Top 5 most dangerous industrial cyberattacks

By Khobeib Benboubaker
– August 19, 2019

In addition to the financial losses they cause, industrial cyberattacks are feared due to the threat they pose for the environment, human lives, as well as the sovereignty of the country affected. We review five — or almost five — of the most dangerous threats that industry has faced up to now.

Top 5 des cyberattaques les plus dangereuses pour les industries

Au-delà des pertes financières qu'elles engendrent, les cyberattaques industrielles sont redoutées car elles présentent un risque pour l'environnement, les vies humaines voir la souveraineté du pays impacté. Retour sur les cinq menaces les plus dangereuses qu'ait connues l'industrie à ce jour – ou presque.

5 SHAMOON

NEARLY CAUSES A POLLUTION EVENT

Though it didn't get very far into the industrial system, this malware paralysed Aramco, the Saudi Arabian national hydrocarbon company, for more than 15 days in 2012. With nearly 35,000 computers rendered unusable, the company found itself disconnected from the world. It lost control of its supervision consoles and production process, which could have led to a large-scale explosion and pollution event. In 2018, the Italian petrol company Saipem was also reportedly impacted by an attack linked to Shamoon.

LA POLLUTION EN RÉPERCUSSION

Sans aller très loin dans le système industriel, ce logiciel malveillant a paralysé Aramco, la société nationale saoudienne d'hydrocarbures, pendant plus de 15 jours en 2012. Avec près de 35 000 ordinateurs inutilisables, l'entreprise se retrouve déconnectée du monde. Elle perd le contrôle de ses consoles de supervision et de son processus de production, faisant courir un risque de pollution et d'explosion à grande échelle. En 2018, le pétrolier italien Saipem aurait à son tour été impacté par une attaque basée sur Shamoon.

4 INDUSTROYER

SHORT CIRCUITS POWER GRIDS

Since 2015, multiple attacks by multiple versions of the malware Industroyer have come on the scene, affecting at least one country, Ukraine. Its speciality? Attacking electrical generation systems. Industroyer gives the attacker complete control of the targeted system, without the victim's knowledge. The possibilities for malfeasance are almost endless: cutting power to a district, city or region; changing the frequency of a power grid; overloading a plant grid; or even interfering with the global power network.

FAIT DISJONCTER LES RÉSEAUX ÉLECTRIQUES

Depuis 2015, plusieurs versions et attaques du malware Industroyer se sont succédées et ont notamment frappé un pays comme l'Ukraine. Sa particularité ? S'attaquer aux systèmes de production d'électricité. Coupures de courant, changement de fréquence du réseau électrique, Industroyer donne à l'assaillant le contrôle total du système attaqué et ce, sans connaissance particulière préalable. À la clé, des possibilités presque infinies : couper le courant d'un quartier, d'une ville ou d'une région, surcharger le réseau d'une usine ou bien encore interférer avec le réseau électrique mondial…

3 TRITON

A MALWARE WITH ENVIRONMENTAL CONSEQUENCES

First detected in 2017, when it was targeting the Saudi Arabian petrol company Petro Rabigh, this malware could have caused enormous harm, including marine pollution, a spike in petrol prices, and even deaths due to explosion. Its MO? Reprogramming the controllers of the Triconex Safety Instrumented System (SIS). According to the latest reports on this cyberattack, Triton went unnoticed for three years before being detected. An unsettling piece of news, now that the malware seems to have resurfaced in April 2019.

UN MALWARE AUX CONSÉQUENCES ENVIRONNEMENTALES

Détecté en 2017 alors qu'il visait la société pétrolière Petro Rabigh, en Arabie saoudite, ce logiciel malveillant aurait pu provoquer d'énormes dégâts : morts en cas d'explosion, pollution maritime, ou encore flambée du prix du baril... Son mode opératoire ? Reprogrammer les contrôleurs du système instrumenté de sécurité (SIS) Triconex. Selon les derniers rapports sur cette cyberattaque, Triton serait passé inaperçu pendant trois ans avant d'être détecté. Une donnée inquiétante, alors que le malware semble avoir refait surface au cours du mois d'avril 2019.

2 STUXNET

RAISES THE SPECTRE OF NUCLEAR FALLOUT

As described in the documentary "Zero Days", Stuxnet is a 2010 cyberattack that targeted centrifuges at the Natanz uranium enrichment site in Iran. Its goal? To halt or slow down production. A warning sign that raises the spectre of an even larger attack, this time with nuclear consequences.

LAISSE PLANER LA MENACE DE RADIOACTIVITÉ

Décrite dans le documentaire « Zero Days », la cyberattaque Stuxnet de 2010 s'en prend aux centrifugeuses du site d'enrichissement d'uranium de Natanz en Iran. L'objectif ? Ralentir voire stopper la production. Un avertissement qui laisse planer la menace d'une attaque de plus grande ampleur dont les conséquences seraient radioactives.

1 ?

AN AS-YET UNIDENTIFIED ATTACK

The fifth most dangerous industrial cyberattack could already be happening right now, without anyone's knowledge. As we saw with Triton and Stuxnet, several years may go by between a malware's first move and its subsequent detection. That's why cybersecurity remains one of the biggest challenges for industry in 2019.

UNE ATTAQUE ENCORE NON IDENTIFIÉE

La cinquième cyberattaque industrielle la plus dangereuse pourrait bien être déjà en cours, sans pour autant avoir été identifiée. Comme dans les exemples de Triton et Stuxnet, plusieurs années s'écoulent parfois entre le premier mouvement du malware et sa découverte. C'est pourquoi la cybersécurité reste un des principaux défis à relever pour l'industrie en 2019.