Практика выявления реальных инцидентов по рассылкам от FinCERT

Эльман Бейбутов

Руководитель направления аутсорсинга ИБ

О чем пойдет речь

- Об информационном обмене с FinCERT
- Подход Solar JSOC к выявлению векторов атаки
- Что делать если найдены индикаторы

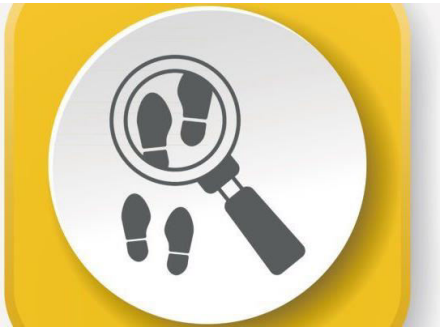
Solar JSOC и FinCERT

- Первое соглашение о сотрудничестве FinCERT подписал с Solar JSOC

- Первый webinar FinCERT запустил 8 апреля 2016 года совместно с Solar JSOC
- Ежеквартальные встречи в рамках клуба «SOC в России» при поддержке Solar JSOC

SOC
В РОССИИ
ЗАКРЫТЫЙ ПРОФЕССИОНАЛЬНЫЙ КЛУБ

- Двусторонний информационный обмен
- Техническая интерпретация рассылок от FinCERT



IOC – Общая информация

- Большинство индикаторов укладываются в следующие категории:
  - сетевые индикаторы: ip\domain, url, user agent, e-mail адреса и т.д.
  - хостовые индикаторы: file name\path, process name\path, file hash, registry и т.д.

- Индикаторы можно проверять различными средствами:
  - SIEM\Log Management
  - визуальная проверка (tcpview, process monitor, autoruns)
  - скрипты на powershell, bat
  - сканеры анализа защищенности (Qualys, MaxPatrol, etc)
  - утилиты по поиску IOC
    - loki (https://www.bsk-consulting.de/loki-free-ioc-scanner),
    - yara (http://plusvic.github.io/yara/),
    - ioc_scanner\redline (https://www.fireeye.com/services/freeware.html)

Подход к выявлению атаки

Что и как ищем

Рассылка писем, содержащих вредоносный код типа Trojan.Downloader с почтового адреса **info@fincert.net.**

Информация для тех участников информационного обмена, кто открыл вредоносный файл: рекомендуем изолировать машину от сети и проверить систему на наличие маркеров заражения согласно бюллетеню ВК-20160303-001 (файл данного бюллетеня прикреплен к сообщению).

2. Основные меры противодействия

№	Мера противодействия	Разъяснение
1	Обновление антивирусных баз	-
2	Добавление отправителя в спам-фильтр на почтовом шлюзе	info@fincert.net

3. Маркеры заражения (рассмотрены на одном из типов вредоносного вложения)

3.1 Вредоносный код представляет собой файл *20160314 - 001 - Возможная компрометация АРМ КБР .doc*.

После активации на компьютере можно увидеть появившиеся процессы **ROMServer.exe** и **romfusclient.exe** (программа предназначена для удаленного управления компьютером).

Файлы программы в составе ROMServer.exe, romfusclient.exe, aledensoftipcserver.dll, avicap32.dll, Config, english.lg, msimg32.dll находятся по пути **C:\Users\<User Name>\AppData\Roaming\Microsoft\MTM**.

3.2 Маркеры данного вредоносного файла:

MD5:	5e268a88b9f5c2591ac01755601d44b0
SHA1	40692503630582bd6b95ec226cec230948d3894b

При обнаружении указанных маркеров на АРМ подготовки рейса или АРМ КБР, а также иных АРМ, отвечающих за формирование рейса, либо имеющих отношение к обеспечению платежных операций, **НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТСЯ** переустановить («переподнять») зараженный АРМ на чистой ПЭВМ, изолировав от остального сегмента локальной сети!

№	Тип	Значение	Комментарий
1.	IP адрес	184.22.223.171	Бэк-коннект сервер удаленного управления
2.	IP адрес	193.124.17.223	Командные сервера бот-клиента
3.	IP адрес	85.93.5.103:80	
4.	Идентификатор	GUID{BFFB193D-2D66-4B8B-9CF9-F67FDEEF6619}	Идентификатор плагина IE (Safe Browsing), в реестре Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Browser Helper Objects\
5.	Файл	Internet Explorer\Plugin (или Safe Browsing.plugin)	Плагин IE, скрывающий активность в окне браузера. Также следует проверить наличие подобного плагина в списке плагинов IE
6.	Файл	Mbrkiller.exe	Уничтожает загрузочные записи
7.	Файл	1.cab, install.cab (в %TEMP%, %APPDATA%)	Архив с ботнет-клиентом
8.	Файл	1.dat, install.dat (в корне системного диска, %TEMP%, %SYSTEM%, %APPDATA%)	Бинарный код вредоносного ПО, инжектируемого в контекст доверенного приложения (содержимое файла отлично от plain text!)
9.	Файл	kdns32.exe (в корне системного диска, %TEMP%, %SYSTEM%, %APPDATA%)	Вредоносное ПО, выполняющее инжект файла п.8
10	Файл	load.exe (%TEMP%, возможно в %APPDATA%)	Загрузчик архива вредоносного ПО (файла 1.cab, install.cab)
11	Набор файлов	System.dll, nsProcess.dll, 7za.exe (в %TEMP%), ExecCmd.dll, pn_pack1.exe (lmpack1.exe), ROMServer.exe, ROMFUSClient.exe	Плагины ботнет-клиента, конкретный набор зависит от окружения. Рекомендуется выполнить поиск по всему диску

Анализ сетевых IOC

Особенности сетевых IOC:

- Больше всего ложных срабатываний.
- Большой объем данных. Есть смысл хранить «метаданные» - ip\host\urlhost\day для быстрого поиска
- На МЭ редко включен аудит сессий. В случае если есть хосты с доступом в интернет в обход прокси – лучше включать заранее.
- Прокси\почтовые сервера как правило уже ведут необходимые логи и по ним есть отчетность минимум 2-3 недели, чего достаточно в большинстве случаев
- Подготовить инструменты для быстрого поиска по нужным индикаторам\договориться с администраторами по нужным отчетам

Анализ хостовых IOC

- Рекомендации
  - По возможности не вносить изменения на потенциально зараженных хостах
  - Настройте необходимый аудит на всех хостах. Это сэкономит время
  - Заранее определите какие индикаторы какими средствами можно искать с минимальными затратами
  - При поиске индикаторов по файлам\процессам – учитывайте полный путь, чтобы избежать ложных срабатываний

Один случай из жизни крупного банка - клиента Solar JSOC

Фиксация инцидента:

- Обнаружено обращение к ip C&C с АРМ сотрудника расчётного центра
- АРМ имеет доступ к работе с отчетностью МЦИ – инцидент высокой критичности
- Эвристика по АРМ установленным антивирусом – результата не дала
- Проверка альтернативным антивирусом выдала вердикт – Обнаружен PDM:Trojan.Win32.Generic

Итоги разбора:

- Вредоносное ПО, маскирующееся под системный процесс sys.exe
- Установлен при запуске файла skazki_dlya_bolshih_i_malenkih.pdf.exe более года назад
- Не детектировался антивирусными базами ни одного из вендоров
- Функционал
  - Фиксация снимков экрана каждые 5 минут
  - Запись клавиатурных вводов
  - Отправка всех данных через прокси на центр управления

Что делать если есть срабатывания

- Начинайте с тех данных, которые удалось получить
  - Какие IOCи сработали?
  - В каком кол-ве на каких хостах?
  - Есть ли явные ложные срабатывания? Возможно стоит поправить скрипты\параметры поиска
- Если найдены индикаторы на критичных хостах
  - Есть активные сессии\процессы – блокируем\изолируем хост
  - Перезалейте хост из образа (лучше выдать новое рабочее место а зараженный хост изолировать\сохранить образ)
  - Сменить все пароли
  - Проверить кто еще подключался к этому хосту (администраторы, саппорт, другие пользователи). Их данные тоже могут быть скомпрометированы
  - Соберите информацию по вредоносам (файлы\доп. IOCи) и отправьте ее вендору\fincert.
- Постарайтесь определить как хост был заражен
  - Почта\веб\флешки\сторонний софт?
  - Были ли удаленные сессии (rdp\admin share)
- Поставьте на мониторинг найденные индикаторы

Что делать если есть срабатывания

- В менее критичных случаях
  - Проверка наличия\актуальности AV. Если нет – установка.
  - Полная проверка хоста антивирусом с последними базами (возможно, после того как вендор добавит сигнатуры)
  - Удаление найденных файлов
  - Работа с пользователями
  - В идеале – замена хоста и смена паролей, чтобы мотивировать пользователей не кликать по ссылкам

Каким должно быть время реакции?

Фазы и время реализации целенаправленной атаки:

- Разведка – **непрерывная и нецеленаправленная** (бот-нет, трафферы)
- Проникновение:
  - Преодоление периметра – **60% день/20% вечер/20% ночь**
  - Соц.методы – **80% день/10% вечер/10% ночь**
  - Фишинг – **50% день/40% вечер/10% ночь**
- Закрепление – **непрерывно**, но ключевые вехи – **вечер**
- Достижение цели – **40% вечер пятницы/20% выходные/20% вечер**

Спасибо за внимание!

Компания Solar Security
+7 499 755 07 70
Центр мониторинга и реагирования на инциденты JSOC
http://solarsecurity.ru/products/jsoc/