Несколько историй из жизни JSOC CERT

или нестандартная форенсика

МОСКВА 28 ноября, 2018

#whoami

Victor Sergeev
Senior DFIR engineer @ JSOC CERT (RTK-Solar)

Будни JSOC CERT

Оценка компрометации сети

Ретроспективный анализ АРМ

Реверс-инжиниринг вредоносного ПО

Экстренное разворачивание мониторинга

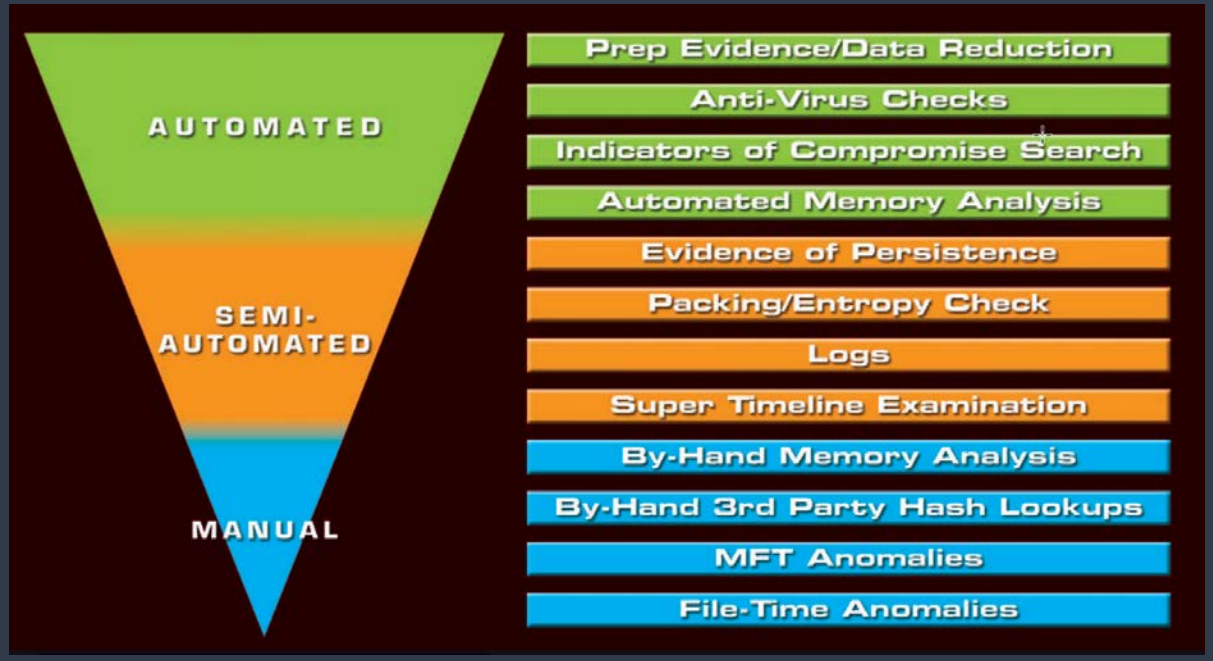
Координация работ по реагированию

} подобные действия во время расследований хорошо описываются методиками

Детально описанный playbook позволяет масштабировать даже комплексные расследования, т.к. по ним можно действовать полуавтоматически

Поиск активной компрометации

Если ВПО не удалено и активно работает, то для его поиска можно применять классическую методику SANS:



Но есть easy win - проверка диска в динамике (песочнице)

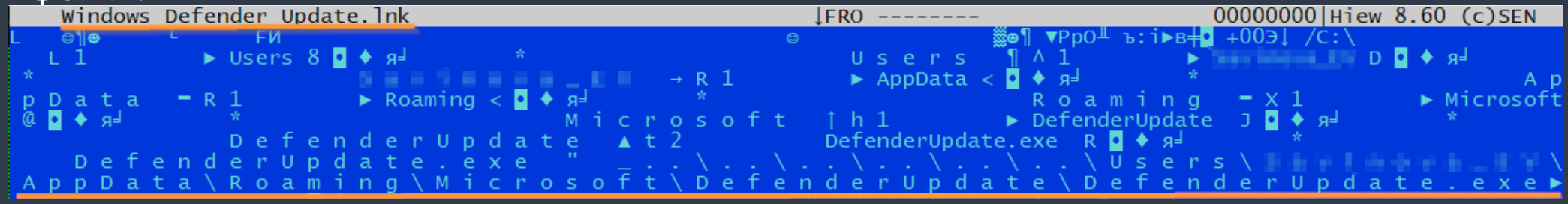
1) Конвертируем dd-образ диска в vmdk
2) Запускаем в Virtual Box
3) Проводим анализ как на живой системе, уделяя внимание траффику

Всегда будут инциденты, для которых нет готовых playbook

CASE 1: Поиск удаленного вредоносного ПО

Удаление ВПО усложняет методику, но не делает ее бесполезной:

- LNK-файл в автозагрузке указывает на нестандартный удаленный файл:



-

```
<fgappentry>
<process>"ROMSERVER.E"</process>
<launchcount>3</launchcount>
<fgcount>3</fgcount>
<path>"\DEVICE\HARDDISKVOLUME2\USERS\[redacted]\APPDATA\ROAMING\MICROSOFT\DEFENDERUPDATE\ROMSERVER.EXE"</path>
</fgappentry>
```

CASE 2: кто удалил мои файлы?

Нужно было настроить аудит работы с файловой системой!

https://serverfault.com/questions/881344/how-to-find-out-who-deleted-files-windows-server-2012-r2

Not unless proper auditing was configured beforehand.

```
For the system:
Advanced Audit Policy, Object Access, Audit File System (Success and Failure)

For the directory:
Advanced Security Settings, Auditing, Everyone - Delete (All)
```

With those configured, you'd see Event ID 4660 `An object was deleted` and Event ID 4663 in the Security Log:

```
An attempt was made to access an object.
  Subject:
    Security ID:        DOMAIN\USER
  Object:
    Object Name:        C:\share\one
  Access Request Information:
    Accesses:       DELETE
```

Так никто не делает.

CASE 2: кто удалил мои файлы?

При удалении файлов, их метки времени не меняются

Но меняются метки времени у папки:

- При удалении файла происходит перестроение B-дерева атрибута $INDEX_ROOT папки -> изменяются метки времени $STD_INFO
- В результате имеем аномалию в MFT:

Record Number	Active	Record type	Filename #1	Std Info Modification date	Std Info Access date	Std Info Entry date	FN Info Creation date
578754	Inactive	Folder	/del_test/xampp/tomcat/webapps/mana	2018-11-26 14:19:40.362251	2018-11-26 14:19:40.362	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4261
578750	Inactive	Folder	/del_test/xampp/tomcat/webapps/mana	2018-11-26 14:19:40.366215	2018-11-26 14:19:40.366	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4191
578766	Inactive	Folder	/del_test/xampp/tomcat/webapps/mana	2018-11-26 14:19:40.368240	2018-11-26 14:19:40.368	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4474
578768	Inactive	Folder	/del_test/xampp/tomcat/webapps/mana	2018-11-26 14:19:40.371235	2018-11-26 14:19:40.371	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4508
578112	Inactive	Folder	/del_test/xampp/tomcat/webapps	2018-11-26 14:19:40.373196	2018-11-26 14:19:40.373	2018-11-26 14:19:40.3	2018-11-26 14:18:14.8408
578774	Inactive	Folder	/del_test/xampp/tomcat/webapps/ROOT	2018-11-26 14:19:40.382191	2018-11-26 14:19:40.382	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4637
578791	Inactive	Folder	/del_test/xampp/tomcat/webapps/ROOT	2018-11-26 14:19:40.383190	2018-11-26 14:19:40.383	2018-11-26 14:19:40.3	2018-11-26 14:18:16.4956
578042	Inactive	Folder	/del_test/xampp/tomcat	2018-11-26 14:19:40.386162	2018-11-26 14:19:40.386	2018-11-26 14:19:40.3	2018-11-26 14:18:14.6290
216711	Inactive	Folder	/del_test/xampp	2018-11-26 14:19:40.399157	2018-11-26 14:19:40.399	2018-11-26 14:19:40.3	2018-11-26 14:17:36.4686
578794	Inactive	Folder	/del_test/xampp/webalizer	2018-11-26 14:19:40.399157	2018-11-26 14:19:40.399	2018-11-26 14:19:40.3	2018-11-26 14:18:16.5016
578818	Inactive	Folder	/del_test/xampp/webdav	2018-11-26 14:19:40.401146	2018-11-26 14:19:40.401	2018-11-26 14:19:40.4	2018-11-26 14:18:16.5646

CASE 2: кто удалил мои файлы?

Знаем когда файлы были удалены - определяем, кто в этот момент работал на сервере:

1. По журналам самого сервера – EventID 4624/4625
2. По журналам контроллера домена – EventID 4768
3. По траффику – netflow/журналы внутренних маршрутизаторов

А если и этих данных уже нет?

CASE 2: кто удалил мои файлы?

Shellbags!

1) Определяем по GPO кто имел доступ к папке
2) Собираем реестры со всех АРМ (напр. https://github.com/jschicht/RawCopy)
3) Кладем в Autopsy -> Shellbags plugin
4) Profit!

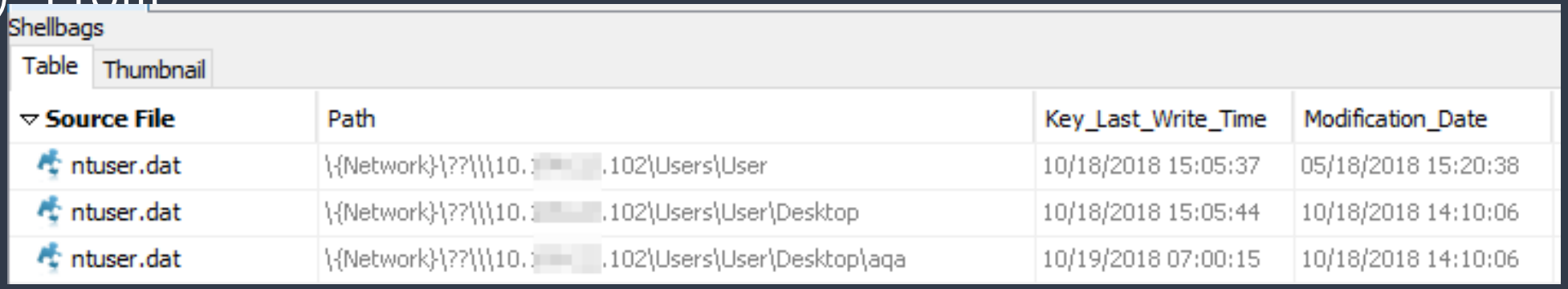

Shellbags

Table | Thumbnail

Source File	Path	Key_Last_Write_Time	Modification_Date
ntuser.dat	\{Network}\??\\\10.[redacted].102\Users\User	10/18/2018 15:05:37	05/18/2018 15:20:38
ntuser.dat	\{Network}\??\\\10.[redacted].102\Users\User\Desktop	10/18/2018 15:05:44	10/18/2018 14:10:06
ntuser.dat	\{Network}\??\\\10.[redacted].102\Users\User\Desktop\aqa	10/19/2018 07:00:15	10/18/2018 14:10:06

CASE 3: Шаг назад

Злоумышленник проник в сеть через VPN и сразу был обнаружен

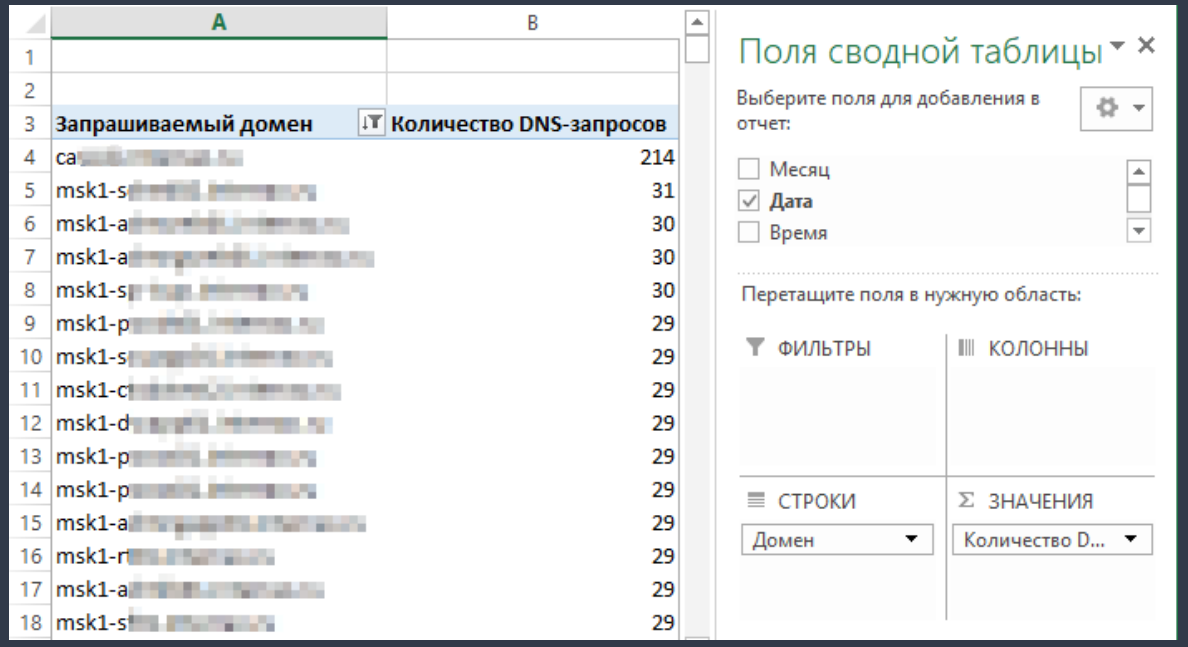
Откуда он мог узнать доменные учетные записи?

- Bruteforce?
- Mimikatz?
- Keylogger?
- Phishing?
- NTLM-hash harvesting? (напр. https://github.com/CylanceSPEAR/SMBTrap)

Проверили кучу версий – пусто. Значит нужно делать шаг назад.

CASE 3: Шаг назад

А куда он вообще ходил?

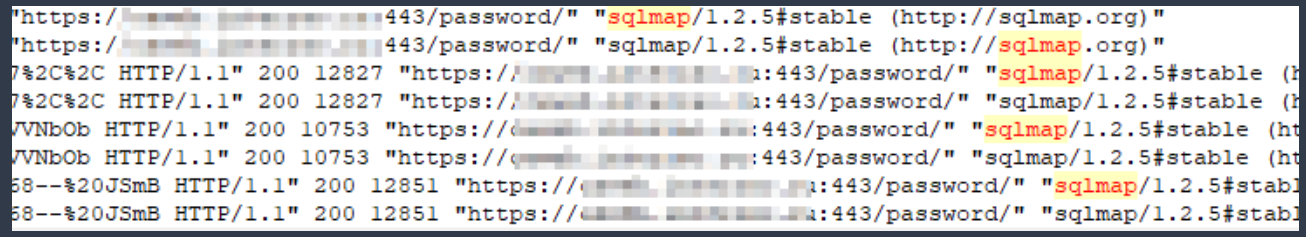


	A	B
1		
2		
3	Запрашиваемый домен	Количество DNS-запросов
4	ca	214
5	msk1-s	31
6	msk1-a	30
7	msk1-a	30
8	msk1-s	30
9	msk1-p	29
10	msk1-s	29
11	msk1-c	29
12	msk1-d	29
13	msk1-p	29
14	msk1-p	29
15	msk1-a	29
16	msk1-r	29
17	msk1-a	29
18	msk1-s	29

Много соединений на доступный из вне сервис по смене паролей. Хм....

CASE 3: Шаг назад

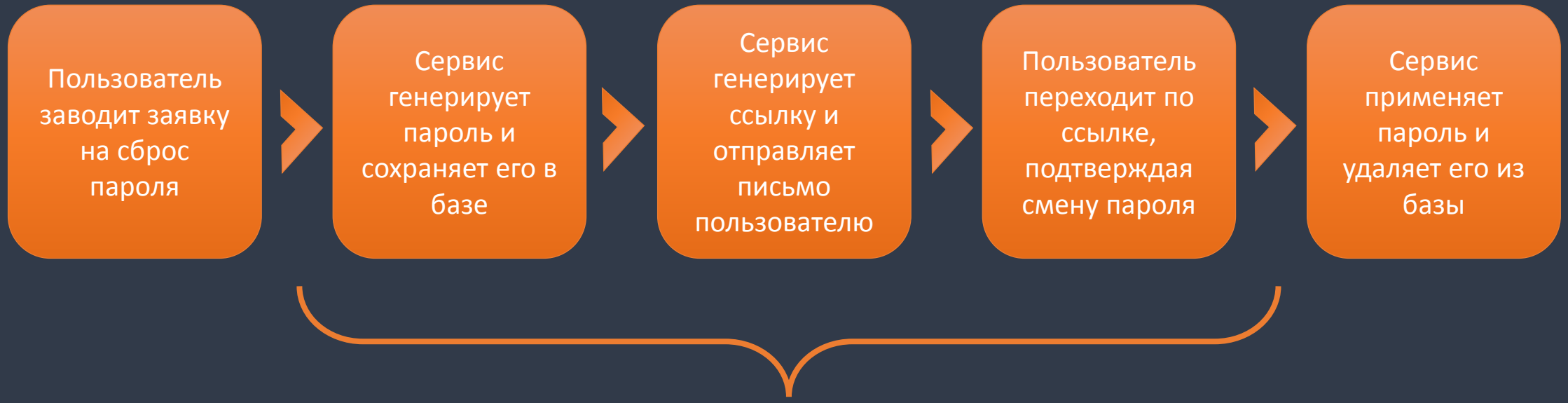
Анализ попыток атак на сервер доступный из вне часто не имеет смысла, из-за “шума Интернета”. Но не всегда.



Атаки на сервис:

1. SQLmap
2. Acunetix
3. Большое количество запросов к одной странице
   - Наверно брут логинов пользователей. Но нет ☺

CASE 3: Шаг назад



Не брут логинов, а SQL-injection!

Вопросы?

Виктор Сергеев

v.sergeev@rt-solar.ru

МОСКВА 28 ноября, 2018