“Утечка Zeus была как бесплатный автомат. Утечка Carberp — это уже бесплатный ракет-ланчер”**... », эксперт по ИБ, автор журнала «Хакер», Денис Мирков

ЗНАКОМЬТЕСЬ – «CARBERP» 2.0 ... !

- ❑ **Логирует** нажатия пользователем клавиш и виртуозно вклинивается в HTTP-трафик
- ❑ **«Вытягивает»** всю имеющуюся аутентификационную информацию из хэша ОС и пр. (в т.ч. сертификаты и ключи)
- ❑ Отлично **маскируется** в системе (после успешного запуска, троянец внедряется в другие работающие приложения, а свой основной процесс завершает)
- ❑ Имеет возможности удаленного управления и использования плагинов, *что позволяет организовывать атаки на конкретную компанию по заказу извне. На данный момент имеются версии плагинов под **ВСЕ** известные банковские системы*

Семейство Carberp крайне сложно обнаруживается антивирусным ПО

Будучи установленным на машину, зловред удаляет антивирусное ПО, подтягивает необходимые детектируемые модули и всячески затрудняет повторную установку антивируса. При этом на других машинах сети злоумышленник использует вполне легитимные средства управления (удаленное администрирование), доступ к которым был получен через зловреда.

БЛИЖЕ К ДЕЛУ... ИЛИ ОДНА ЖИЗНЕННАЯ ИСТОРИЯ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: «ДОЛГОЖДАННАЯ» КОРРЕСПОНДЕНЦИЯ



- ✓ Реальный клиент по договоренности с представителем Компании
- ✓ Письмо с файлом «Реквизиты»
- ✓ Запуск исполняемого файла (уникальный эксплойт)
- ✓ Заражение машины и получение полного контроля над ней

ПОЛУЧЕНИЕ ПРИВИЛЕГИЙ В СИСТЕМЕ



- ✓ Удаление антивируса на инфицированной машине, противодействие повторной установке
- ✓ Дозагрузка необходимых модулей и компонент (легальные средства удаленного администрирования, др. «полезные» утилиты)
- ✓ Мониторинг и анализ системы (кейлоггер, пароли из хэша ОС)
- ✓ Применение подтянутых эксплойтов и повышение привилегий в системе
- ✓ Получение привилегированного доступа к другим машинам сети (пользовательские, контроллеры доменов, ключевые станции)

ПОЛУЧЕНИЕ ПРИВИЛЕГИЙ В СИСТЕМЕ



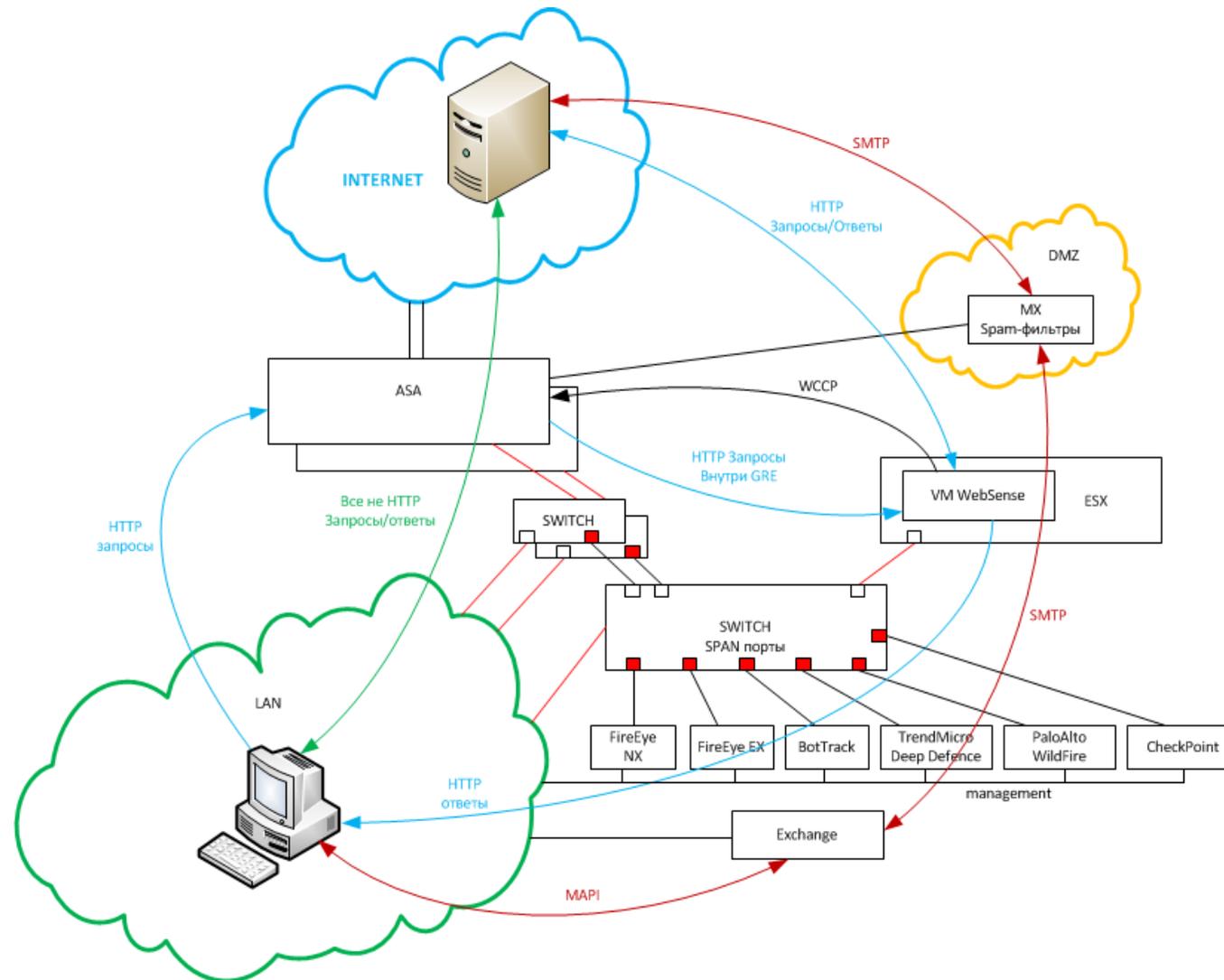
- ✓ Перехват конфиденциальной информации
- ✓ Доступ к СДБО
- ✓ Доступ к Процессингу
- ✓ Доступ к Управляющим рабочим станциям (банкоматы и пр.)

РЕГИСТРАЦИЯ И УСТРАНЕНИЕ ИНЦИДЕНТА

ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА

- ✓ Подозрительная сетевая активность с хоста из внутренней сети
- ✓ Проблемы с установкой антивирусного ПО на машинах
- ✓ Подозрительные колбэки, детектируемые на IPS/МЭ (websense)
- ✓ **«Занимательная информация» с тестового стенда**

ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: РАЗВЕРНУТЫЙ ТЕСТОВЫЙ СТЕНД



ЗАХВАЧЕННЫЕ ХОСТЫ

The screenshot displays the FireEye Alerts dashboard. The main alert is a 'Malware Callback' with ID 27984, detected at 20:55:06. The malware is identified as 'InfoStealer.Banker.Zbot'. The alert details include a communication capture showing a GET request from source host 10.48.10.10 to target host 146.185.220.200. The request is for a public resource on the target host. The user-agent is Mozilla/4.0 (compatible; MSE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; NET4.0C; NET4.0E).

Type	ID	ET	Malware	Severity	Time (MSK)	Source IP	Target IP	URL/URI	Location
Malware Callback	27984		InfoStealer.Banker.Zbot	■■■■■■■■	20:55:06	10.48.10.10	146.185.220.200	http://public-dns/QWxTrFw/YkTtheNFLg	BR/So Paulo

Callback: InfoStealer.Banker.Zbot

Interface: network A1 (mode tap)

Blocking Action: NOT blocked

Communication Capture: pcap 978 bytes (text)
 IP Protocol: TCP
 Source Host: 10.48.10.10
 Src IP: 10.48.10.10
 Src MAC Address: 0026...
 Dest MAC Address: c84...

Callback communication from infected host:
 Server DNS Name: 146.185.220.200 Service Port: 80 Location: BR/So Paulo Signature Name: InfoStealer.Banker.Zbot

Direction	Command	User-Agent	Host	Connection	Pragma
GET	/QWxTrFw/YkTtheNFLg/IDGJ/7YkX-dVWSP-8/tR0oVSudXdkq7YRSNgv.cg79Gz=Y&gWX=g&WY/bx=B68861uALiYOrMNHxtr8P'b=WSeUp.tu HTTP/1.1	Mozilla/4.0 (compatible; MSE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; NET CLR 2.0.50727; NET CLR 3.5.30729; NET CLR 3.0.30729; NET4.0C; NET4.0E)	public-dns		

Others: Accept: */*

ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: ОБНАРУЖЕНИЕ ИНФИЦИРОВАННЫХ ПИСЕМ С ПОМОЩЬЮ FIREEYE EX 5400

The screenshot displays the FireEye eAlerts dashboard. At the top, there are navigation tabs for Dashboard, eAlerts, eQuarantine, Settings, Reports, and About. The main heading is "Email Alerts" with a sub-note "(as of [redacted] 13:01:54 MSK)".

Below the heading, there are filters for "Page: 1 of 1", "Results per page: 20", "Duration From: Now", and "Going Back: 3 months". The total number of alerts is 2.

The main content area shows a summary table and two detailed email alert views.

Recipient	Total Malicious Email	Malicious Header	Attachment (Total)	URL (Total)	Last Malware	Last seen at (MSK)
doz or07@mail-mirror.local	2	0	2 (2)	0 (0)	Malware.archive	[redacted] 17:26:09
[redacted]openru, [redacted]openru	1	0	1 (1)	0 (0)	Malware.archive	[redacted] 17:26:09

Sender	Received	Subject	Malicious Header	Attachment (Total)	URL (Total)	Last Malware	Action
[redacted]@gmail.com	Mon, [redacted] 14 17:22:50 +0400	CPL [redacted] 14 #1001	0	1 (1)	0 (0)	Malware.archive	View_email
[redacted]@gmail.com	Mon, [redacted] 14 17:22:50 +0400	CPL [redacted] 14 #1001	0	1 (1)	0 (0)	Malware.archive	View_email

Sender	Received	Subject	Malicious Header	Attachment (Total)	URL (Total)	Last Malware	Action
[redacted]@mail.com	Mon, [redacted] 14 17:22:50 +0400	CPL [redacted] 14 #1001	0	1 (1)	0 (0)	Malware.archive	View_email

ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: FIREEYE NX 7400

Appliance Type: CMS 7400 | IP: 10.88.88.47 | ID: 0025908790BC
 Hostname: CM7400 | Logged in as: monitor | Role: monitor | [Log out](#)

Dashboard | Appliances | Alerts | Summaries | eAlerts | Analysis | Filters | Settings | Reports

Malware Object	783530	rar	Malware.archive	NX7400	14 16:47:55	62.213.110.14	10.51	a2c8380d2f996ed123fe6b53187dd398
Malware Object	783531	exe	Malware.Binary	NX7400	14 16:47:55	62.213.110.14	10.51	4183599ecf65960ddcf4195c81f4b3b3

Malware: ■ Malware.Binary
 Application Type: Windows Explorer
 File Type: exe

VM Capture
 Src IP: 62.213.110.14
 Analysis OS: [Microsoft WindowsXP 32-bit 5.1 sp3 13.1125](#)

■ Malicious Behavior Observed

Bot Communication Details:
 Server DNS Name: 46.183.149.181 Signature Name: Malware.Binary

Raw Command

```
POST /gopotadetected/beypoeblu/o4ko.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/4.0
Host: 46.183.149.181
Content-Length: 74
Cache-Control: no-cache
Pragma: no-cache

eal++y4ZzHOR/wUpUCbUk9WHf8ISG5T/3XcmR3cty94+DVtA+yAu6OUb1txAqRlg
VT/kxw==
```

Server DNS Name: update.microsoft.com Service Port: 80 Signature Name: Malware.Binary

OS Change Detail (version: 4.1963) | Items: 94 | OS Info: Microsoft WindowsXP 32-bit 5.1 sp3 13.1125 [Top](#)

Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)	Process ID	Parent ID	File Size
Analysis	Malware				
Os		Name: windows Version: 5.1.2600 Service Pack: 3			
Os Monitor		Version: 6.3.3 Build: 151945 Date: Nov 16 2013 Time: 11:29:23			
Uac	Audit policy change				
Regkey	Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BITS\Start" = 0x00000002	552		
Malicious Alert	Misc Anomaly	Message: Process initializing auto-load for driver Detail: Process initializing auto-load for drive r in existing service			

УСТРАНЕНИЕ ПОСЛЕДСТВИЙ ИНЦИДЕНТА

Page: 1 of 1

ID	Device	Type	File Type	Malware	Name	Md5sum	Submitted	
354431	sec-feex00	Attachment	doc	Malware.Binary.Doc	ОБЕД на 26.11.14.doc	df17336b558417b51aabc7a0419dd2ae Get malware binary	11/26/14 09:56:09	
Malware:		Malware.Binary.Doc		VM Capture:(s)		[1] _Get pcap file		
Application Type:		MS Word 2003				[2] _Get pcap file		
File Type:		doc				[3] _Get pcap file		
Original analyzed at:		11/26/14 10:42:27				[4] _Get pcap file		
Suspicious Behavior Observed				Analysis OS(es):		Microsoft Windows7 64-bit 6.1 sp1 14.0528 Microsoft WindowsXP 32-bit 5.1 sp3 14.0528 Microsoft Windows7 32-bit 6.1 sp1 14.0528 Microsoft WindowsXP 32-bit 5.1 sp2 14.0528		
OS Change Detail (version: 4.2420) Items: 7 OS Info: Microsoft Windows7 64-bit 6.1 sp1 14.0528 Top								
Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)				Process ID	Parent ID	File Size
Analysis	Malware							
Os		Name: windows Version: 6.1.7601 Service Pack: 1						
Os Monitor		Version: 14R1 Build: 210263 Date: May 8 2014 Time: 14:25:30						
Uac	Service	Multimedia Class Scheduler						
Uac	Service	Windows Time						
Regkey	Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS\Start" = 0x00000003				472		
OS Change Detail (version: 4.2420) Items: 7 OS Info: Microsoft WindowsXP 32-bit 5.1 sp3 14.0528 Top								
Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)				Process ID	Parent ID	File Size
Analysis	Malware							
Os		Name: windows Version: 5.1.2600 Service Pack: 3						
Os Monitor		Version: 14R1 Build: 218052 Date: May 28 2014 Time: 18:57:15						

- ✓ Расследование инцидента и определение хронологии событий
- ✓ Определение всех зараженных машин (экспертиза с необходимым инструментарием)
- ✓ Разработка и внедрение инструкции по очистке зараженных машин (абсолютно нетривиальный процесс)
- ✓ Изоляция зараженных машин
- ✓ Тотальная (централизованная) смена паролей
- ✓ Запрет и контроль запуска средств удаленного администрирования

НАШИ ДНИ. И ПОВТОРИТСЯ ВСЕ, КАК ВСТАРЬ...

Социальная инженерия Новые вирусы Новые идеи

По данным WHOIS.TCINET.RU:

⌘ By submitting a query to RIPN's Whois Service
⌘ you agree to abide by the following terms of use:
⌘ <http://www.ripn.net/about/servpol.html#3.2> (in Russian)
⌘ <http://www.ripn.net/about/en/servpol.html#3.2> (in English).

```
domain:      EXTERN-CONTUR.RU
nserver:     ns5.hosting.reg.ru.
nserver:     ns6.hosting.reg.ru.
state:       REGISTERED DELEGATED, UNVERIFIED
person:      Private Person
registrar:   REGRU-RU
admin-contact: http://www.reg.ru/whois/admin_contact
created:     2014.11.12
paid-till:   2015.11.12
```

По данным WHOIS.NIC.RU:

```
domain:      CONTUR-EXTERN.RU
nserver:     ns1.sedoparking.com
nserver:     ns2.sedoparking.com
state:       REGISTERED DELEGATED
person:      Private person
admin-contact: https://www.nic.ru/cgi/whois_webmail.cgi?domain=CONTUR-EXTERN.RU
registrar:   RU-CENTER-RU
created:     2007.09.17
paid-till:   2015.09.17
source:      RU-CENTER
```

>>> Last update of WHOIS database: 2014.12.09T22:26:29Z <<<
⌘ By submitting a query to RU-CENTER's Whois Service
⌘ you agree to abide by the following terms of use:
⌘ <http://www.nic.ru/about/servpol.html> (in Russian)
⌘ <http://www.nic.ru/about/en/servpol.html> (in English).

Message ID: E1Xrgy5-0006Zr-Ca@extern-contur.ru
Email Analysis Type: attach
Timeframe: 1 month

Page: 1 of 1

ID	Device	Type	File Type	Malware	Name	Md5sum	Submitted
85097	sec-feex00	Attachment	rtf	FE_Exploit_CVE_2014_1761_RTF	???? ? 81-?????-14-115.doc	1b8b3657bcebd8ed094b6e8e943cc458 Get malware binary	11/21/14 08:41:56

Malware: ■ FE_Exploit_CVE_2014_1761_RTF
Application Type: MS Word 2003
File Type: rtf
Original analyzed at: 11/21/14 07:04:38
Yara rules: ■ FE_Exploit_CVE_2014_1761_RTF
FE_Exploit_CVE_2012_0158_RTF
FE_Exploit_MSCOMCTL_JMPESP_RTF
FE_Exploit_ObfsStrm_RTF

■ Malicious Behavior Observed

Analysis OS(es):
[1] [Get pcap file](#)
[2] [Get pcap file](#)
[3] [Get pcap file](#)
[Microsoft Windows7 32-bit 6.1 sp1 14.0528](#)
[Microsoft WindowsXP 32-bit 5.1 sp3 14.0528](#)
[Microsoft WindowsXP 32-bit 5.1 sp2 14.0528](#)

МОЖЕТ ЧТО-ТО ЕЩЕ?



Интеграция с SIEM



Интеграция с IDS



Интеграция с IPS



Интеграция с HelpDESK

СПАСИБО ЗА ВНИМАНИЕ!