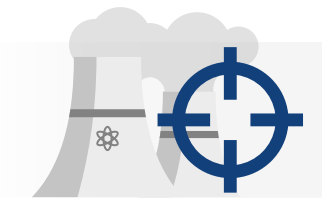
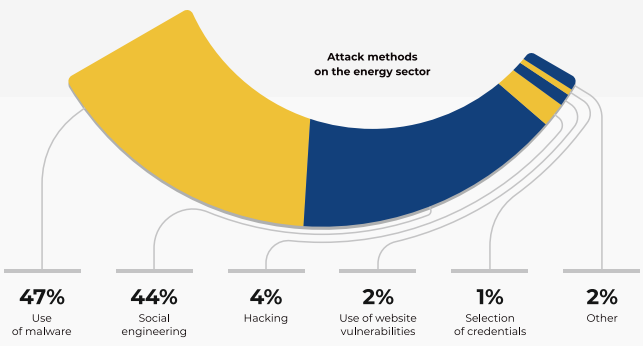
ENERGY SECTOR – NETWORK SECURITY

ROOT LEVEL RESOURCES

Energy companies are part of critical government infrastructure which makes them highly attractive targets for government-backed attack groups. Usually, their objective is to ensure long-term presence in the networks of critical infrastructure objects for the purposes of espionage and sabotage. However, some attacks are carried out with the goal of shutting down critical infrastructure objects. Therefore, energy sector security is one of the most critical components of a country's national security.



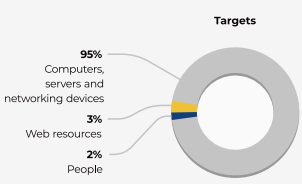
The key challenges to cyber security in the energy sector:

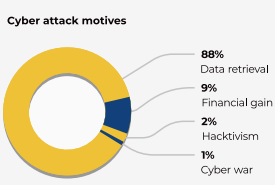


Generally, the attackers try to penetrate the system by compromising IT networks using traditional malware and techniques, including livind off the land" . Access to the system is necessary to spy and gather information on how to best attack a specific energy company for the purpose of sabotage.

So far, experts have been able to identify two frameworks that can influence technological processes: Industroyer and Triton (Trisis). Both frameworks were discovered as a result of an error made by their operators. Cyber security experts have traced both frameworks to Russia.

A significant number of security threats remain undetected - a ticking time bomb.





Following a successful penetration of an IT network segment, the next step is to compromise OT networks. It is only possible to detect a compromise of the OT-network in two cases: if the attack was carried out with the objective of sabotage or if the malware operator made a mistake. Therefore, most of the time, attackers hide as long as possible until the moment when a mass attack can be conducted.

Experts suggest that "supply chain" attacks by software and hardware suppliers pose a major threat to the energy sector. Firstly, attackers target company management. They then launch attacks on the networks of energy companies.

Government-sponsored groups pose a threat to the sector

ROOT LEVEL RESOURCES

Over the past few years, experts have published a large number of studies on government-sponsored groups. Nevertheless, this area remains under-researched.

Moreover, while well-known government-backed groups mainly originate from developing countries, the greatest threat is presented by groups from developed countries. The latter have access to higher-quality equipment and tools to conduct their attacks. So their activities are less detectable and stay under-researched.

Name/ Period	Geography of attacks	Penetration vector	Instruments
HEXANE (also known as LYCEUM) *June 2018 – now*	Middle East and Africa; Russia and the CIS	Hackers target industrial control systems and attack oil and gas and energy companies in the Middle East (mainly in Kuwait). Criminals circumvent protection systems through trusted suppliers by compromising devices, software, and telecommunications networks used by targets.	DanBot, Posh C2, PowerShell Empire
LEAFMINER (Iran) *January 2018 – July 2018*	Middle East and Africa	Watering hole attacks: hackers insert malware into links of com promised websites to open an SMB connection and steal user credentials.	Inception Framework, Trojan.Imecab, Backdoor.Sorgu (Symantec)
XENOTIME (Russia) *December 2018 – now*	USA; Asian-Pacific area	Attacks on Triconex Safety Instrumented System (SIS) controllers manufactured by Schneider Electric. In addition, they launch attacks on a number of emergency protection systems.[2]	Triton (Trisis)
LAZARUS (North Korea) *April 2017 – now*	USA; Europe; Asian-Pacific area; Middle East and Africa; Russia and the CIS	Attacks on the accounts of executives of energy companies.	Ratankba, PowerRatankba, ClientRAT, ClientTraficForwarder (Proxy), AppleJeus, PowerTask, PowershellRAT, Banswift/BBSwift, RatankbaPOS, Mimikatz, Metasploit, Dtrack, Rising Sun
BLACKENERGY (one of the most "savvy" groups attacking the energy sector) *May 2014 – July 2018*	USA; Europe; Asian-Pacific area; Middle East and Africa; Russia and the CIS	Attacks on ICS/SCADA systems.	Industroyer (Crashoverride), allows to remotely control remote terminal units (RTU), responsible for physical make-and-break of BadRabbit, VPNFilter, which contains a module for detecting Scada-systems (for attacking routers)
DRAGONFLY (aka Energetic Bear and Crouching Yeti) (Russia) *February 2013 – August 2018*	USA; Europe; Asian-Pacific area	Data collection from energy and industrial facilities. Attacks are launched by sending phishing emails to employees, as well as watering hole attacks for mass theft of corporate data.	Goodor, DorShel, Karagany
APT33 (aka Elfin, Magnallium) (Iran) *June 2016 – December 2018*	USA; Europe; Middle East and Africa	Overwriting MBR, partitions, and files in a randomly generated data system	Shamoon

Energy companies continuously improve their cybersecurity systems. This is, in part, a response to improvements in malicious programmes, which usually target industrial control systems and are created to jeopardise power grids, as well as, in part, a response to stronger requirements being imposed by the State when it comes to the security of critical infrastructure.

Government institutions finance the activities of such groups, develop detailed plans that cover strategic and operational levels, and, of course, ensure ongoing control and monitoring of plan implementation. Such careful preparation makes it exceedingly difficult to identify the attacks and the attackers. What is more, the prospect of holding such persons accountable for their crimes remains illusory.

Therefore, it is up to the network security providers and developers of technologies to prevent new security gaps from emerging in the future and to effectively combat existing ones. For instance, it is possible to make improvements to router security, which would, in turn, reduce the likelihood of malicious acts being committed in the energy sector.

1 – The use of legitimate local applications for malicious purposes to install Trojans

2 – Special protective equipment that connects to the management of production processes in cases of a threat

Sources:

ROOT LEVEL RESOURCES

1 Secureworks reports // URL: https://www.secureworks.com/

2 Dark Reading reports // URL: https://www.darkreading.com

3 The PCI Security Standards Council reports // URL: https://www.pcisecuritystandards.org

4 Dragos reports // URL: https://dragos.com/

5 Group-IB reports // URL: https://www.group-ib.ru/

6 Positive Technologies reports // URL: https://www.ptsecurity.com/ru-ru/