Подходы, методы и решения в обеспечении информационной безопасности: практический опыт

Виктор Гурин,
hv@cert.by

PenTesting — поиск входа
PostTesting — поиск вошедших

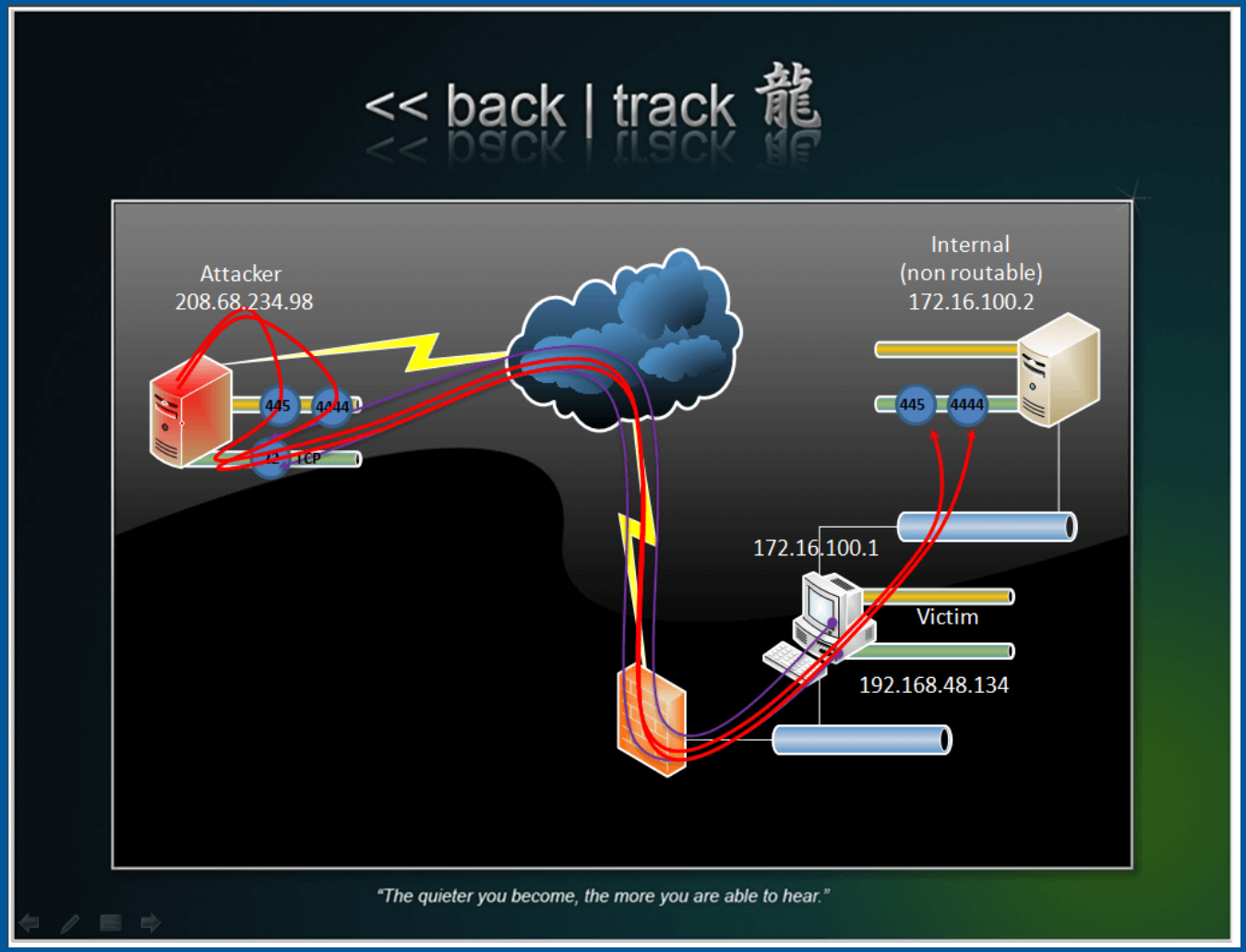
Сравнение PostTesting с общепринятыми методиками

Анализ инцидента на базе PostTesting

Анализ кибернетических групп

PenTest

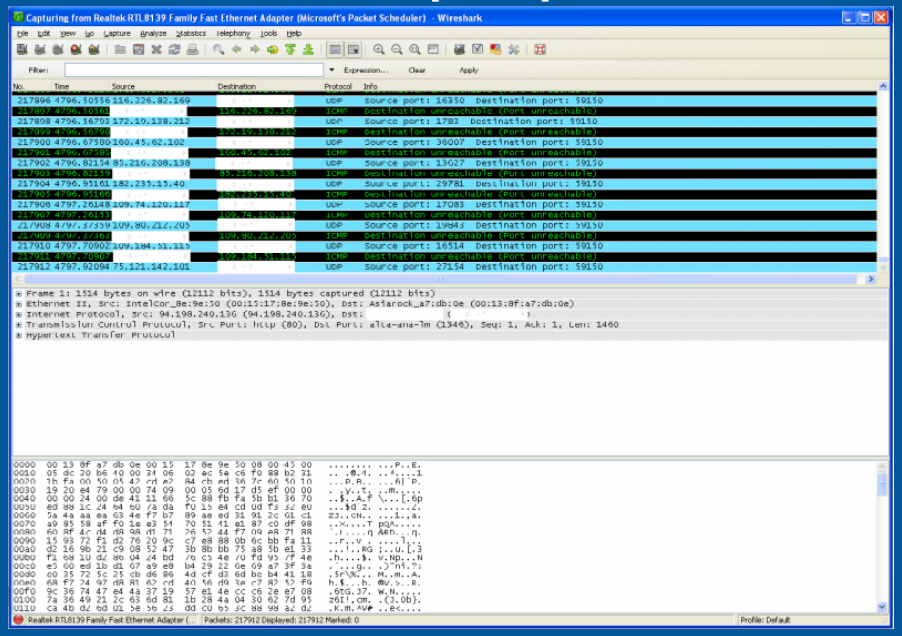
Выявление мест, через которые злоумышленник **может проникнуть** в инфраструктуру



Используемые признаки

Сеть:
Анализ событий безопасности;
Известные C&C;
Аномалии трафика.

Рабочая станция:
Аномалии системы;
Нестандартные изменения системы;
их природа и источник.



Подходы CERT.BY
PenTesting vs PostTesting

	PenTesting	**PostTesting**
1.	Какие слабые места, приложения, настройки есть в системе (обычно во входе в систему) согласно каталогу уязвимостей	Выявление скомпрометированных элементов инфраструктуры, в том числе внутри самой инфраструктуры
2.	Выдача результата как совокупность выявленных уязвимых мест	Анализ действий, результат проникновения
3.	Повторное исследование через промежуток времени для контроля	Блокирование выявленных угроз, в том числе в последующем, предотвращение и оценка реального ущерба (технический уровень)

Подходы CERT.BY

Антивирусные облака

vs

Собственная лаборатория (исследовании состояний системы)

Подходы CERT.BY

	Антивирусные облака	*Исследование состояния системы*
1.	Получение информации (зачастую избыточной и конфиденциальной) о действиях системы, в том числе пользователя	Выявление аномалий в ОС (где запускается утилита), **а также сетевых аномалий, получаемых от уполномоченных поставщиков Интернет-услуг**
2.	Анализ представленных, одновременных событий у разных пользователей продукта АВП	Анализ полученной информации с целью выявления изменений, полученных в результате деятельности ВПО.
3.	Принятие решения на базе статистической информации (неприменимо к APT, сработок которых крайне мало)	Получение экземпляра для последующего анализа. Выявление признаков ВПО и передача их взаимодействующим сторонам (не только тем, у кого стоит утилита)

Анализ

HOME

Autorun: : : ::
IMG001.exe : : C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\IMG001.exe ::
Punto Switcher.lnk : : C:\Users\user_208_2082\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Punto Switcher.lnk :: Подписан
Google Chrome.lnk : : C:\Users\user_208_2082\Application Data\Microsoft\Internet Explorer\Quick Launch\Google Chrome.lnk :: Подписан
Launch Internet Explorer Browser.lnk : : C:\Users\user_208_2082\Application Data\Microsoft\Internet Explorer\Quick Launch\Launch Internet Explorer Browser.lnk :: Подписан
Mozilla Thunderbird.lnk : : C:\Users\user_208_2082\Application Data\Microsoft\Internet Explorer\Quick Launch\Mozilla Thunderbird.lnk :: Подписан
Shows Desktop.lnk : : C:\Users\user_208_2082\Application Data\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk :: Подписан
Window Switcher.lnk : : C:\Users\user_208_2082\Application Data\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk :: Подписан
Shows Desktop.lnk : : C:\Users\administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk :: Подписан
Window Switcher.lnk : : C:\Users\administrator\Application Data\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk :: Подписан
Mozilla Thunderbird.lnk : : C:\Users\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Mozilla Thunderbird.lnk :: Подписан
Shows Desktop.lnk : : C:\Users\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk :: Подписан
Window Switcher.lnk : : C:\Users\Admin\Application Data\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk :: Подписан
HotKeysCmds : Software\Microsoft\Windows\CurrentVersion\Run : C:\Windows\system32\hkcmd.exe :: Подписан
IgfxTray : Software\Microsoft\Windows\CurrentVersion\Run : C:\Windows\system32\igfxtray.exe :: Подписан
Persistence : Software\Microsoft\Windows\CurrentVersion\Run : C:\Windows\system32\igfxpers.exe :: Подписан
SynTPEnh : Software\Microsoft\Windows\CurrentVersion\Run : %ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe :: Подписан
SysTrayApp : Software\Microsoft\Windows\CurrentVersion\Run : C:\Program Files\IDT\WDM\sttray64.exe :: Подписан
Sidebar : S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Run : %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun :: Подписан
Sidebar : S-1-5-20\Software\Microsoft\Windows\CurrentVersion\Run : %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun :: Подписан
ccleaner : S-1-5-21-2541418808-2970423025-3187528270-1202\Software\Microsoft\Windows\CurrentVersion\Run : "C:\Program Files\CCleaner\CCleaner64.exe" /AUTO :: Подписан

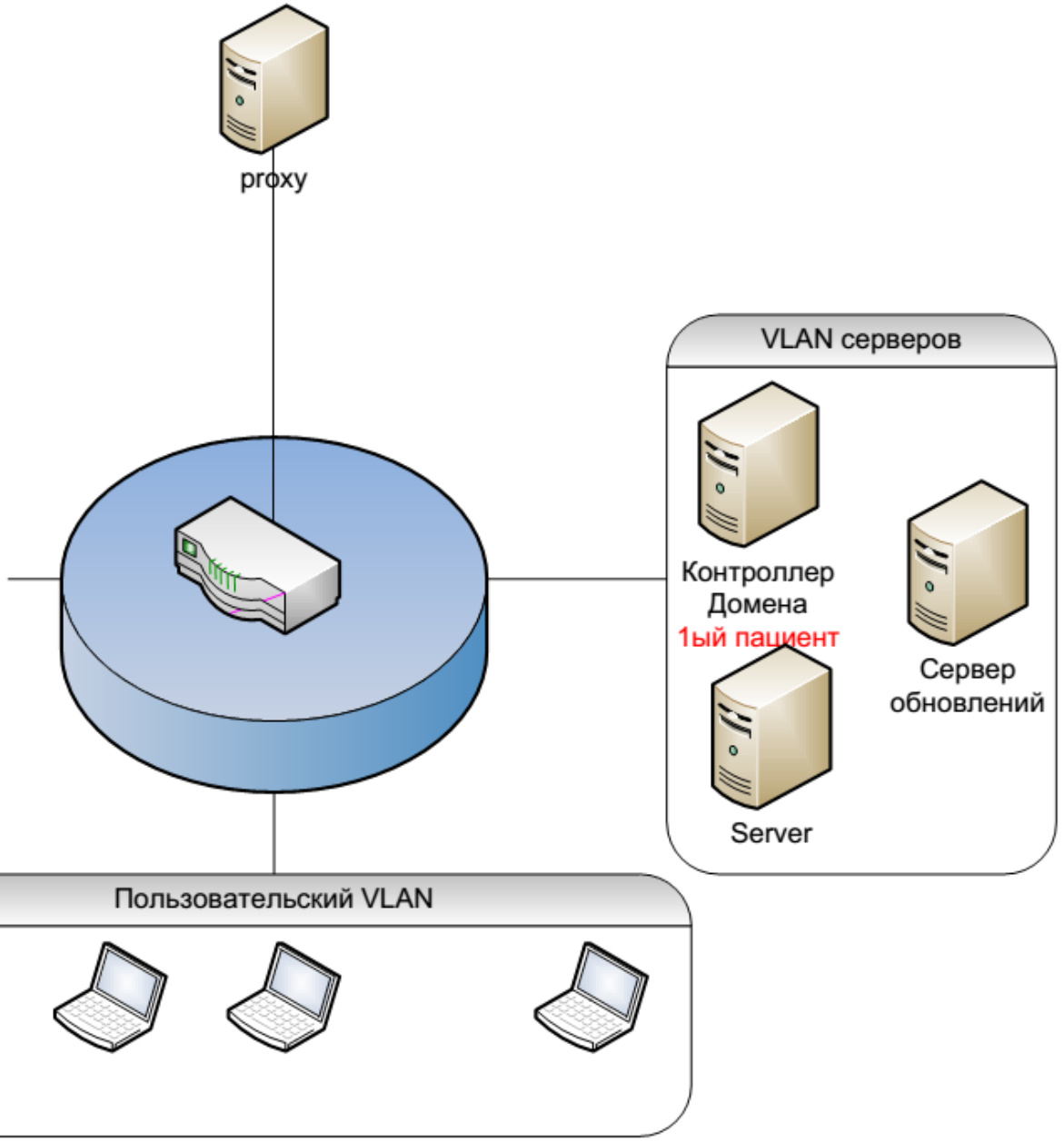
14	user_c	2upr	PC-508-5051	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
15	user_c	2upr	PC-511-5221-2	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
16	user_c	2upr	PC-511-5221-2	IMG001.exe	C:/Users/Administrator/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
17	user_c	2upr	PC-513-5241	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
18	user_c	4upr	PC-401-4133	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
19	user_c	4upr	PC-403-4112	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016
20	user_c	4upr	PC-407-4063	IMG001.exe	C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup/IMG001.exe	09.03.2016

Этапы заражения

1) Заражен 0-ой компьютер – гараж
2) Вход с 0-го компьютера по администратором домена - заражение сервера администратора доменов
3) Заражение машин от имени администратора домена (в том числе и других серверов) , пути которых были закешированны на момент заражения

Поведение зараженной машины

1) Попытки прописаться в открытые сетевые папки по известным путям сети
2) Перебор по библиотеке сочетаний логин:пароль к обнаруженным машинам для получения доступа
3) Попытка создания записи в автозагрузке используя маски стандартных путей windows



ВОПРОС: как распространялась ВПО между машинами, если p2p заблокирован?

Дальнейший анализ показал,
что при отключенной настройке
неиспользования прокси для локальной сети,
запрос через системные настройки (прокси)
будет идти через прокси,
а не p2p, что разрешено сетью.

Классификация угроз(групп) по используемым подходам, технологиям

Классификация объектов по обрабатываемой информации, сферам ответственности

Получение вектора заражения

Использования «сигнальных» объектов (обычно те, с кем хорошее взаимодействие).

Анализ инфраструктур объектов того же класса заражения

Выявление группы, использовавшей для C&C один и тот же хостинг

Выявление всех Зараженных объектов, разделение на группы «интересов»

Выявлены группы одного направления (финансовая, инвестиционная, технологическая, военная). Определение «сигнальных» объектов по каждой группе (один из НИИ)

Установка точек контроля на «входе» в систему
Выявление попытки заражения, анализ подобных действий у других объектов

Наш подход это

Выявление APT другим способом, надежным, стабильным.
Из минусов — не онлайн, часть объектов уже будут зараженными

Поиск APT нестандартным подходом

Мониторинг
групп злоумышленников
и сфер их интересов

Открытость для взаимодействия.
внедрения к заинтересованным
Предоставления признаков заражения,
пока для тех с кем работаем,
в перспективе — для общественности

Объекты – государственно-частного сектор,
у которого и коммерческая тайна
в том или ином виде,
и чувствительная информация,
похищение которой крайне нежелательно

ВОПРОСЫ?