GreyEnergy: Updated arsenal of one of the most dangerous threat actors

welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

October 17, 2018

ESET research reveals a successor to the infamous BlackEnergy APT group targeting critical infrastructure, quite possibly in preparation for damaging attacks

Recent ESET research has uncovered details of the successor of the BlackEnergy APT group, whose main toolset was last seen in December 2015 during the first-ever blackout caused by a cyberattack. Around the time of that breakthrough incident, when around 230,000 people were left without electricity, we started detecting another malware framework and named it GreyEnergy. It has since been used to attack energy companies and other high-value targets in Ukraine and Poland for the past three years.

It is important to note that when we describe 'APT groups', we're making connections based on technical indicators such as code similarities, shared C&C infrastructure, malware execution chains, and so on. We're typically not directly involved in the investigation and identification of the individuals writing the malware and/or deploying it, and the interpersonal relations between them. Furthermore, the term 'APT group' is very loosely defined, and often used merely to cluster the abovementioned malware indicators. This is also one of the reasons why we refrain from speculation with regard to attributing attacks to nation states and such.

We have already extensively documented the threat actors' transition towards TeleBots in cyberattacks on high-value targets in the Ukrainian financial sector, the supply-chain attacks against Ukraine and in an analysis of TeleBots' cunning backdoor. All from the group most notable for the NotPetya ransomware outbreak. At the same time, we have also been keeping a close eye on GreyEnergy – a subgroup operating in parallel, but with somewhat different motivations and targeting.

Although ESET telemetry data shows GreyEnergy malware activity over the last three years, this APT group has not been documented until now. This is probably due to the fact that those activities haven't been destructive in nature, unlike the numerous TeleBots ransomware campaigns (not only NotPetya), the BlackEnergy-enabled power grid attack, and the Industroyer-caused blackout – which we have linked to these groups for the first time last week. Instead, the threat actors behind GreyEnergy have tried to stay under the radar, focusing on espionage and reconnaissance, quite possibly in preparation of future cybersabotage attacks or laying the groundwork for an operation run by some other APT group.

GreyEnergy's malware framework bears many similarities to BlackEnergy, as outlined below. It is similarly modular in construction, so its functionality is dependent on the particular combination of modules its operator uploads to each of the targeted victim systems. The modules that we have observed were used for espionage and reconnaissance purposes (i.e. backdoor, file extraction, taking screenshots, keylogging,

password and credential stealing, etc.). We have not observed any modules that specifically target Industrial Control Systems (ICS). We have, however, observed that the GreyEnergy operators have been strategically targeting ICS control workstations running SCADA software and servers, which tend to be mission-critical systems never meant to go offline except for periodic maintenance.

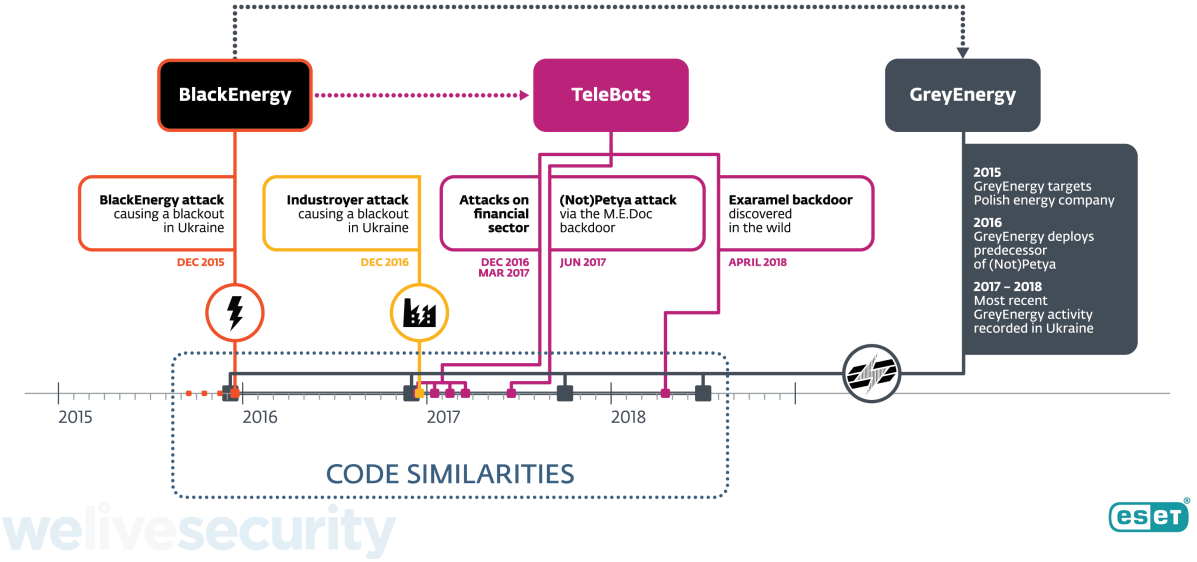
Links to BlackEnergy and TeleBots

Some of the reasons ESET researchers consider BlackEnergy and GreyEnergy related are listed below:

- The appearance of GreyEnergy in the wild coincides with the disappearance of BlackEnergy.
- At least one of the victims targeted by GreyEnergy had been targeted by BlackEnergy in the past. Both subgroups share an interest in the energy sector and critical infrastructure. Both have had victims primarily in Ukraine, with Poland ranking second.
- There are strong architectural similarities between the malware frameworks. Both are modular, and both employ a “mini”, or light, backdoor deployed before admin rights are obtained and the full version is deployed.
- All remote C&C servers used by the GreyEnergy malware were active Tor relays. This has also been the case with BlackEnergy and Industroyer. We hypothesize that this is an operational security technique used by the group so that the operators can connect to these servers in a covert manner.

Compared to BlackEnergy, GreyEnergy is a more modern toolkit with an even greater focus on stealth. One basic stealth technique – employed by both families – is to push only selected modules to selected targets, and only when needed. On top of that, some GreyEnergy modules are partially encrypted using AES-256 and some remain fileless – running only in memory – with the intention of hindering analysis and detection. To cover their tracks, typically, GreyEnergy’s operators securely wipe the malware components from the victims’ hard drives.

In addition to the outlined similarities with BlackEnergy, we have observed another link between GreyEnergy and the TeleBots subgroup. In December 2016, we noticed an instance of GreyEnergy deploying an early version of the TeleBots’ NotPetya worm – half a year before it was altered, improved, and deployed in the most damaging ransomware outbreak in history. There is significant code reuse between this ransomware component and the GreyEnergy core module. We call this early version “Moonraker Petya”, based on the malware writers’ choice of filename – most likely a reference to the James Bond movie. It didn’t feature the infamous EternalBlue spreading mechanism, as it had not been leaked at that time.



GreyEnergy Tactics, Techniques and Procedures

We have observed two distinct infection vectors: “traditional” spearphishing, and the compromise of public-facing web servers. When such a vulnerable web server was hosted internally and connected to the rest of a targeted organization’s network, the attacker would attempt to move laterally to other workstations. This technique is used not only as a primary infection vector but also as a backup reinfection vector.

The attackers typically deploy internal C&C proxies within the victims’ networks. Such proxy C&Cs redirect requests from infected nodes inside the network to an external C&C server on the internet. This is another stealth tactic, as it is less suspicious to a defender to see that multiple computers are “talking” to an internal server, rather than a remote one.

A very curious observation – one that is also indicative of the group’s targeting – is that some of the GreyEnergy samples we detected were signed with a certificate from Advantech, a Taiwanese manufacturer of industrial and IoT hardware. These were most likely stolen from the company, just as in the case of Stuxnet and a recent Plead malware campaign.

The GreyEnergy operators also employ common external tools in their arsenal, such as Mimikatz, PsExec, WinExe, Nmap, and a custom port scanner.

For a detailed analysis of the GreyEnergy toolset and operations refer to our white paper GreyEnergy: A successor to BlackEnergy. A full list of Indicators of Compromise (IoCs) and samples can be found on GitHub. For any inquiries, or to make sample submissions related to the subject, please contact us at: threatintel@eset.com.

For more information about how to protect yourself you can visit our website and find out more about GreyEnergy.

Anton Cherepanov and Robert Lipovsky 17 Oct 2018 - 11:55AM