Stuxnet Virus Cyberattacks on Iran's Nuclear Power Program

Posted on September 11, 2018

The failure of such a large number of centrifuges made us think – is not this the result of some kind of diversion planned with the help of the newly developed computer virus Stuxnet – which in Iran has become quite widespread in comparison with other states, which can serve as proof that the developers of the virus were tagged in Iran. And, as it turns out, directly to the uranium enrichment plant, using the known vulnerabilities of its operating system and the notorious "human factor."

However, the customer is unknown; the hypothetical executor is supposedly the employee of Siemens Concern (Siemens) who inserted the infected flash drive into the production control system. The damage caused to Iran's nuclear program, in this case, is comparable to the damage from the notorious strike of the Israeli Air Force in 1981, just before the launch of the nuclear power plant, when the entire infrastructure of the enterprise was completely destroyed.

As the results of the investigation show, it is precisely cybernetic attacks that can just become an ideal tool for such large-scale damage to equipment – they are swift, highly effective in their destructiveness, and, at the same time, absolutely anonymous.

It should be noted that the Stuxnet virus attacks at the level of logical controllers (controllers – computers that manage large industrial and power complexes), infecting the software basis of the system. In the list of its purposes – converters frequency-controlled drives (VFD). Among the activated frequencies in the body of the virus, there are also those that can affect the electronic equipment of Iranian IR-1 centrifuges. However, these circumstances in itself do not mean anything.

What actually sought the developers of the virus is unknown. If they set themselves the task of physically destroying centrifuges, then their plan did not work because the Stuxnet virus did not provide this. But if they intended to damage these or other nodes of centrifuges or disable them for a long time, then, perhaps, they even succeeded since the damage caused by the virus was sudden and very noticeable. It should be noted that when the staff realized that something was going wrong with the work of the centrifuges and cut off the supply of electricity to them, it was too late, and the situation in the shop resembled the consequences of a terrorist act involving the use of multiple explosive devices at the same time.

Officially, Iran did not recognize that the plant was under the impact of a computer virus. However, at the highest level, it is confirmed that cyber attacks on its nuclear facilities are underway. Thus, at the end of November 2010, President Mahmoud Ahmadinejad stated that a "limited number of centrifuges" had problems with software in electronics.

At the same time, the head of the Atomic Energy Organization of Iran, Dr. Ali Akbar Salehi, designated the date when the Stuxnet virus appeared in Iranian nuclear facilities – this is the middle of 2009. Consequently, the time it takes for a malicious virus to pass from the first infected personal computers to the factory shops is more than one year.

At the same time in 2009-2010. Iranian specialists dismantled and replaced about 1,000 IR-1 centrifuges at the plant. Before that, this rather outdated model of centrifuges often went out of order (about 10% per year), but the replacement of such a large batch, as in 2010, made you think to start an investigation and a deep scientific study of this issue.

Of course, the uranium enrichment plant is a closed enterprise with limited access, a high level of secrecy of the control and monitoring system, and is not connected to the Internet. According to experts, the virus could reach the control computers only through the personal computers of the plant's specialists – first by infecting their home computers or through computers of people who are somehow connected with the plant, and then by means of their flash drives, the virus could get on the computers of control systems.

Editorials of the world press have filled gloomy prophecies about the advent of the era of cybernetic wars. A clue to the mystery of the Stuxnet virus, which hit the uranium enrichment plant in Iran, is being punctuated by experts from a wide range of disciplines: from IT security to linguistics and anthropology. It should be noted that the Stuxnet virus was detected by antivirus laboratories for a long time. However, the world learned about the true extent of infection only at the end of September 2010.

For quite understandable and logical reasons, the developers of the Stuxnet virus prefer to stay in the shadows. However, specialists emphasize the fact that it is quite obvious that the complexity of this virus can be called unprecedented, and the creation of such a project requires huge intellectual and financial investments, which means that only structures of state scale can be implemented. Experts agree that this virus is not the fruit of an effort; it is simply "a group of enthusiasts." Laurent Esso, head of security systems at Symantec, suggests that at least ten people worked on the Stuxnet virus for six to nine months. Frank Rieger, technical director of GSMK, supports his colleague: according to him, the virus was created by a team of experienced programmers, and the development took about six months. Rieger also calls the estimated cost of creating the Stuxnet virus at least $ 3 million. Evilty Kaspersky, the general manager of Kaspersky Lab, says about the virus's sabotage mission: "Stuxnet does not steal money, does not send spam, and does not steal confidential information. This malware is created to control production processes and literally manage huge production capacities. In the recent past, we have fought against cyber-criminals and Internet hooligans; now, I'm afraid, it's time for cyberterrorism, cyber-weapons, and cyberwar. " Tilman Werner, a member of the Commonwealth of experts in the field of Internet security, I am sure: single hackers are not capable of such.

"Stuxnet is so sophisticated from a technical point of view that one should proceed from the fact that

experts from government agencies took part in the development of a malicious program or that they at least provided some meaningful assistance in its creation, ” says Werner.

Specialists note that the Stuxnet virus penetrates into the computer through the USB socket from the infected media, usually disk-on-key, popularly known as a flash drive. From this point on, the infected computer becomes the source of the infection itself.

The “worm” inside it (the Stuxnet virus is marked by six different ways of penetration and fixing in the operating system of the computer) starts to operate in an autonomous mode. No command from the outside is no longer needed. He knows by birth how to do it. The Stuxnet virus tests the contents of the computer, incoming and outgoing commands and behaves perfectly normal to the system that has absorbed it, does not harm either itself or its partners until it stumbles upon the signs of the target for which it was created – program management production of the concern “Siemens”. And then he turns into a cruel predator-destroyer.

The specialization of the Stuxnet virus is the computer programs of large-scale industrial control systems SCADA (Supervisory Control and Data Acquisition), i.e., “dispatch control and data collection”. These systems regulate the technological processes of power plants, oil and gas pipelines, military plants, civil infrastructure enterprises, and so on.

The Stuxnet virus, possessing the necessary initial capabilities of the system administrator and knowing the vulnerabilities of the operating system that he does not know, except him and his creators, no one, raises himself in the current administrative hierarchy to the level of command initiation, actually seizes power in the system and redirects it to the execution of his own destructive purpose.

First of all, it changes the computer to the “head” and reprograms the PLC program (Programmable Logic Controler), which is responsible for the logic. And he begins to give commands himself.

According to Ralph Langner, an expert in industrial safety at Siemens concern, the Stuxnet virus can change the parameters of the “operational block 35”, which monitors critical production situations that require an urgent reaction of 100 milliseconds. If so, the brutalized “worm” does not cost anything to bring the system to a devastating accident.

Having taken control of itself, the Stuxnet virus consistently leads the system to the destruction of production. He is not a spy, as many at first thought, he is a saboteur. As soon as the source code of the PLC stops executing, says Ralph Langner, we can expect that soon some link will explode, it will collapse. And, most likely, it will be something important.

Experts agree that the development and implementation of such a complex virus is a task beyond the power of either the hacker, the hacker group, or any private structure. This is clearly the work of the state. Only the state could afford to run such an expensive “worm”, thereby actually declassifying it, only for the sake of an extremely important goal for it and only because it could not wait any longer.

In this regard, the same Ralph Langner expresses a logical assumption that the Stuxnet virus has probably done its work. Nevertheless, the “worm”, although clearly not a spyware program, provides some information, including for the general public, even if it is the very fact of its existence.

Problems Of The Siemens Concern

A well-known fact is that the Bushehr NPP was built by Russian Atomstroyexport specialists in Russian technologies and using computer production management systems of the Siemens concern.

It should be noted that, according to experts, the Stuxnet virus affects only a specific type of Siemens controller, SIMATIC S7, which, according to the IAEA (International Atomic Energy Agency), is used by Iran. At the same time, about 60% of computers infected with the Stuxnet virus are in Iran, and the remaining 40% are in the countries associated with it: Indonesia, India, and Pakistan.

An important detail of the issue under consideration is that it was the Siemens concern that took an active part in the 1970s. The last century in providing high-tech equipment for Iran’s nuclear program. After the victory of the Islamic revolution, the concern stopped working in the country, but then the Germans returned, and Iran became one of the largest customers of specific equipment for them. However, after the introduction of international sanctions, with great reluctance and under severe pressure from the German government, Siemens Concern announced the termination of contracts with Iran. This fact is still referred to by representatives of the concern in response to the continually arising reproaches. However, soon, they were caught on supplies of banned equipment and dual-use components, which can be used for installation at Iran’s nuclear facilities, as will be discussed below.

Software Support Version

Like the world’s nuclear power plants, the uranium enrichment plant is closed and has large restrictions, including those related to the access of outsiders to its territory. However, some ideas about the specifics of the production process by the organizers of the sabotage were: For example, in 2007-2008, the plant was visited by IAEA inspectors, but the Iranian authorities did not close the doors before them. Experts learned a lot of interesting information, even from the official Iranian television and photography, dedicated to the visit to the plant of President Mahmoud Ahmadinejad in 2008. The security services then worked surprisingly unprofessionally. So, in the photo, you could see the monitors of computers running under the Windows operating system; it became known exactly what centrifuges are used in Natanz (Iran bought centrifuges in Pakistan, bypassing the embargo on deliveries of prohibited equipment), and computer control of centrifugal motors is carried out with the help of controllers of the Siemens concern. Owning this information, it was only necessary to decide how to safely put the malicious program into the enterprise’s computer network because, for safety reasons, it is not connected to the Internet. And the authors of the Stuxnet virus have developed a cunning solution:

As for the needs of a particular product for Siemens controllers, special software (the management system itself) is always created, and the management programs are “written” on them under the order; therefore, the developers subsequently engage in their planned support and regularly deliver the update files for production. The most possible way to deliver information to a closed plant network is through external media. Hackers “threw” the Stuxnet virus into six Iranian companies – software developers, who, in their opinion, could have contact with the plant in Natanz. Infecting the computers of these companies was a matter of technology because they are connected to the Internet, and their employees use e-mail. As was to be expected, the calculation that sooner or later, the virus would fall to its intended purpose was fully justified: the infected computers that control the production, at some point, commanded the spinning of centrifuges until some of them failed. Only then did the plant’s maintenance personnel notice something wrong and de-energize them.

Israeli Footprint

Iran turned into an object of increased international attention when Western countries began taking every possible step to disrupt its nuclear programs aimed, in their opinion, at the creation of their nuclear weapons. Under these conditions, work is underway to break up his economy while simultaneously attacking the military-industrial and scientific sectors. Such a conclusion is contained in the book published in the European Union by intelligence specialist Ivonnik Denoel, “The Secret Wars of the Mossad.” This edition is the first to describe in detail the operation to disrupt the operation of centrifuges for enriching uranium using a computer virus.

The first information about the underground uranium enrichment plant in Natanz was obtained by Western special services in 2002 when German intelligence agents recruited an Iranian businessman whose company took part in the creation of this facility. Proceeding from the author’s words, the Iranian agreed to provide maps, photographs, technical descriptions, and other information about this object in exchange for a promise to take him out of the country later and grant him German citizenship. However, Denoel, the Iranian counterintelligence, exposed this agent in 2004 and liquidated it. Nevertheless, his wife was able to remove from Iran to Germany the laptop computer of her deceased husband.

The book’s author notes that “the computer became a genuine cave of Ali Baba, and German intelligence took months to study the documents that came into her hands. “

Following this, in 2006, a “suspicious” series of explosions followed the plant in Natanz and the Isfahan nuclear center, when transformers were withdrawn during the launch of gas centrifuges, at which enrichment of uranium takes place. As a result, up to 50 centrifuges were damaged in Natanz.

Meanwhile, in 2009, a joint US team of experts was monitored at Israel’s Dimona nuclear facility in the Negev desert to monitor the Israeli nuclear program. At the same time, the Israeli special services created an accurate working copy of the Iranian enrichment plant in Natanz on the basis of

intelligence documents received. These works were facilitated by the fact that both “Dimona” and in Natanz used French nuclear technology. Daniel writes that the Israeli special services managed to acquire centrifuges on the world’s “black market,” similar to those used by Iran to enrich uranium.

As a result, according to independent experts, Israel’s creation of a “mirror Natanz” with its production cycle allows it in real-time to monitor the progress in the key area of the Iranian nuclear program – works on enriching uranium. According to the author, it was the centrifuges of the Natanz plant that became the object of an attack by Western intelligence agencies using computer networks for this purpose.

According to Denoel, in 2008, the German machine-building concern Siemens, which was carrying out transactions with Iran, “agreed to cooperate with the US Department of Homeland Security in order to help its specialists find vulnerabilities in the computer system of the armed forces of Iran.” This was facilitated by the fact that Siemens participated in the creation of computers that manage large production and energy complexes (controllers). As it turned out, the computer equipment of the German company was used by the Iranians and at the plant in Natanz.

Simultaneously, the special services of Israel and the United States organized a group to create the computer virus Stuxnet, which began work in Dimona. In this connection, the New York Times wrote that without the reconstruction of the production process of the Iranian plant in Natanz at the Israeli nuclear center, the Stuxnet virus could not have worked with high efficiency. At the same time, Israel attracted the work of retired scientists and technicians who worked in the nuclear sector in the 1950s and 1960s. – so specific, and, moreover, the production process in Natanz was rather out of date. However, it was these veteran specialists who had the necessary knowledge to reconstruct the technological processes of the Iranian nuclear program.

The operation on industrial sabotage in Iran had several levels. So, in June 2009, US and Israeli specialists created and launched a simplified version of the Stuxnet virus on the Internet, the source of origin of which could not be determined. Initially, this virus allowed the theft of information stored in computers, such as identification numbers, passwords, and codewords, as well as information about the configuration of networks.

A few weeks after the first appearance of the Stuxnet virus on the World Wide Web, its complex version was launched, aimed at attacking Iranian production facilities. It was she who was sent by specialists from the USA and Israel to the plant network in Natanz, where he took control of the centrifuge control system. According to Denoel, the virus forced control programs to report “normal operation,” penetrating at the same time deeper into production systems.

The book’s author notes that “in this way, a virtual reality was created in the computer system of Natanz, which did not allow Iranian specialists to suspect the fact of a virus attack. “

Everything indicates that in 2010 an order was issued to initiate the attack, and the virus, taking control of the centrifuges’ control, forced them to increase the rotor rotation speed from 1,000 rpm to

1,400. When this speed is reached, a breakdown occurs and the output is out of the action of the centrifuge.

IAEA inspectors immediately reported that there were some events at the plant in Natanz. Usually, at this enterprise, where 8,700 centrifuges were deployed, the number of failed ones did not exceed 10% per year. However, within three months of 2010, Iranian technicians replaced up to 2,000 centrifuges, IAEA representatives said. According to Western analysts, the technological attack allowed to drop back 24 months of progress in works on uranium enrichment. Thus, according to the former Mossad leader Meir Dagan, "a successful operation delayed the beginning of Iran's production of enriched weapons-grade uranium for several years."

Nevertheless, according to Denoel, this operation could not stop Iran's nuclear power program. Damaged centrifuges have been replaced, and according to Western intelligence services, Tehran has up to 8,000 reserve centrifuges.

Investigation Materials

According to statistics collected prior to the events of 2010, the spare centrifuges available for Tehran are a rather outdated model (IR-1), and they also often fail. So, back in 2009-2010 years. Iranian specialists dismantled and replaced about 1,000 IR-1 centrifuges at the uranium enrichment plant.

Published IAEA data confirm that in early 2010, something strange happened at the plant. In the workshop (technological module A26), 11 out of 18 cascade centrifuges were switched off, and only 1,804 machines were switched off. In other shops, the situation looked better, although there were recorded trips of one or two cascades.

The A26 module was installed in 2008. This is the second module assembled at the plant. As of June 2009, 12 out of 18 cascades of this module enriched uranium. In August 2009, 10 cascades were involved in enrichment, and in November, only six.

Such a reduction in the number of uranium enrichment cascades confirms that the A26 module is experiencing significant problems. And in the period between November 2009 and the end of January 2010 (more precisely not), something happened that required the shutdown of 11 cascades at once.

At the same time, it should be noted that the mere failure of IR-1 centrifuges is not an out-of-the-way event. IR-1 centrifuges break down and do this often. According to unofficial estimates of the IAEA experts, in a year at this plant, up to 10% of the total number of centrifuges installed, that is, 800-900 cars per year, fails.

It is possible that the centrifuges of module A26 were rejected for "natural" reasons, although the number of out-of-order machines is large enough and exceeds the annual rate of failure.

Another explanation, excluding any external sabotage, is the quality of the installation of the

centrifugal assemblies in module A26, which may be low and could make itself felt. Thus, it is known that the centrifuges of the first Iranian module (A24) operate steadily. However, in the second module (A26), the quality of work for the installation of centrifuge assemblies conducted after the introduction of the international ban (for the delivery of the relevant specific equipment) could be lower than that of the first one. This explanation does not contradict the realities. It is not clear, however, why the factory marriage was affected a year or more after the launch of the second module.

There is also a third version. So, the first module (A24) could be manufactured from officially purchased imported components and the second (A26) – from unknown parts that were imported to Iran. In this case, the mass yield of centrifuges of the second module should not cause any special surprise.

At the same time, it should be noted that experts from Symantec determined that the Stuxnet virus, among other things, attacks frequency converters that were manufactured by the Iranian company Fararo Paya and the Finnish Vacon. Corresponding sequences of commands in the body of the virus experts were designated as “A” and “B.” Frequency converters in centrifuges are needed for the motor control system, which allows specifying with high accuracy the rotational speeds of centrifuge rotors.

The converters to which the Stuxnet virus targeted are of limited scope, including those intended for centrifugal installations. Many specialists, after the message from Symantec, “believed that the virus was developed to combat Iran’s nuclear program.

References

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015). Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In *2015 IEEE International Conference on Intelligence and Security Informatics: Securing the World through an Alignment of Technology, Intelligence, Humans and Organizations, ISI 2015* (pp. 85–90). https://doi.org/10.1109/ISI.2015.7165944

Himanen, P. (2001). The Hacker Ethic and the Spirit of the Information Age. *Max Weber Studies*. https://doi.org/loc?

Audette, C. (2015). EEG Hacker: Brain-Controlled Shark Attack! Retrieved from https://eeghacker.blogspot.hk/2015/03/brain-controlled-shark-attack.html

Stoll, C. (1988). STALKING THE WILY HACKER. *Communications of the ACM*, *31*(5), 484–497. https://doi.org/10.1145/42411.42412

Karpati, P., Opdahl, A. L., & Sindre, G. (2011). HARM: Hacker Attack Representation Method. In *Communications in Computer and Information Science* (Vol. 170, pp. 156–175). https://doi.org/10.1007/978-3-642-29578-2

Mirovalev, M., & Freeman, C. (2014). Russian hacker wanted by US hailed as hero at home. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/worldnews/europe/russia/10883333/Russian-hacker-wanted-by-US-hailed-as-hero-at-home.html