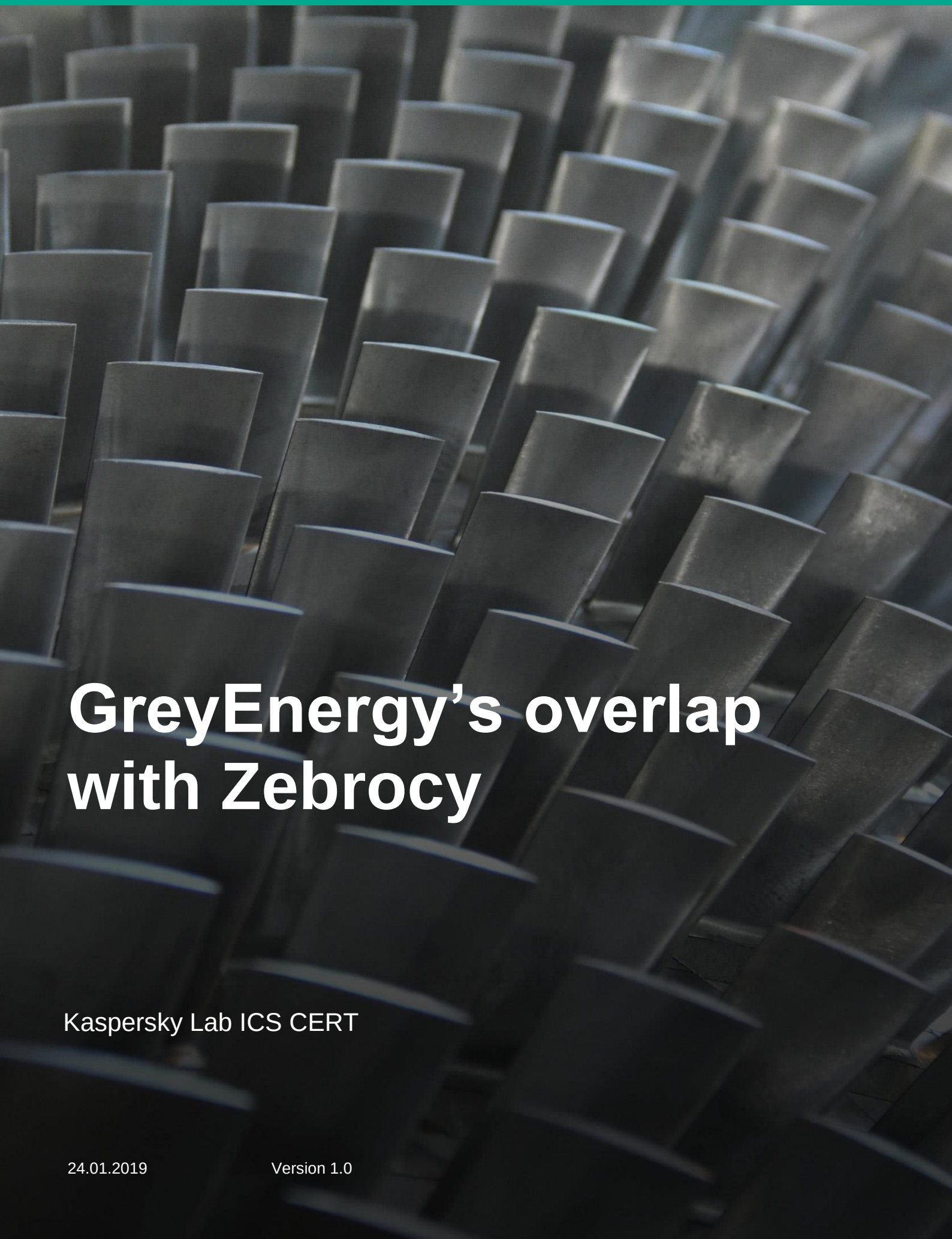


GreyEnergy's overlap with Zebrocy

Kaspersky Lab ICS CERT

24.01.2019 Version 1.0

In October 2018, ESET published a report describing a set of activity they called GreyEnergy, which is believed to be a successor to BlackEnergy group. BlackEnergy (a.k.a. Sandworm) is best known, among other things, for having been involved in attacks against Ukrainian energy facilities in 2015, which led to power outages. Like its predecessor, GreyEnergy malware has been detected attacking industrial and ICS targets, mainly in Ukraine.

Kaspersky Lab ICS CERT has identified an overlap between GreyEnergy and a Sofacy subset called "Zebrocy". The Zebrocy activity was named after malware that Sofacy group began to use since mid-November 2015 for the post-exploitation stage of attacks on its victims. Zebrocy's targets are widely spread across the Middle East, Europe and Asia and the targets' profiles are mostly government-related.

Both sets of activity used the same servers at the same time and targeted the same organization.

Details

Servers

In our private APT Intel report from July 2018 “Zebrocy implements new VBA anti-sandboxing tricks”, details were provided about different Zebrocy C2 servers, including **193.23.181[.]151**.

In the course of our research, the following Zebrocy samples were found to use the same server to download additional components (MD5):

7f20f7fbce9deee893dbce1a1b62827d
170d2721b91482e5cabf3d2fec091151
eae0b8997c82ebd93e999d4ce14dedf5
a5cbf5a131e84cd2c0a11fca5ddaa50a
c9e1b0628ac62e5cb01bf1fa30ac8317

The URL used to download additional data looks as follows:

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

This same C2 server was also used in a spearphishing email attachment sent by GreyEnergy (aka FELIXROOT), as mentioned in a FireEye report. Details on this attachment are as follows:

- The file (11227eca89cc053fb189fac3ebf27497) with the name “Seminar.rtf” exploited CVE-2017-0199
- “Seminar.rtf” downloaded a second stage document from: hxxp://**193.23.181[.]151**/Seminar.rtf (4de5adb865b5198b4f2593ad436fceff, exploiting CVE-2017-11882)
- The original document (Seminar.rtf) was hosted on the same server and downloaded by victims from: hxxp://**193.23.181[.]151**/ministerstvo-energetiki/seminars/2018/06/Seminar.rtf

Another server we detected that was used both by Zebrocy and by GreyEnergy is **185.217.0[.]124**. Similarly, we detected a spearphishing GreyEnergy document (a541295eca38eaa4fde122468d633083, exploiting CVE-2017-11882), also named “Seminar.rtf”.

This document downloads a GreyEnergy sample (78734cd268e5c9ab4184e1bbe21a6eb9) from the following SMB link:

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

"Seminar.rtf", a GreyEnergy decoy document

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

The following Zebrocy samples use this server as C2:

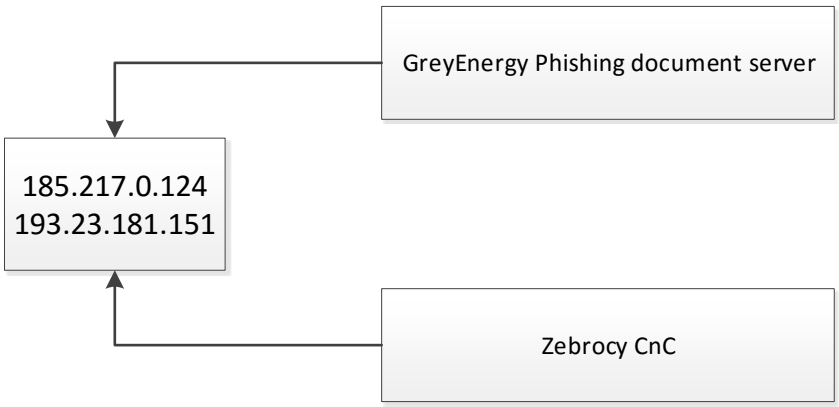
7f20f7fbce9deee893dbce1a1b62827d
170d2721b91482e5cabf3d2fec091151
3803af6700ff4f712cd698cee262d4ac
e3100228f90692a19f88d9acb620960d

They retrieve additional data from the following URL:

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

It is worth noting that at least two samples from the above list use both **193.23.181[.]151** and **185.217.0[.]124** as C2s.

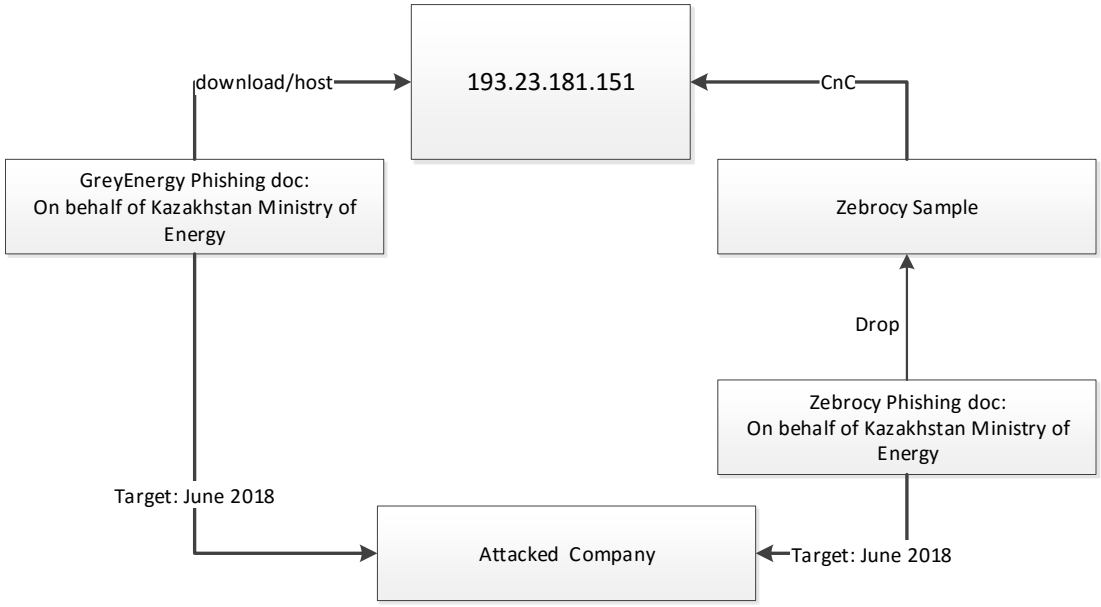
Hosts associated with GreyEnergy and Zebrocy



Attacked company

Additionally, both GreyEnergy and Zebrocy spearphishing documents targeted a number of industrial companies in Kazakhstan. One of them was attacked in June 2018:

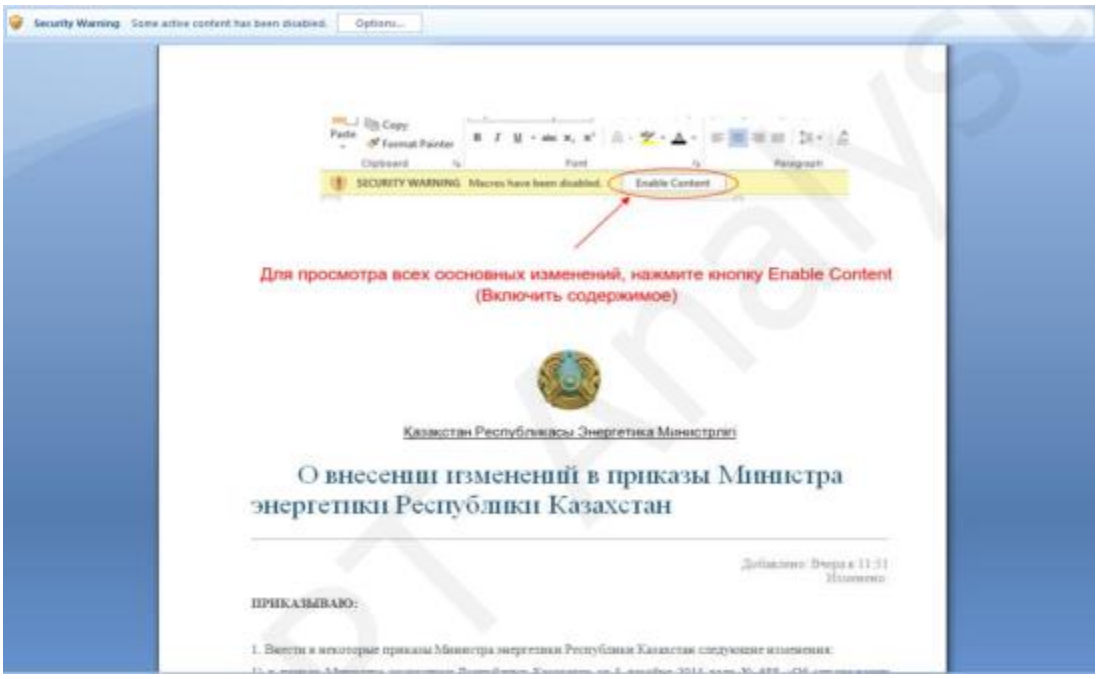
GreyEnergy and Zebrocy overlap



Attack timeframe

A spearphishing document entitled 'Seminar.rtf', which retrieved a GreyEnergy sample, was sent to the company approximately on June 21, 2018, followed by a Zebrocy spearphishing document sent approximately on June 28:

'(28.06.18) Izmeneniya v prikaz PK.doc' Zebrocy decoy document *translation: 'Changes to order, Republic of Kazakhstan'*



The two C2 servers discussed above were actively used by Zebrocy and GreyEnergy almost at the same time:

- 193.23.181[.]151 was used by GreyEnergy and Zebrocy in June 2018
- 185.217.0[.]124 was used by GreyEnergy between May and June 2018 and by Zebrocy in June 2018

Conclusions

The GreyEnergy/BlackEnergy actor is an advanced group that possesses extensive knowledge on penetrating into their victim´s networks and exploiting any vulnerabilities it finds. This actor has demonstrated its ability to update its tools and infrastructure in order to avoid detection, tracking, and attribution.

Though no direct evidence exists on the origins of GreyEnergy, the links between a Sofacy subset known as Zebrocy and GreyEnergy suggest that these groups are related, as has been suggested before by some public analysis. In this paper, we detailed how both groups shared the same C2 server infrastructure during a certain period of time and how they both targeted the same organization almost at the same time, which seems to confirm the relationship's existence.

For more information about APT reports please contact: intelreports@kaspersky.com

For more information about ICS threats please contact: ics-cert@kaspersky.com

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky Lab ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky lab ICS CERT ics-cert@kaspersky.com