

Пересечение активности GreyEnergy и Zebrocy

Kaspersky Lab ICS CERT

В октябре 2018 года компания ESET опубликовала [отчет](#), описывающий деятельность группы GreyEnergy, которая считается преемником группы BlackEnergy. BlackEnergy (также известна как Sandworm) получила широкую известность, помимо прочего, после атаки на украинские энергетические сети в 2015 году, которая привела к масштабному отключению электроснабжения. Вредоносные файлы GreyEnergy были обнаружены в атаках на промышленные и критически важные объекты, в основном на Украине.

Эксперты [Kaspersky Lab ICS CERT](#) обнаружили пересечение активности группы GreyEnergy и подмножества группы Sofacy (Fancy Bear, Sednit, APT28, Tsar Team, и др.), которое получило название [Zebrocy](#). Название Zebrocy выбрано по имени семейства вредоносных программ, которое группа Sofacy использует с середины ноября 2015 года в качестве инструмента пост-эксплуатации на компьютерах своих жертв. Мишени Zebrocy разбросаны по всему Ближнему Востоку, они находятся и в Европе, и в Азии. Большая часть целей относится к госучреждениям.

GreyEnergy и Zebrocy использовали одни и те же серверы в одно и то же время и атаковали одну и ту же организацию.

Детали

Серверы

В июле 2018 года в приватном аналитическом отчете «Лаборатории Касперского» об АРТ-угрозах за июль 2018 года «Zebrocy implements new VBA anti-sandboxing tricks» были приведены сведения о разных серверах управления группировки Zebrocy, включая **193.23.181[.]151**.

В ходе нашего исследования были найдены следующие образцы Zebrocy, которые использовали сервер **193.23.181[.]151** для скачивания дополнительных компонентов (MD5):

```
7f20f7fbce9deee893dbce1a1b62827d
170d2721b91482e5cabf3d2fec091151
eae0b8997c82ebd93e999d4ce14dedf5
a5cbf5a131e84cd2c0a11fca5ddaa50a
c9e1b0628ac62e5cb01bf1fa30ac8317
```

Эти образцы используют для скачивания дополнительных файлов URL следующего вида:

```
hxxp://193.23.181[.]151/help-desk/remote-assistant-service/PostId.php?q={hex}
```

Этот же сервер использовался в целевой фишинговой атаке GreyEnergy с применением вредоносного документа— как это уже описано в [отчете компании FireEye](#). Подробные сведения об этом документе:

- Документ (11227eca89cc053fb189fac3ebf27497) с именем “Seminar.rtf” эксплуатировал уязвимость CVE-2017-0199.
- “Seminar.rtf” скачивал с адреса: `hxxp://193.23.181[.]151/Seminar.rtf` документ второго этапа (4de5adb865b5198b4f2593ad436fceff), который эксплуатировал уязвимость CVE-2017-11882).
- Исходный документ “Seminar.rtf” был размещен на том же сервере и был скачан жертвами с адреса: `hxxp://193.23.181[.]151/ministerstvo-energetiki/seminars/2018/06/Seminar.rtf`.

Еще один сервер, который был использован как Zebrocy, так и GreyEnergy, – это **185.217.0[.]124**. Также был найден документ целевого фишинга GreyEnergy под названием “Seminar.rtf” (a541295eca38eaa4fde122468d633083), эксплуатирующий уязвимость CVE-2017-11882.

“Seminar.rtf” –
документ-
приманка
GreyEnergy)

**План проведения семинаров
в области охраны окружающей среды и недропользования на 2018 год**

| № | Наименование курса | Место проведения | Дата проведения |
|----|---|---|-----------------|
| 1 | Экологический кодекс. Правоприменение | г. Астана | 07-09 февраля |
| 2 | Экологическая экспертиза и регулирование природопользования | г. Астана | 21-23 февраля |
| 3 | Экологический кодекс. Правоприменение | Алматинская область (г.Талдыкорган, г.Алматы) | 14-16 марта |
| 4 | Государственный контроль в области охраны окружающей среды и природопользования | г.Астана | 28-30 марта |
| 5 | Инвентаризация парниковых газов. | г.Астана | 18-20 апреля |
| 6 | Экологический кодекс. Правоприменение | г.Атырау | 25-27 апреля |
| 7 | Экологический кодекс. Правоприменение | г.Астана | 23-25 мая |
| 8 | Экологический кодекс. Правоприменение | ЮКО (г.Тараз, г.Шымкент) | 29-31 мая |
| 9 | Экологический аудит | г.Астана | 13-15 июня |
| 10 | Управление отходами производства и | г.Астана | 20-22 июня |

Этот документ скачивает вредоносный файл GreyEnergy (78734cd268e5c9ab4184e1bbe21a6eb9) по SMB-ссылке:

\\185.217.0[.]124\Doc\Seminar\Seminar_2018_1.AO-A

Следующие образцы Zebrocy использовали тот же самый сервер:

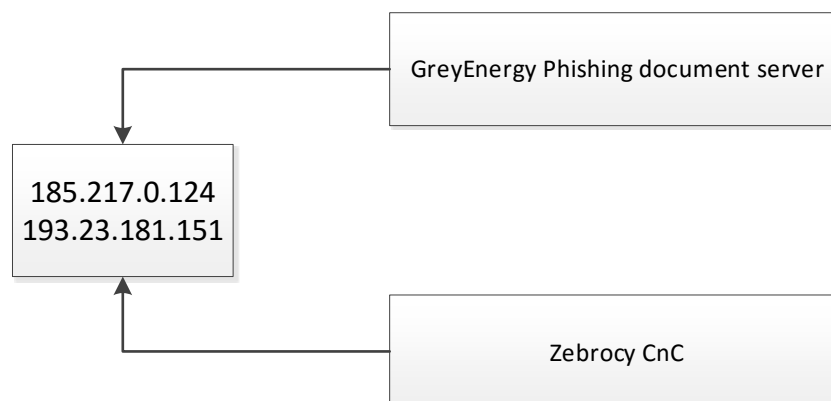
7f20f7fbce9deee893dbce1a1b62827d
170d2721b91482e5cabf3d2fec091151
3803af6700ff4f712cd698cee262d4ac
e3100228f90692a19f88d9acb620960d

Они скачивали дополнительные файлы по ссылке:

hxxp://185.217.0[.]124/help-desk/remote-assistant-service/PostId.php?q={hex}

Также стоит отметить, что по крайней мере два образца из списка выше используют оба сервера – 193.23.181[.]151 и 185.217.0[.]124 – в качестве командных.

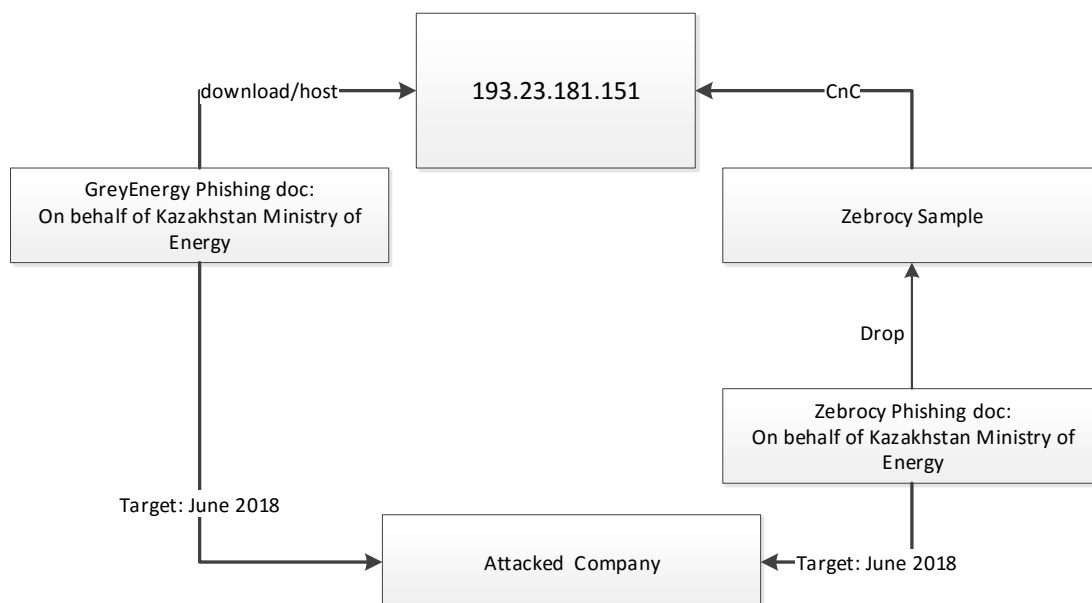
Серверы,
ассоциированные
с GreyEnergy
и Zebrocy



Атакуемая компания

Документы целевого фишинга, использованные как GreyEnergy, так и Zebrocy атаковали ряд промышленных компаний в Казахстане. Одну из компаний обе группировки атаковали в июне 2018 года.

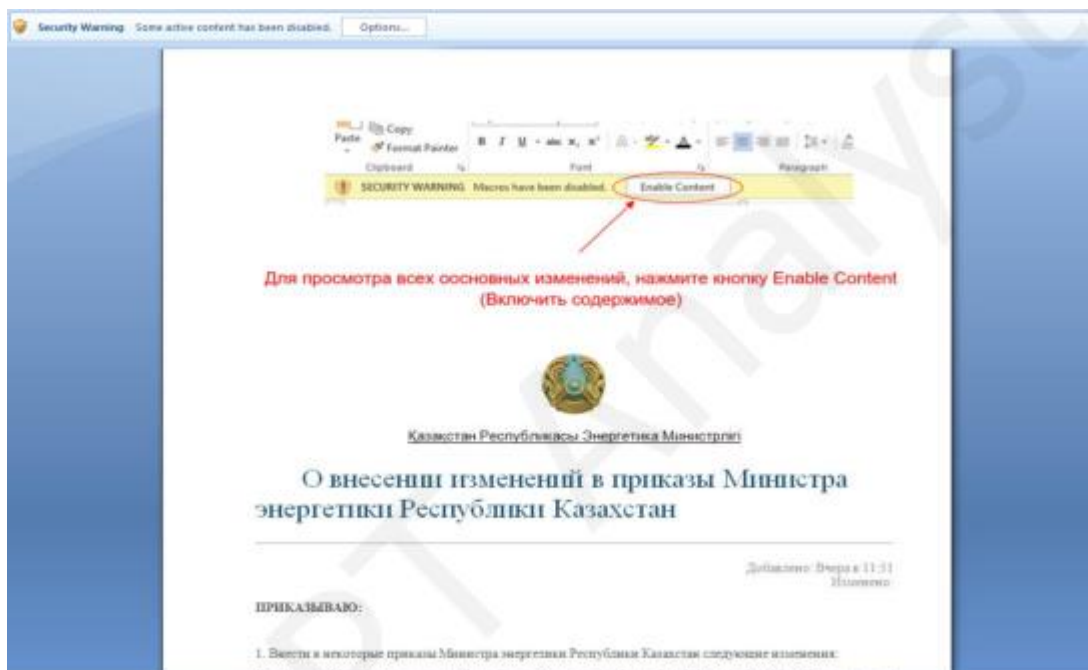
Пересечение
активности
GreyEnergy
и Zebrocy



Время атак

Документ целевого фишинга "Seminar.rtf", который устанавливал вредоносный файл GreyEnergy, был отправлен атакуемой компании приблизительно 21 июня 2018. Фишинговый документ от Zebrocy – приблизительно 28 июня.

Документ-приманка Zebrocy – “(28.06.18) Izmeneniya v prikaz PK.doc”



Оба сервера использовались обеими группами практически в одно и то же время:

- 193.23.181[.]151 использовался GreyEnergy и Zebrocy в июне 2018 года;
- 185.217.0[.]124 использовался GreyEnergy с мая по июнь 2018 года, а Zebrocy в июне 2018 года.

Выводы

GreyEnergy/BlackEnergy - продвинутая группа, обладающая обширными знаниями, связанными с проникновением в сети жертв и использованием любых известных им уязвимостей. Эта группа активно обновляет свои инструменты и инфраструктуру, чтобы избежать обнаружения, отслеживания и атрибуции.

В этой статье представлены сведения о том, как GreyEnergy и подмножество группы Sofacy, известное как Zebrocy, использовали в определенное время, хотя и по-разному, одну и ту же инфраструктуру серверов и как они атаковали одну и ту же организацию приблизительно в одно время. Достоверная атрибуция GreyEnergy отсутствует, однако найденные факты указывают на то, что группы GreyEnergy и Sofacy связаны, как и предполагали ранее авторы некоторых публикаций.

За более подробной информацией об отчетах по АРТ-угрозам вы можете обратиться по адресу intelreports@kaspersky.com

За более подробной информацией об угрозах, актуальных для АСУ ТП, вы можете обратиться по адресу ics-cert@kaspersky.com

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

[Kaspersky lab ICS CERT](#)

ics-cert@kaspersky.com



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University