Press Release
Oct 07, 2010
http://enisa.europa.eu

EU Agency analysis of Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection

The EU cyber security' Agency ENISA, i.e. the European Network and Information Security Agency, has produced an initial comment and brief, high level analysis of the recent Stuxnet' attacks; on its importance, and its technical implications for Europe. The Agency considers Stuxnet' a paradigm shift, and warns that similar attacks may occur. It argues that Europe should reconsider its protection measures for Critical Information Infrastructure Protection (CIIP).

ENISA has produced a high-level impact analysis of the Stuxnet malware. The purpose is to provide EU decision makers with guidance on how to interpret the malware, its potential impact, mitigation and what these new types of attacks in general mean for Europe.

The Executive Director of ENISA, Dr Udo Helmbrecht, comments:

> Stuxnet is really a paradigm shift, as Stuxnet is a new class and dimension of malware. Not only for its complexity and sophistication, e.g. by the combination of exploiting four different vulnerabilities in Windows, and by using two stolen certificates, and from there attacking complex Siemens SCADA systems. The attackers have invested a substantial amount of time and money to build such a complex attack tool. The fact that perpetrators activated such an attack tool, can be considered as the "first strike", i.e. one of the first organized, well prepared attack against major industrial resources. This has tremendous effect on how to protect national (CIIP) in the future.
>
> After Stuxnet, the currently prevailing philosophies on CIIP will have to be reconsidered. They should be developed to withstand these new types of sophisticated attack methods.
>
> Now, that Stuxnet and its implemented principles have become public, we may see more of these kinds of attacks. All security actors will thus have to be working more closely together and develop better and more coordinated strategies." Dr Helmbrecht concludes.

For a more **detailed, online, technical analysis, and Agency recommendations,** pls click.

How ENISA supports the Member States to prepare for attacks on critical information infrastructure

Large scale attacks on Critical Information Infrastructure needs a coordinated reaction, involving the key players from both public and private sector. No Member State, hardware/software vendor, CERT or law enforcement agency can successfully mitigate sophisticated attacks like Stuxnet on their own.

ENISA, as an EU body of expertise in Network and Information Security (NIS), is supporting the European Commission's CIIP action plan. This involves working closely with the Member States, public and private sector stakeholders' to secure Europe's Critical Information Infrastructure.

ENISA's Resilience and CIIP program helps the Member States and private sector to develop good practices in a number of areas relating to the protection of Critical Information Infrastructure. These include combating botnets, improving the security of interconnected networks and reporting major security incidents.

In 2011, ENISA will support the development of good practices in securing SCADA systems and analyse dependencies of critical sectors to Information and Communication Technologies.

'CYBER EUROPE 2010' 1st Pan European cyber security Exercise

In addition ENISA, in co-operation with all EU Member States and 3 EFTA countries, is coordinating the first CIIP pan cyber security European exercise, the 'CYBER EUROPE 2010'. This exercise will test Member States' plans, policies and procedures for responding to potential CIIP crises or incidents, such as Stuxnet'.

Reinforcing 'digital firebrigades'; CERTs

ENISA is also active in **reinforcing national/governmental 'digital firebrigades' i.e. Computer Emergency Response Teams, or CERTs,** by supporting the Member States with the setting-up, training and exercising of incident response capabilities. Together, we define a set of baseline capabilities all teams should exhibit. We also work on enhancing capabilities in e.g. cross-border cooperation, Early Warning, and cooperation with law enforcement.

ENISA actively supports a coordinated reaction to large scale attacks, and will (if called upon) willingly take its role as coordinator and facilitator for appropriate counter measures.

Further information:
Several NIS agencies in the EU Member States published information about Stuxnet in their respective language. Please refer to the ENISA country reports for an overview of security activities in each Member State.

On e.g. these websites you can find more information on the malware itself, detection and mitigation, published by (external actors), Siemens and Symantec.

- Siemens tool & procedures for removal
- Symantec ongoing analysis of Stuxnet
- Stuxnet White Paper (PDF)
- Ongoing Stuxnet Response Blog

For interviews: Ulf Bergstrom, Spokesman, ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143

For further details, please contact:
Tim Mertens, Head, Public Affairs/Marco Thorbruegge, Sen.Exp

Ulf Bergstrom, Spokesman, ENISA