Security

One page description

Final Year

Alexandru Sulea
D Stream
#12315152
N April 2017

Contents

List of Tables

1 Overview

The most interesting security attack to date is the STUXNET worm developed by the Tailored Access Group inside the NSA. This attack was especially interesting due to the complexity of the worm and also that it is the first public attack perpetrated by a state against another states energy systems.

Although the united states has been an active agent in intelligence communications attack since its inception.. The theory of the worm is rooted in warfare which has existed since the invention of the telegram.In the American civil war, confederate and union soldiers would routinely compromise each others telegram communication to gain the upper hand in warfare. Initial attacks would just mean cutting the telegram wire of the enemy. This then evolved to listening to the enemies communications and then splicing the wire to send different orders to enemy units.. It is far more harmful to misdirect the enemy than trying to cease their communications. Not only does it cost the enemy far more resources, (for example by having an enemy unit walk into an ambush set up by your own teams), but it also causes lasting psychological effects to enemy units, who then do not fully trust the orders received by commanders and may hesitate to follow a direct orders.
In much the same way STUXNET not only caused industrial damage to nuclear centrifuges but also psychological damage to the research teams who will now doubt the results of their equipment.

STUXNET was designed as a worm which was needed to pass over the air filter, the nuclear facilities in Iran were not linked up to the Internet thus STUXNET needed to pass undetected in a camera or usb over many devices until it was sure that its location was inside an Iranian nuclear facility.
Once inside the facility it would spread across computers to the control hardware linked to to the centrifuges which enriched the uranium for nuclear bombs.
At this point STUXNET needed to perform lasting damage without ever being detected, thus it would check for specific control hardware which controlled the spin of the centrifuges but also the dials which displayed the pressure and rmp of the centrifuge.
STUXNET would then perform an asymmetric spin of the centrifuge arm, weakening the material strength of the carbon fibre as well as increasing the pressure inside the centrifuge while showing normal operating circumstances on the display dials.
This would lead to the carbon fiber arm inside the centrifuge breaking, shattering the centrifuge and contaminating the facility, rendering it useless for a prolonged period. At the same time the data on the centrifuge would be changed to show that the centrifuge had broken down under normal operation procedures. Even if the centrifuges were then changed the same process would happen again as the worm was in-bedded across all the computers in the facility. It is documented that the Iranian administration had imprisoned several scientist for suspicion of working for foreign intelligence agencies while in actual fact the scientist were extremely confused as they could never find the actual reason of why the centrifuges had shattered into a million pieces.
The worm was detected due to the updated version which was worked on by the Israel intelligence agency. The agency altered the worm so that it could pass through emails and added a number of zero day exploits so as to possibly phish for Iranian scientists.
This and a number of other more aggressive alterations led to the worm being more active in systems and thus more detectable.
The downside of this was not only that the Iranian government was able to detect the worm but that it now had a powerful weapon in its arsenal which was specifically tailored to attack uranium enrichment facilities. With the addition of smart cars and other autonomous industries evolving rapidly and embedding themselves more into society it is not hard to imagine how such a worm can be re-purposed to target a smart car system. Where using low level instructions a car can be reprogrammed to break when going at 60 kph and turn sharply to the right if known government employees are present. The worm would then delete any incident analysis from the system and re-write that the car failed under normal operating procedures before going dormant.
Academics have agreed that STUXNET is especially dangerous given the lax security protocols found in energy systems around the world which are not prepared for such an advanced and intelligent attack tool.

References