

# **Information Security Risk Analysis of Industrial Control System**

**Dr. Xiao Junfang**

**Electronic Technology Information Research  
Institute, Ministry of Industry and Information  
(ETIRI)**





Information Security Situation of Industrial Control Systems

Information Security Risks of Industrial Control Systems

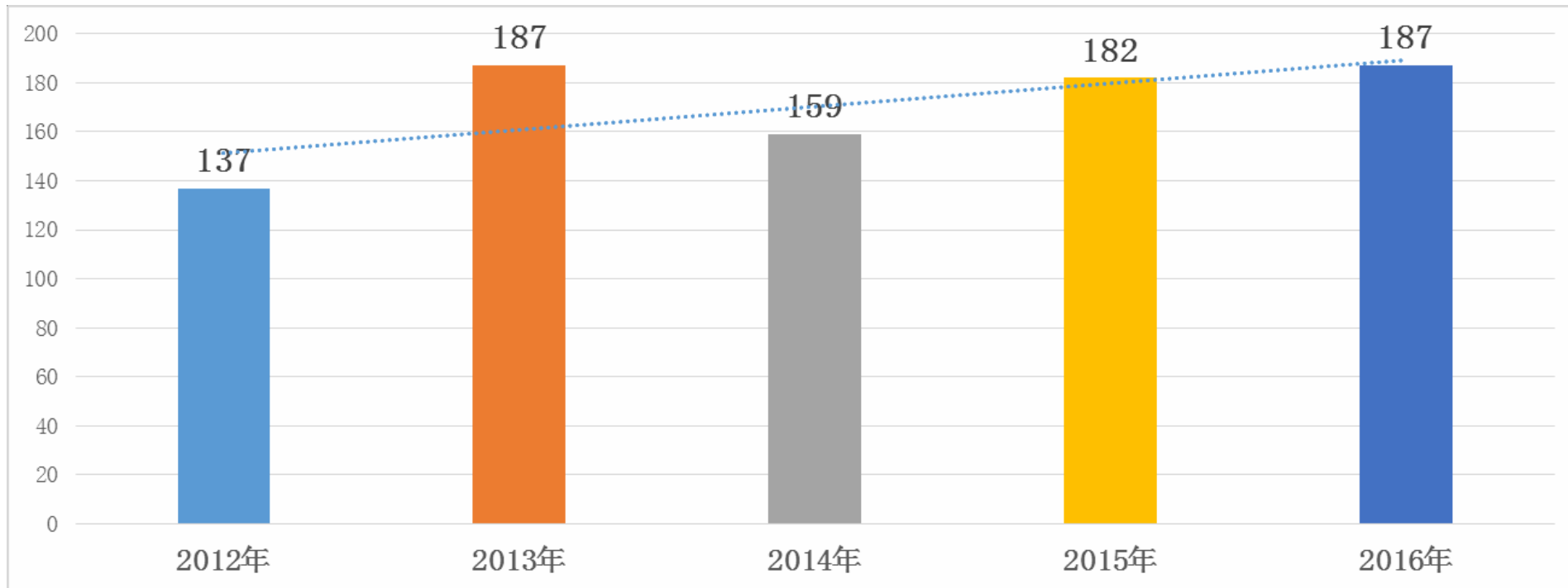
Suggestion of Strengthening the Security of Industrial Control Systems



# **Information Security Situation of Industrial Control Systems**



## 1. The number of vulnerabilities remains high, and the attack difficulty is decreasing



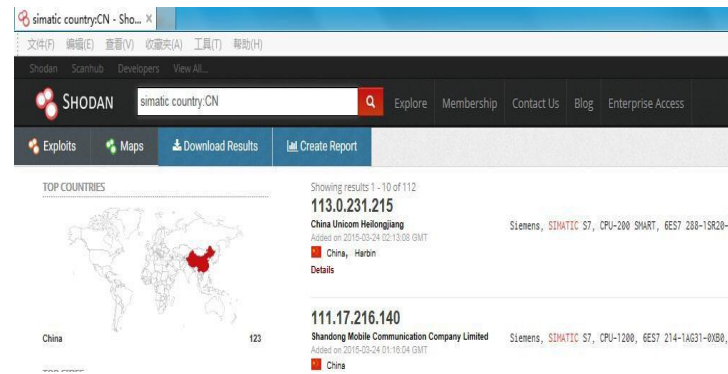
Source from ICS-CERT

# 1. The number of vulnerabilities remains high, and the attack difficulty is decreasing

Hackers can find industrial control systems with the following three ways at least:



1. Search through google and other web search engines.



2. Search through host search engine such as Shodan.



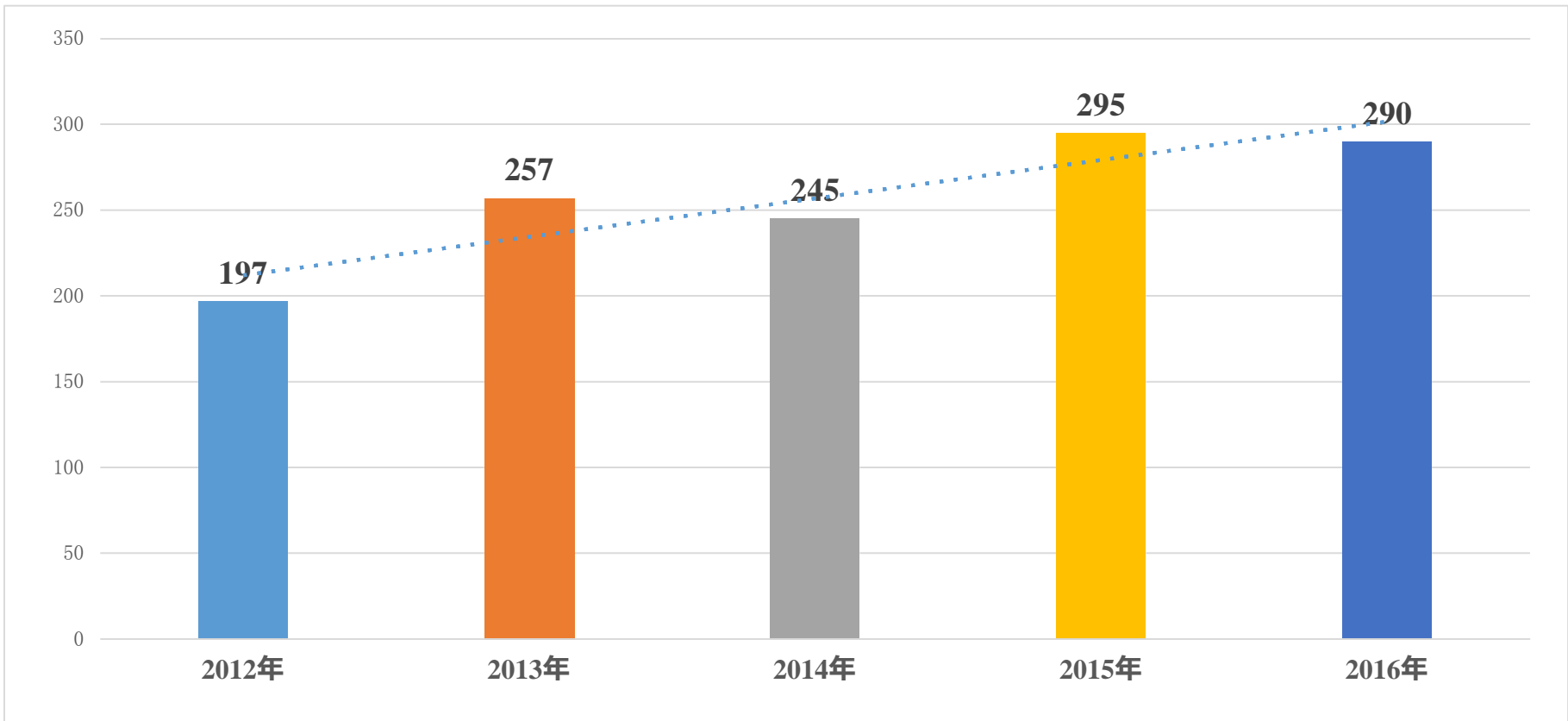
3. Match the network fingerprint characteristics on private protocol and port for industrial control communication through online monitoring platform.

# 1. The number of vulnerabilities remains high, and the attack difficulty is decreasing





**2. Industrial Control System Information Security incidents are frequent,  
and the scope of influence is wide**



Source from ICS-CERT



## 2. Industrial Control System Information Security incidents are frequent, and the scope of influence is wide



In 2010, the virus Stuxnet attacked the Bushehr Nuclear Power Plant in Iran



In 2012, the energy industry in the Middle East was infected with the virus Flame.



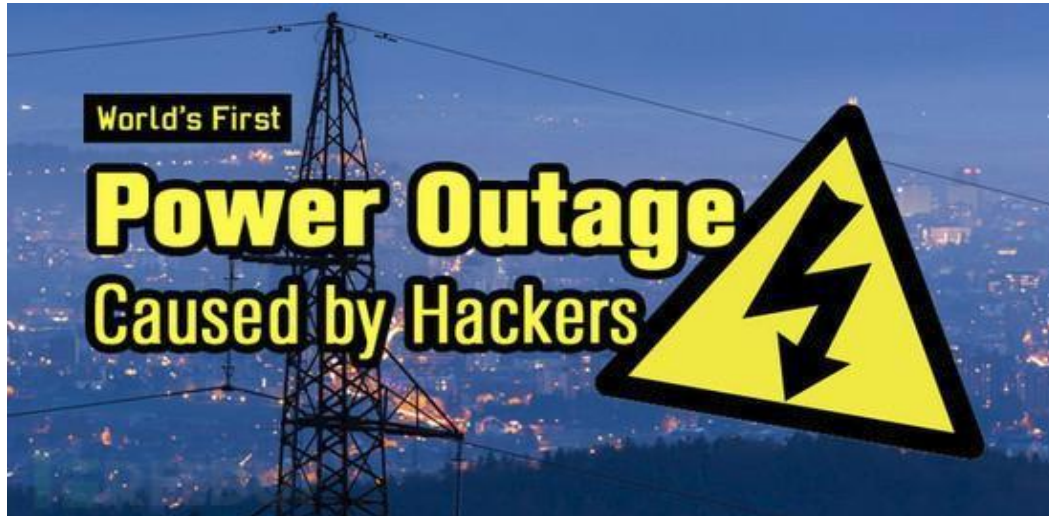
In 2011, the virus Duqu attacked the energy industries in the Middle East and Europe.



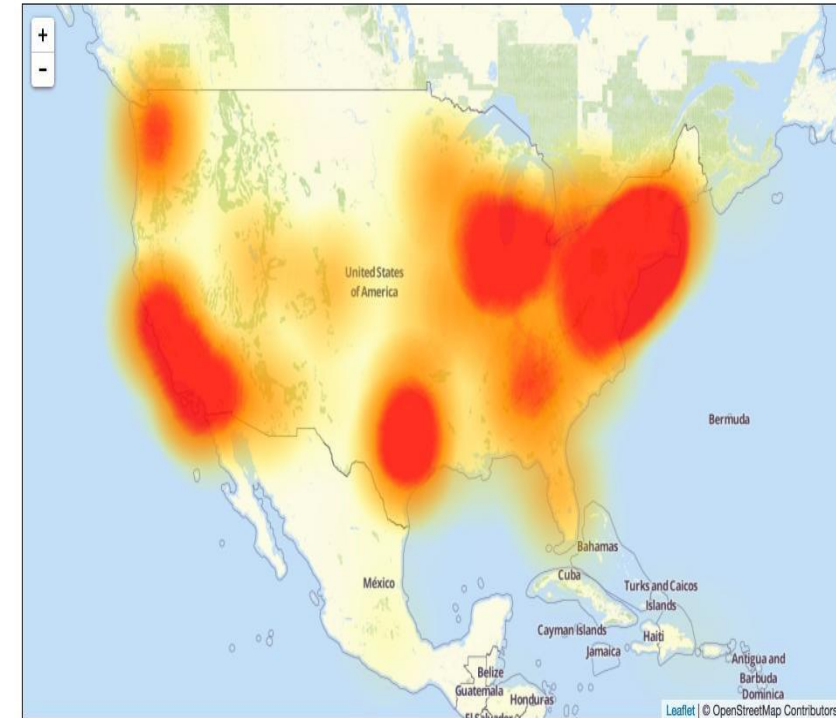
In 2014, the energy industry in Europe and America was infected with the malware Havex.



## 2. Industrial Control System Information Security incidents are frequent, and the scope of influence is wide



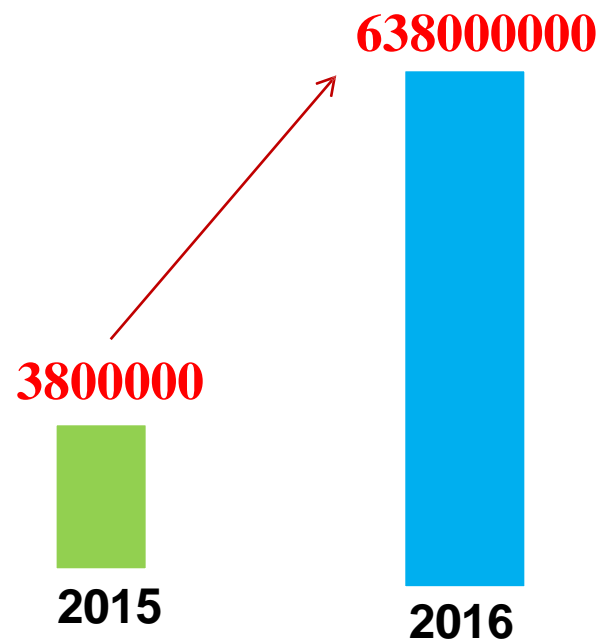
Ukrainian power grid blackout by “blackenergy”



half of the US Internet down by DDoS attack

### 3. The ransomware attack against industrial control system is worth paying attention

The number of recorded ransomware families largely **increased by 748%**.



The number of traceable ransomware attacks

### 3. The ransomware attack against industrial control system is worth paying attention



In 2016, the subway system in San Francisco was attacked by blackmail software.



In 2017, a global large-scale "Wannacry" infection incident occurred.

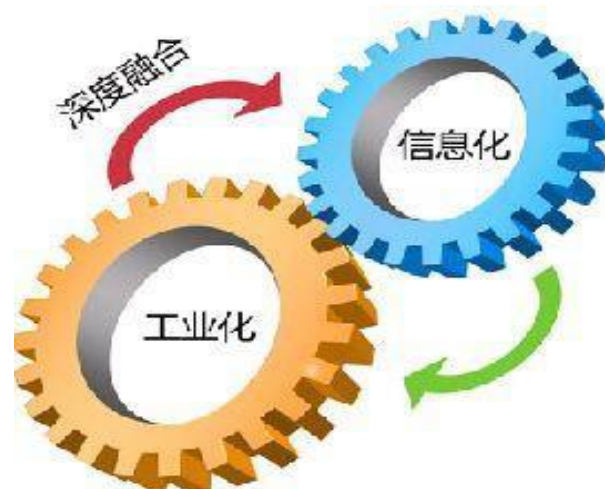
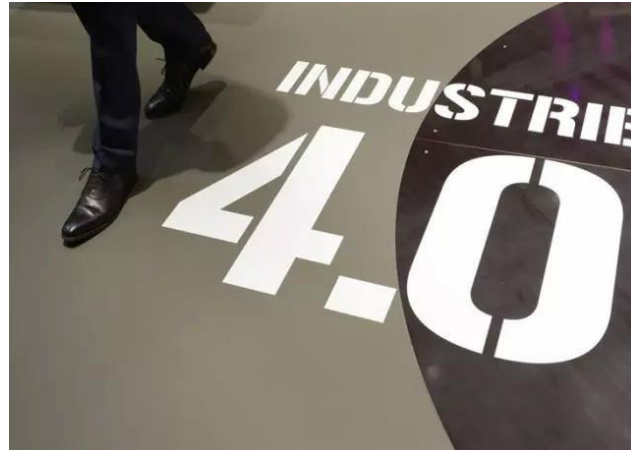
In the future, ransomware attacks are very likely to influence the industrial control system.



# **Information Security Risks of Industrial Control Systems**



# 1. The connection of ICS to Internet has become prevalent, and the traditional information security threats continue to penetrate into ICS





## 2. The traditional information security protection mode is difficult to protect the ICS security effectively

- ◆ characteristic of IT security: Confidentiality, integrity, availability
- ◆ IT security protection mode is no longer applicable



### 3. The security protection means of industrial control system are required to meet the system's characteristics of high availability and real-time performance



The industrial control systems in petroleum refining, power and other sectors with automatic process should run continuously for **7\*24 hours**.

#### 4. Enterprises' consciousness of industrial control system security is weak and their management and protection capabilities are not enough



Weak consciousness



Lack of Management mechanism

# Suggestion of Strengthening the Security of Industrial Control Systems



## We do

**Risks Assessment**

**Simulation Test**

**Threat Monitoring**

**Technical Research**

## We hope

**Standard development**

**Technical exchanges**

**Information sharing**

**Fight against cybercrime**



**THANK YOU**