Institute for Science and International Security

ISIS REPORT

February 26, 2013

Basic Attack Strategy of Stuxnet 0.5

By the Institute for Science and International Security (ISIS)

Symantec has recently established that an earlier attack strategy of the malware Stuxnet involved the secret closing of a set of valves in six of 18 cascades in a module at the Natanz Fuel Enrichment Plant (FEP). [1] This attack strategy was apparently active by late 2007, when Iran was setting up and operating its first module of about 2,952 IR-1 centrifuges. The reason for attacking only one third of a module's cascades is unclear. But this attack could have damaged many centrifuges without destroying so many that the plant operator would have become suspicious. The code takes over the monitoring system, keeping the operator unaware of the attack.

The attack involves singling out a set of centrifuges in the cascade. Figure 1 lists the Natanz cascade of 164 IR-1 centrifuges organized into 15 stages and the 110 centrifuges that are isolated during the attack. None of the affected centrifuges are in the feed stage, which is stage 10 in the table and includes 24 centrifuges. In total, 54 centrifuges are not affected. By themselves, these 54 centrifuges form a cascade of 11 stages, the stages of which are all very narrow except for a very wide feed stage.

Based on an analysis of the code and the Natanz cascade, the most likely valves closed are the three fast acting valves on the three thin pipes for feed, product, and waste (or tails) that pass through the top cap of an IR-1 centrifuge (see figure 2). The three fast-acting electronically-controlled valves are part of an emergency response system of the cascade aimed at protecting the remaining centrifuges in the cascade from the effects of a crashing centrifuge. If a centrifuge crashes, or there is an imminent risk of one crashing, the computer monitoring system closes the valves of the affected centrifuge rapidly, effectively isolating it. The kinetic energy of a rotating centrifuge is huge. Because this energy is converted mainly into heat, a crashing centrifuge produces a large pulse of hot uranium hexafluoride gas and other gases that must be contained. Otherwise, this pulse travels down the cascade, taking out additional centrifuges in its path. Thus, the emergency system is designed to act within milliseconds in the event of an anticipated crash and isolate the centrifuge from the cascade. The Natanz cascade emergency response system appears to rely principally on a vibration sensor, an accelerometer, on each centrifuge. Many pressure transducers are also in each cascade to measure pressure, but the most important sensor to detect crashing appears to be the accelerometer. This sensor sends a shut-off signal to the computer monitoring system if the vibration level exceeds a certain, dangerous value.

[1] This report should be read in conjunction with Symantec's report, *Stuxnet 0.5: The Missing Link*, version 1: February 26, 2013 by Geoff McDonald, Liam O. Murchu, Stephen Doherty, and Eric Chien.

This earlier version of Stuxnet appears to exploit this emergency response system. The attack closes 330 fast-acting valves of 110 centrifuges in the cascade while leaving the valves on the other 54 open.[2] As Symantec has explained, the attack lasts for a fixed period of time or until certain conditions are met. One of these conditions is that the pressure near the feed stage registers five times its normal value.

Based on a theoretical analysis, the wall pressure in an IR-1 centrifuge could be about 20-30 torr. Uranium hexafluoride condenses at about 130 torr at a temperature of 300 Kelvin. Thus, raising the pressure five-fold would raise the wall pressure of the uranium hexafluoride gas to near its condensation point. If the uranium hexafluoride gas reaches a pressure exceeding 130 torr, it will condense and form a uranium solid, likely uranium hexafluoride. This solid will attach to the wall of the rapidly spinning rotor. This non-uniform buildup of solid material could cause an imbalance in the rotor, causing it to wobble, possibly damaging the bearings or causing the rotor to strike the side of the outer casing. Both would destroy the centrifuge. So, the analysis suggests that an attack aims to raise the pressure of the uranium hexafluoride gas sufficiently to damage or destroy the centrifuges.

Attack Effect on Centrifuges with Open Valves

How could this happen in practice? The code continues the flow of uranium hexafluoride gas into the feed stage while secretly monitoring the buildup in pressure. We looked at two scenarios, based on discussions with Symantec. The first is that the code also closes the valves in the product and tails piping close to where these connecting pipes leave the cascade. In this case, the gas flows into this cascade but has no way to exit, slowing building up pressure throughout. The second is if the valves at the end of the cascade in the product and tails lines are not closed by the attack scenario. In this scenario, the uranium hexafluoride gas would continue to flow through a smaller cascade, as described above.

Product and Tails Valves Close

If the code closes the valves in the product and tails lines, then the cascade is a semi-closed system with gas flowing into it but unable to exit. The result would be a relatively rapid increase in pressure in this modified cascade. The pressure would build up sufficiently to cause the gas near the wall to condense and cause damage to the centrifuges, including their possible destruction. The pressure would be expected to build up in the non-feed stages faster, causing them to fail first. The attack ends when the pressure increases five-fold, as measured near the feed stage. Thus, the attack may spare the centrifuges in the feed stage.

In this scenario, all non-isolated centrifuges could be destroyed, or one third of the total number in the cascade. However, if the centrifuges in the feed stage survived, up to 30 centrifuges would be destroyed, or up to about 18 percent of the total number of centrifuges in the cascade.

Product and Tails Valves Open

If the valves in the product and tails end remain open, the attack would seem not to have much impact. However, a transient phenomenon may cause significant damage.

As the attack proceeds, the gas flow in the cascade would reach a new equilibrium, producing less enriched uranium and a product with a lower enrichment level. This state may be slightly disruptive but not destructive.

[2] According to Symantec, the particular centrifuge valves closed per stage are randomly chosen. The code will randomly choose a starting centrifuge valve and then close the next one in order until the last centrifuge valve in the stage. If the total desired number of valves to close for that stage has not been reached, the code will continue from the first centrifuge valve in the stage until the maximum valves to close are reached.

However, right after the valves are closed, a transient situation develops that could be destructive of these centrifuges. In this initial period, the rate of uranium hexafluoride gas entering into the non-feed stages of this modified cascade would greatly increase, as the fraction of closed centrifuges in the non-feed stages is often 70 to 80 percent (see figure 1). Based on a preliminary estimate, the feed rate going up would increase the wall pressure quickly and significantly. Preliminary calculations show that an increase in the feed rate by four to five times would likely cause an increase in the wall pressure to near or above the condensation point of uranium hexafluoride. Any condensation could cause the centrifuge to crash.

In this case, the feed stage is unlikely to be affected. The number of centrifuges that could be destroyed would be up to 30, or about 18 percent of the total number of centrifuges in the cascade.

Effect on Centrifuges with Closed Valves

Our analysis suggested another type of damage may occur in the 110 centrifuges with the closed valves. After the three fast-acting valves close, the centrifuge will still contain a small amount of gas. After closure, the uranium hexafluoride gas will continue to circulate in the centrifuge. Typically, an operator does not want to keep these valves closed for more than a few minutes. In an emergency shutdown during regular operations, the valves on the good centrifuges are normally reopened relatively quickly, typically within a few minutes. However, if these valves remain closed and the gas continues to re-circulate, the centrifuge can be damaged.

This case is not well understood, since it does not occur in normal operation. But our analysis suggests that this internal flow could cause the gas to heat up from impinging on the centrifuge scoops with no method to remove that heat. The small opening into the aluminum scoop could be choked off by ionized gas particles. This damage could impact the centrifuge's performance negatively after the attack. So, the attack strategy could damage the centrifuges with closed valves as well as those with open valves.

Opening of Valves at End of Attack

According to Symantec, near the end of the attack, the code opens almost all of a set of 25 valves. Most of these valves could be in the "dump" line piping of the cascade, where each stage has a connecting pipe to the main dump line that contains one valve. The dump line allows the gas in the cascade to be emptied, in the event of an unusual occurrence. The main effect of opening these valves may be to empty the cascade of uranium hexafluoride gas via the dump line, which ends in a cooled tank. Afterwards, after some delay, the code returns the system to state 0, as defined in the Stuxnet code, and waits for the right conditions to launch another attack.

In addition to the 15 valves between the stages and the dump line, there are also two dump valves at the ends of the dump line, three feed, product, and tails valves (in the connecting piping near the cascade), and five valves at the tails and product end of the stages to allow the taking off of product and tails at varying enrichment levels.

Effectiveness of the Attack?

Did this attack scenario work? Clearly, it was replaced by a strategy that attacked the frequency converters, causing the rotors to speed up to the point of rotor material failure. Thus, a reasonable conclusion is that the operators of Stuxnet wanted to destroy more centrifuges than this initial attack strategy appeared capable of doing.

ISIS found one data point that may be relevant. During the initial phase of operations of Natanz Fuel Enrichment Plant, the number of crashed centrifuges was up to 20 percent, far higher than expected by the

Iranians, who had expected occasional centrifuge failures. This failure rate is approximately the same as discussed above in those non-feed stage centrifuges whose valves remained open. Given that the first module started in about 2007, the intent of the code writers may have been to keep breaking a limited number of centrifuges in sets of six cascades. However, the 20 percent failure rate could have also resulted from incompetent operations.

To explore the effectiveness of the code further, ISIS evaluated centrifuge operation data from the quarterly International Atomic Energy Agency (IAEA) safeguards reports on Iran. This data is presented graphically in a series of ISIS reports. Two of the graphs are presented here as figures 3 and 4.

Figure 3 tracks the relationship between feed and product. Typically, the feed to product ratio should be about 10 to 1. In this graph, if this ratio is achieved, the two lines track directly on top of one another. As can be seen, during most of 2007, the feed to product ratio exceeded ten. This extra feed may have reflected extra uranium going into the dump line and not going to the product tank, which would contain uranium enriched to about 3.5 percent, or the tails tank. Similarly, starting in late 2008 and continuing into 2009, this phenomenon occurred again.

It is known from the IAEA reports that several tonnes of enriched uranium have ended up in the dump tanks at the FEP. It is unlikely that all this waste uranium resulted from Stuxnet, given the operational problems the FEP also encountered. However, some of it may have been due to this earlier version of Stuxnet.

Figure 4 plots the enrichment output, in terms of average separative work units (swu) per year per centrifuge. The data start after 2007, so the initial period cannot be studied with this data. This graph provides a measure of how well the cascades are enriching. It can be affected if many centrifuges crash, but Iran, and subsequently the IAEA, include them in the total number of operational centrifuges. In that case, the average value would decrease accordingly.

Starting in late 2008 and continuing into early 2009, the average enrichment output decreased sharply, before rising again. This could imply many centrifuges crashing but not being reflected in the total number of enriching centrifuges stated by the IAEA in its reports. This could occur for example if the crashed centrifuges were not removed until later. In addition, during this time period, the number of enriching centrifuges remained relatively flat, so this decrease in enrichment output does not appear to result from a ramping up of newly installed, but poorly performing, centrifuges.

Thus, based on the IAEA data, the initial attack strategy could have had an impact in 2007 and again in late 2008 or early 2009. Without more data, this conclusion remains preliminary.

The damage from the second attack strategy was more systematic, destroying most of the centrifuges in each cascade. As such it was more noticeable, in that the Iranians would remove many centrifuges at one time and the IAEA would record this removal. As such, the crashed centrifuges would not affect the average enrichment output.

Stage	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Centrifuges	2	2	4	6	8	10	12	16	20	24	20	16	12	8	4
Centrifuge valves to close	2	2	2	4	6	8	10	13	14	0	14	13	10	8	4
Percentage closed	100%	100%	50%	67%	75%	80%	83%	81%	70%	0%	70%	81%	83%	100%	100%

Figure 1 IR-1 cascade and the number of valves closed.

Figure 2, IR-1 cascade in the Natanz Pilot Fuel Plant, showing the pipework above the centrifuge.

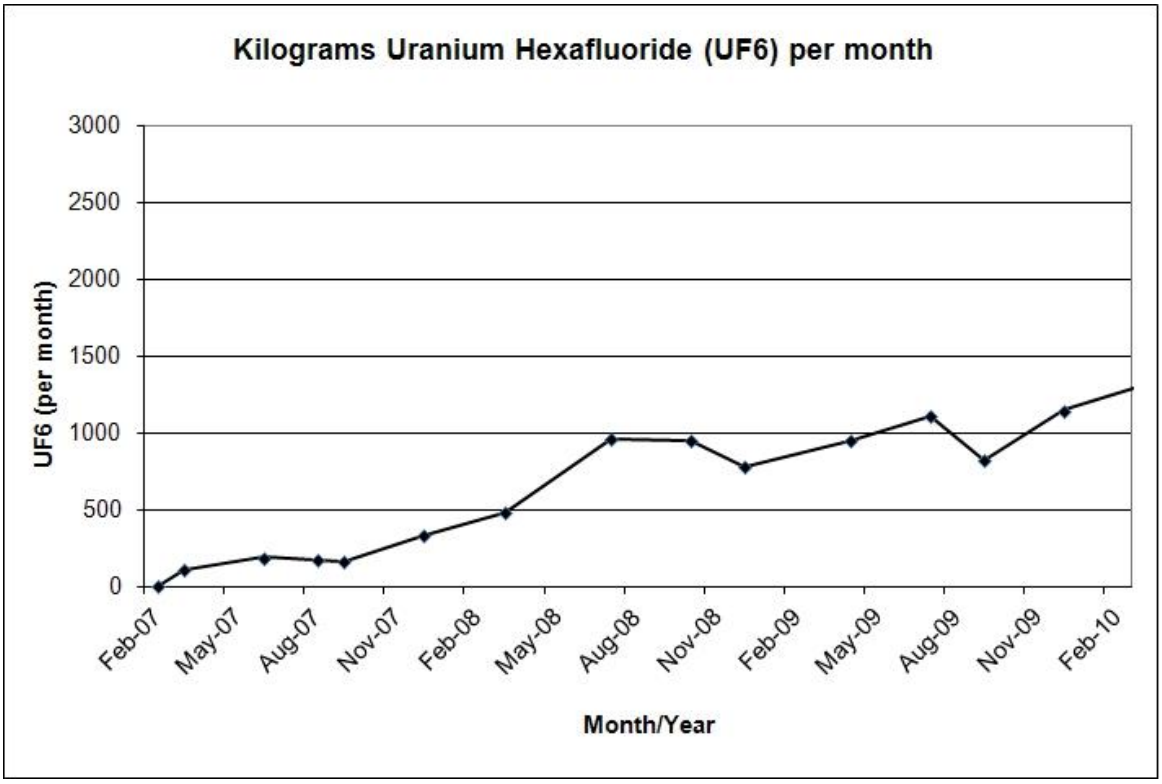

Figure 3 Cumulative uranium feed and product in the Natanz Fuel Enrichment Plant.

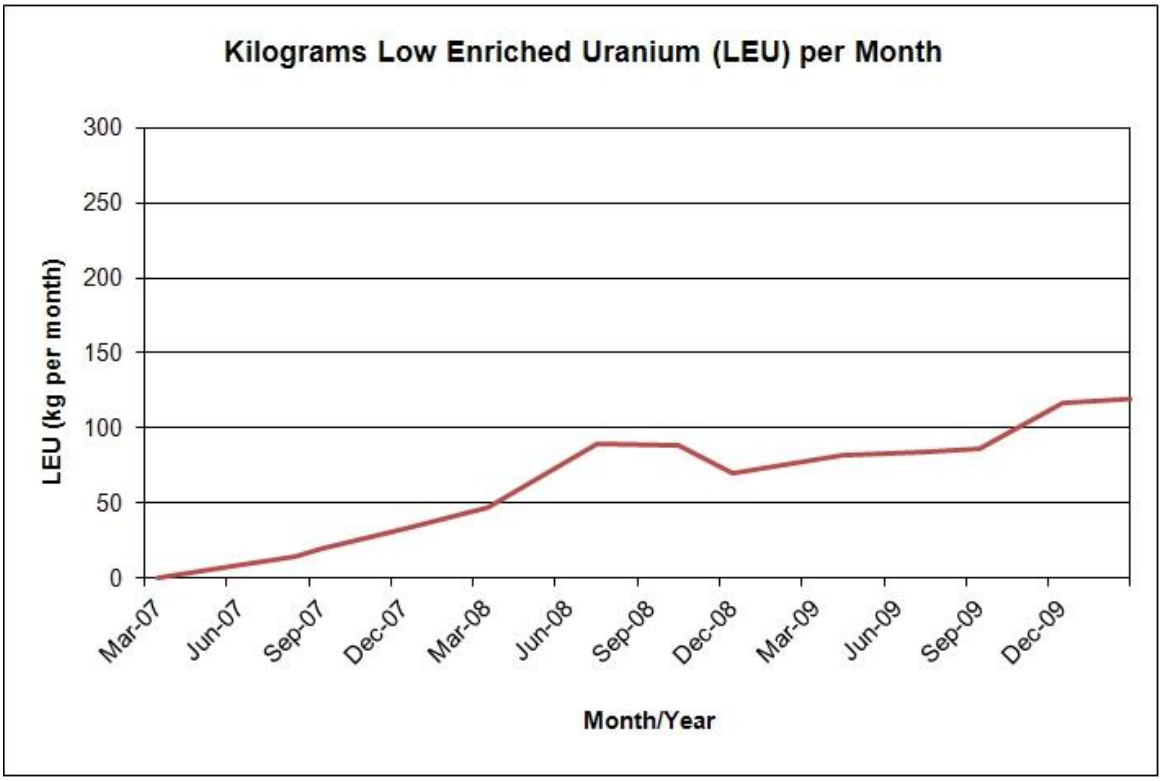

Figure 4 The total number of centrifuges claimed to be enrichig compared to the average enrichment output in the Natanz Fuel Enrichment Plant.