The cybernetic war.

An analysis of Conficker, Stuxnet, DuQu about Flame, mini-Flame , Gauss, Mahdi to Shamoon

Forum für Informationssicherheit

www.gocs.de; -eu; -info; -com.de

Abstract

Do we ask the simple question first, has this one started already, then?

One can answer this question easily yes and no.

For the reply to this question we have made the effort once to evaluate press publications to this topic.

We would have used "information keeping closed secretly" for the ones who want to assume us. They let it emphasize again we have analysed only publicly accessible material for us.

We have only the period of time after "Stuxnet to Shamoon" used, that is a relatively short time for the analysis time period.

Simultaneous also became made a restriction with respect to the enormous masses of harming software. Because this one was interested in only the typical "cybernetic arrows" fulfil the attribute "warlikely".

The but also simultaneously the typical structures which are typical of weapon systems. But also the temporal dependences of the individual weapon systems.

Although only few "cybernetic arrows" were described comprehensively, they permit a very interesting insight so. You we can look, about this write later where one, because otherwise they lose the connections. Because from book pieces no strategy can build up for the defence. This natural only, if they want it.

The cybernetic fight means used in this above-mentioned time period from the spying means up to the destruction means are known to them or are put ahead as confessed.

We have divided her up into two groups.

This group contains the destruction and sabotage weapons.

The other group contains the spying systems as well as some subsystems, like manipulation systems.

Methods which stored information is changed or deleted shall be understood, under these Subkategorie manipulation systems. However no systems for the production control.

1 Group

The most well-known representatives of this group are "**Stuxnet"** and "**Shamoon".** Your effect consists in the destruction of program-controlled process systems. (Stuxnet) but also in the destruction of the computer infrastructure, how magnetic storage systems (hard disks) and ä.

The first world-famous cybernetic arrow is indicated by a very specific destruction module. This grips only special production control systems (uranium enrichment systems with a SPS from Siemens).

At a use against other production controls of the same manufacturer no serious damages were watched.

The first use of these cybernetic arrows is indicated by an unusual feature. These first attacks were by specific use - this is said, run through a direct implementation into the cybernetic system (computer). After different press publications both strokes were undertaken by authorized employees of the respective computer centres.

This concerned the attacks in Iran and the attacks where in Saudi Arabia the oil industry was met.

How far does nothing reduced the inner security procedures, the respective damages has, is known?

Therefore possible protective substances could not get effective from the communication system (Internet or other communication channels). At such an attack Internet based security procedures are ineffective (so-called **cyber defence head offices).**

This applied to use of "Stuxnet" and "Shamoon" similarly.

Like many of these infections authorized employees were is not known running through. Is alone for this way of the attack of importance, that one of these was carried out directly into the computer system.

The type is this one this type, a protection system directly in the computer system required or corresponding operating systems or more detailed protective measures, how internal encoding or deciphering. Except for the known protection systems once. Nothing else is called what, these systems must according to the value of the information.

In the case of "Stuxnet" it still came to a mass infection after first use via Internet. Units shall have been infected approx. 60.000. What should be aimed by this distribution is unclear, since "Stuxnet" was a highly specialized cybernetic arrow and still is.

The holes then in the used software systems were filled only after the long time, more months.

Until this "Flickenschusterei" was carried out, a cybernetic war (Cyberwar) could have been waged over these holes successfully.

The one penetrating body made a very intelligent drop possible. The successors or the platform is products make use of a variety of one penetrating bodies.

As many there are holes!

The emphasis arises from the fact that only the corresponding harming modules need to be exchanged for another aim characteristics, also in the presence.

The same behaviour also applies "to the penetration bodies" for penetrating into the respective cybernetic units of (computer systems).

A characteristic of modern cybernetic arrows is the modularity.

2 Group

This second group is fundamentally more extensive. Bekannte Vertreter sind DuQu, Flame, Gauss, MiniFlame und Mahdi.

One can describe this group as "cybernetic spies". These cybernetic spies are indicated by unusual features against the classic spies.

Becomes these unusual features and closer to the cybernetic spying come in on.

The group of cybernetic spies was used very in detail. The representatives DuQu and Mahdi got that way only in a small number eigesetzt. This is called nothing else, as which some of these cybernetic arrows only relatively were used or what can be the case also, very few were discovered. Is also little known about the special ones to formulations of these means. They are nevertheless assessed as "most dangerous". So among others also of the BSI/Germany. From other sources a long-term use is not excluded with new spying modules.

One can compare DuQu with a reconnaissance satellite. He is there up but one does not know further!

It must be calculated according to these sources with a renewed use. After the known experiences from the development of all sorts of platforms "DuQu and Stuxnet" systems developed further are used.

This development line is also recognizable at the known spying systems.

This is also applied principle application. What is called nothing else, the proven and successful systems become by use of new modules, developed for changed formulations. At the same time the experiences are modified and optimized with older solutions to do justice to the growing requirements. This one concerns the analysis modules but also the communication modules. The latter are of special importance since they must pass information about covered servers on won. This one applies to the information quantities like but also for the secrecy. These turn " won " for this reason information transmits in an encoded or encoded form. The same principle was already used in the second World War. So information which was won from the "Enigma" was encoded for the further conveyance. Which method on a British side to use came, seems today, too, to be another secret. The name "extremist" got these all of the methods.

It was prevented with that that the German side gets knowledge of the "drop" into the cipher system Enigma and the decoded information is protected simultaneously. There also

was an analogy into the eighties in connection with decoded information by the ZCO of the ex.DDR.

This old procedure is ascertainable also among the cybernetic spies. The information is protected also here, through this no revelation of the information spied out is possible. You also cannot close at knowledge of this information which is transmitted in the field of assignment to the servers on the "interesting information".

The cybernetic object which was cleared up by these cybernetic arrows should not get any significant notes which are information for the clearing up of importance.

There is a very interesting starting point also:

(1)

Some buyers buy "magnetic data carriers" for valuable information (e.g. tax data of German tax evaders) with interesting and for her and pay millions of € for this. The value of this information amounts to a multiple.

Are known on the market of the information generally, the European tax authorities seek "information about the financial increase".

This information is not traded on the market there, they can be obtained only in an "illegal way". These deeds are undertaken by "authorized persons".

(2)

Use of cybernetic means is preferentially required another form of the information extraction, this one, of others.

In this case cybernetic arrows take over the function of the information collector in strange cybernetic plants. The information collected is transmitted via communication servers. In some cases data massifs shall have been transmitted of 5 gigabytes size. You can be taller or smaller, however.

The data collection via a "cybernetic arrow" is more flexible in comparison with a human source. The use of these arrows allows to give a matching answer corresponding to the customer.

Of course another advantage arises, one can carry out fast changes because this one has discovered customers, further unknown sources.

The fast variability is part of the characteristics of the cybernetic clearing up beyond all doubt within the aim object.

The different procedures are dependent on the respective types of state.

This has a size small spying helper flax like every other programme or cybernetic arrow. Slim, others are thick ships some of these against this. They originate from one and the same platform.

The best known "thick ship" is "Flame man".

Use of the cybernetic spies is very differently carried out.

So there are some as DuQu or mini-Flame man employed only in low quantities. It is calculated per system with up to 60 infections.

The total number of these special cybernetic spies therefore amounts to approx. 120 infections.

This seems to be a very special and sensitive cybernetic spy.

The details on it are not evaluable for an analysis.

Others however are put into masses. Infection instalments of 10.000 or more were stated.

Flame man approx. 5.000 to 6.000 infections

Gauss approx. 2.500 infections

Mahdi greater 700 infections

Conficker approx. 60.000 or possible still greater.

The use instalments of these cybernetic spies were around 10-fold up to 100-fold over the special systems. In individual cases this value can be exceeded considerably (Conficker).

The area of the infections hesitates between the minimum of 68.200 and the maximum of up to 100.000 or more infections.

The number of unrecorded cases is, however, fundamentally higher. From analysis of other harming systems factors can be assuming between 3 ... 8, however.

The reasons for these high numbers of unrecorded cases are known and shall here not be given further treatment.

Also on the geographical distribution of the "found harming programmes" you shall not come in here consciously more nearly. Since a number of applications of cybernetic arrows provides other, divergent results. Simultaneous is the use of certain cybernetic arrows illogically from more geopolitical.

A very interesting analysis point devotes itself to the question in which areas, politics, economy, armed forces, research and development, infrastructure etc.

The knowledge won here is very interesting.

These results are not published, however, since "misinterpretation" could between minimize and lead panicmongering of a cybernetic war to end of the world scenarios.

Stand of the analysis 10.12.2012

Remarks:

This material is component of the "forum for information security".

There published and ongoingly updated.

This material is only based on publicly accessible publications.

Publish under following addresses on the Internet:

www.gocs, de bzw. www.gocs.eu bzw . www.gocs.info or www.gocs.com.de

Berlin, 23.12.2012

Author Old Gocs

Further use requires the consent of the author. This analysis is revised ongoingly. Mistakes are excepted.