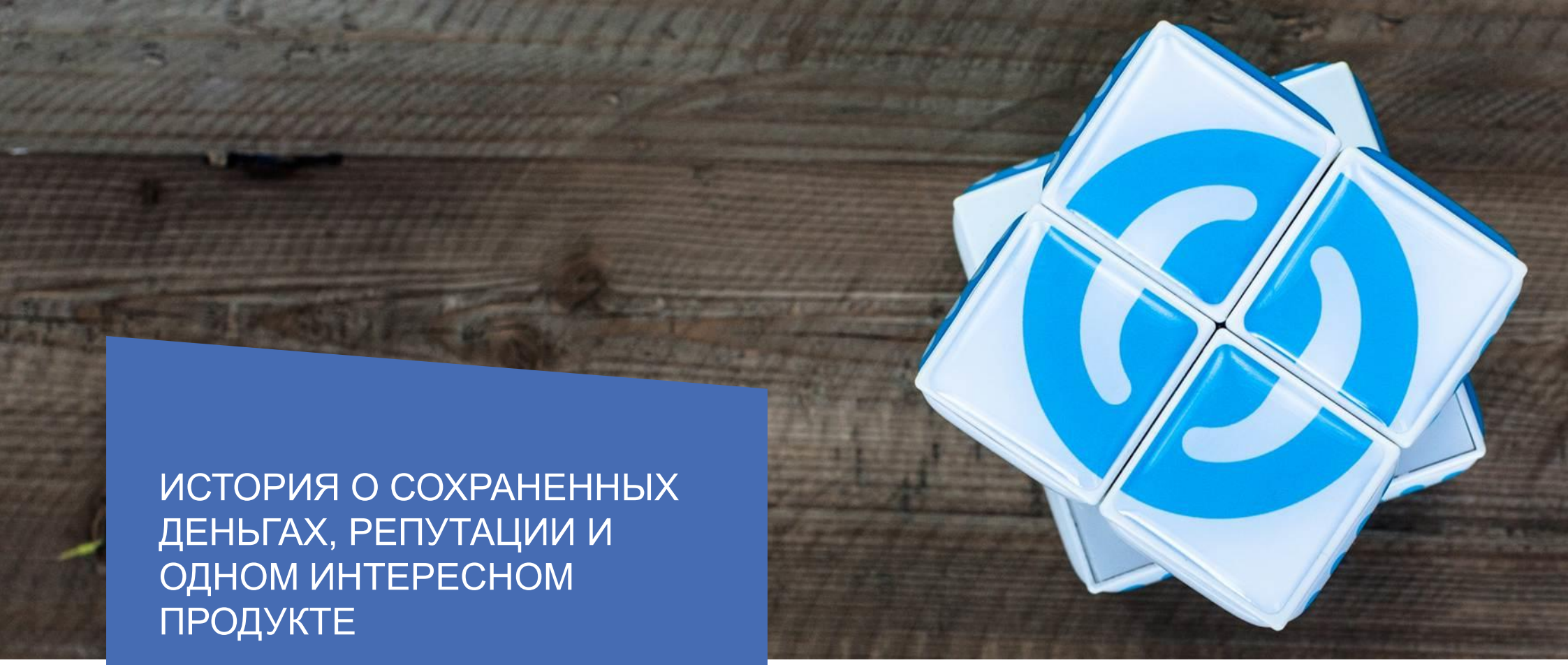


ИСТОРИЯ О СОХРАНЕННЫХ ДЕНЬГАХ, РЕПУТАЦИИ И ОДНОМ ИНТЕРЕСНОМ ПРОДУКТЕ

открытие | ХОЛДИНГ

Инфосекьюрити

IT Guard

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 рокет-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 волне 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

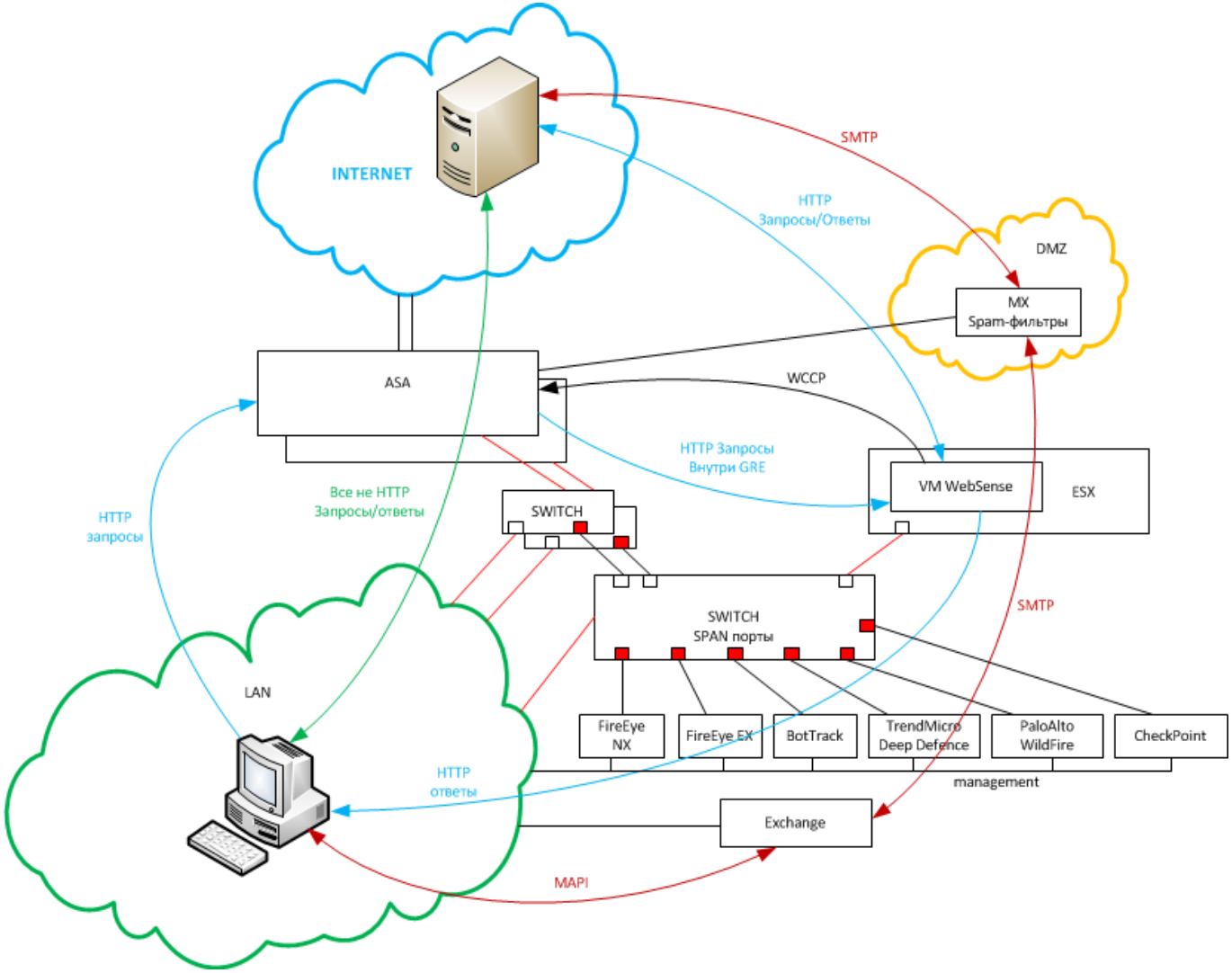
- Перехват конфиденциальной информации
- Доступ к СДБО
- Доступ к Процессингу
- Доступ к Управляющим рабочим станциям (банкоматы и пр.)

РЕГИСТРАЦИЯ И УСТРАНЕНИЕ ИНЦИДЕНТА

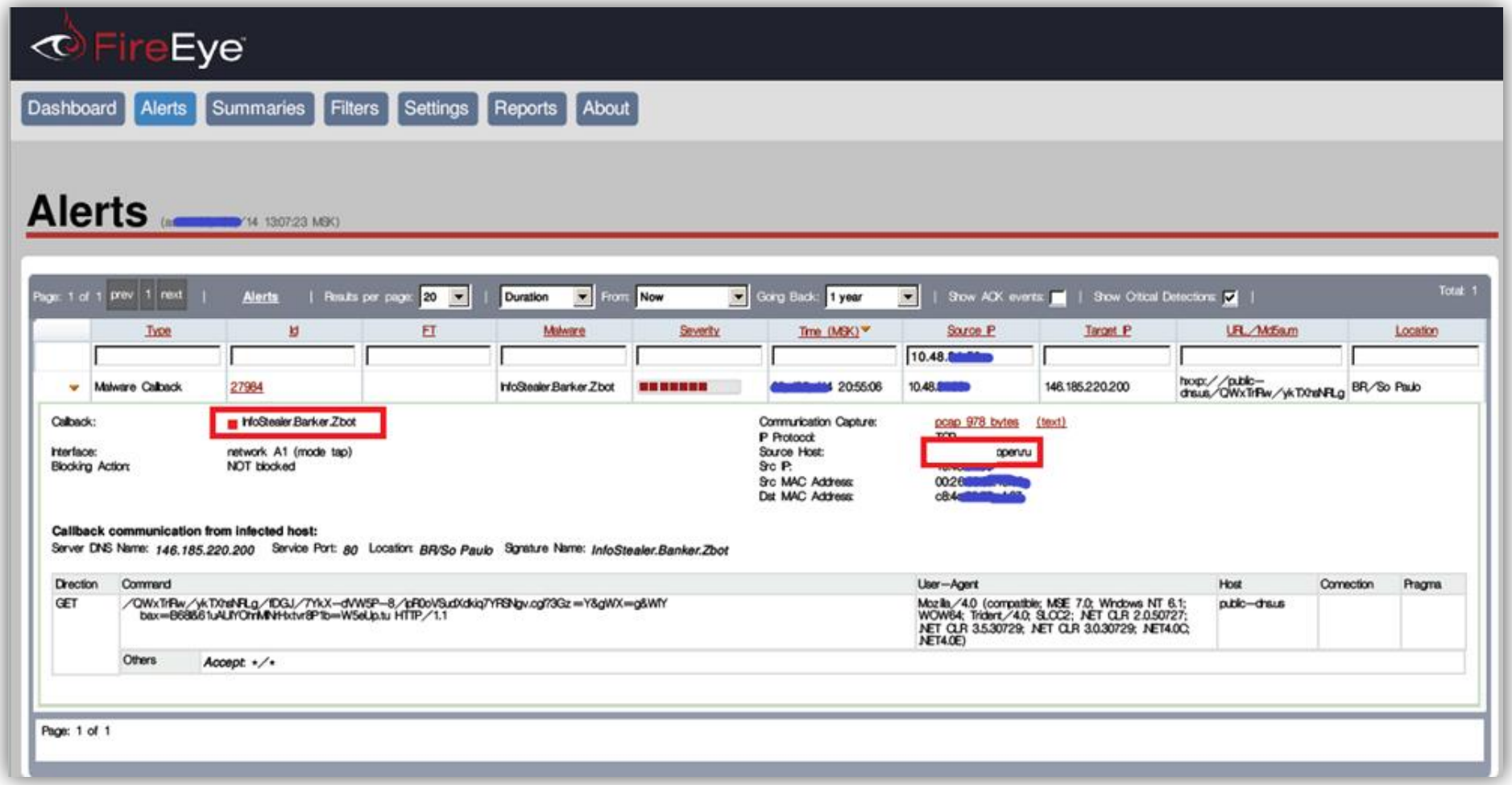
ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА

- 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**

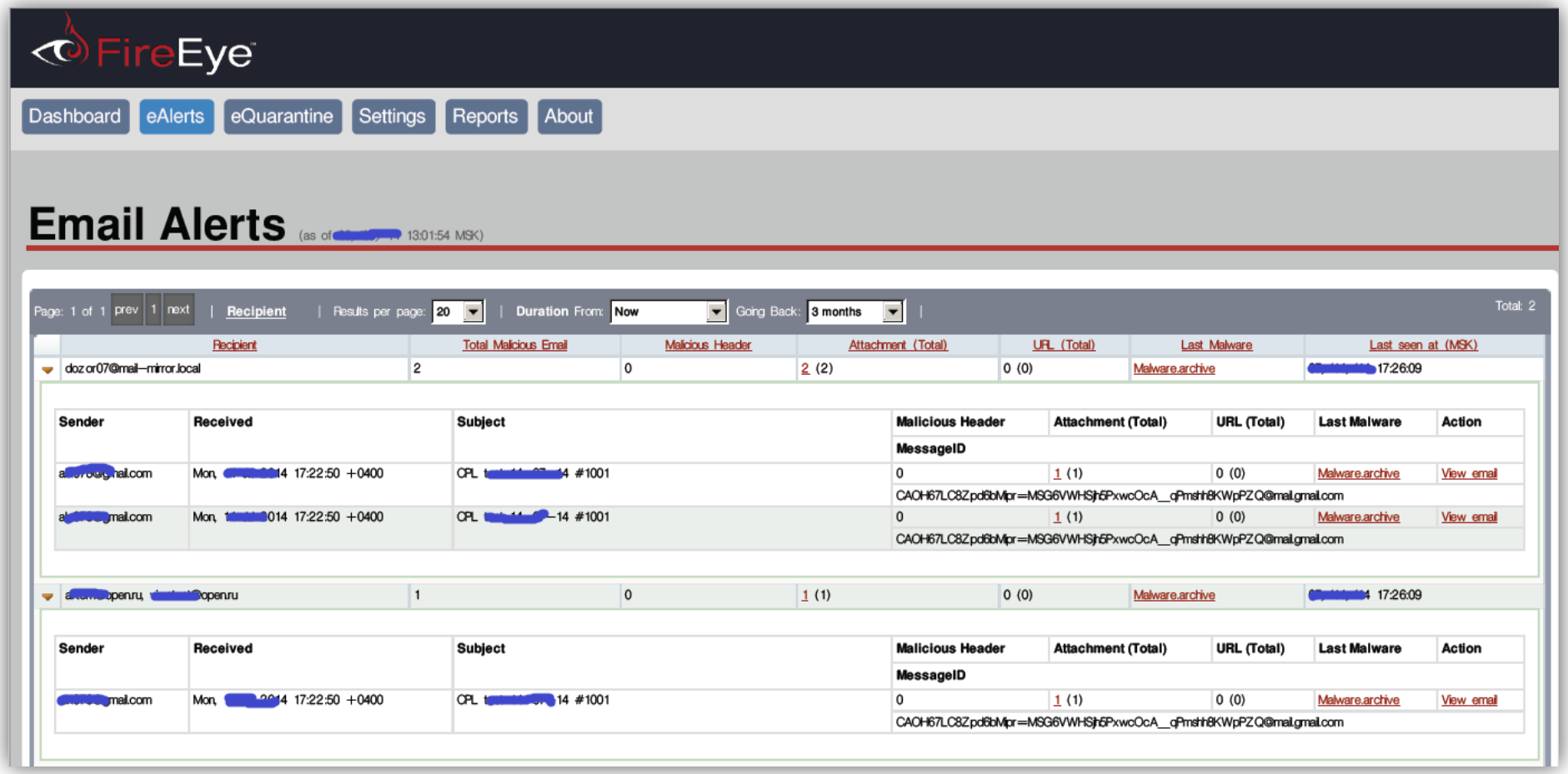
ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: РАЗВЕРНУТЫЙ ТЕСТОВЫЙ СТЕНД



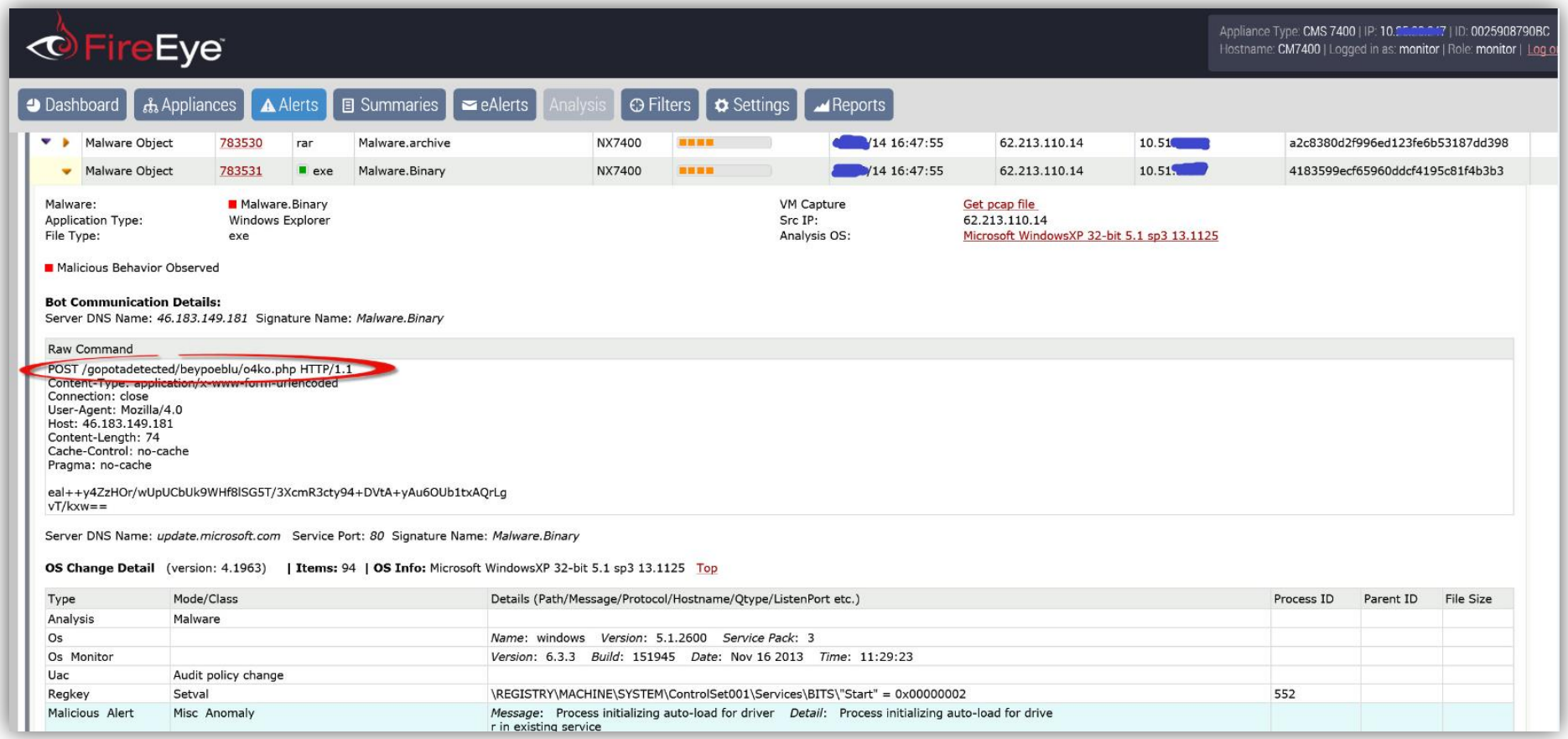
ЗАХВАЧЕННЫЕ ХОСТЫ



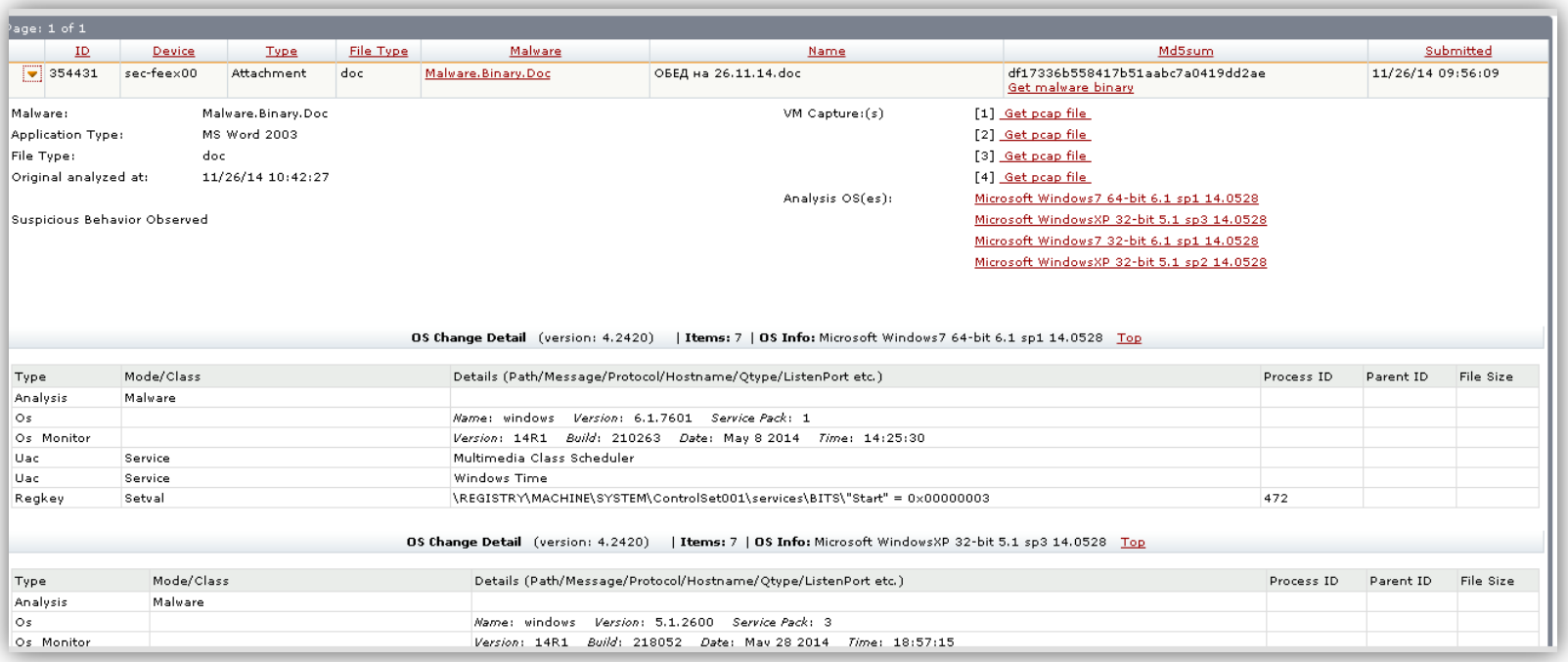
ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: ОБНАРУЖЕНИЕ ИНФИЦИРОВАННЫХ ПИСЕМ С ПОМОЩЬЮ FIREEYE EX 5400



ДЕТЕКТИРОВАНИЕ ИНЦИДЕНТА: FIREEYE NX 7400



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
Application Type: MS Word 2003
File Type: doc
Original analyzed at: 11/26/14 10:42:27

Suspicious Behavior Observed

VM Capture:(s) [1] Get pcap file [2] Get pcap file [3] Get pcap file [4] Get pcap file

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: attch
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_IMPESP_RTF
FE_Exploit_ObfsStrm_RTF

Malicious Behavior Observed

VM Capture:(s)
[1] Get pcap file
[2] Get pcap file
[3] Get pcap file
Analysis OS(es):
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!