公共基础设施威胁与安全

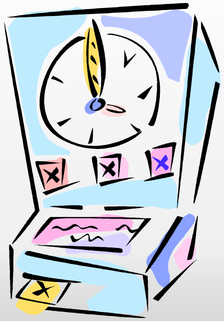
AhnLab EPS

演讲人：金起荣
部　门：融合产品开发室
职　位：室长

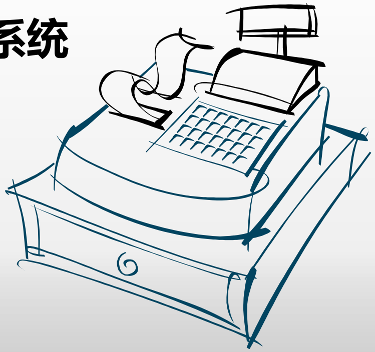
AhnLab

方便有效率的专用终端

- 产业系统
  - 公共基础设施
  - 工厂设备



- 金融系统
  - POS
  - ATM



- KIOSK
  - 机场
  - 商场
  - 活动场所

- 封闭网 业务领域

为什么专用终端很危险?

升级困难

如AV这样占容量大的安全解决方案难以适用.

各种各样的人员来经营

网络连接松懈

中断困难.

专用终端的维护和保护工作难进行。

错误的观念

封闭的网络
免疫恶意代码威胁

不使用外置储存
设备等于安全

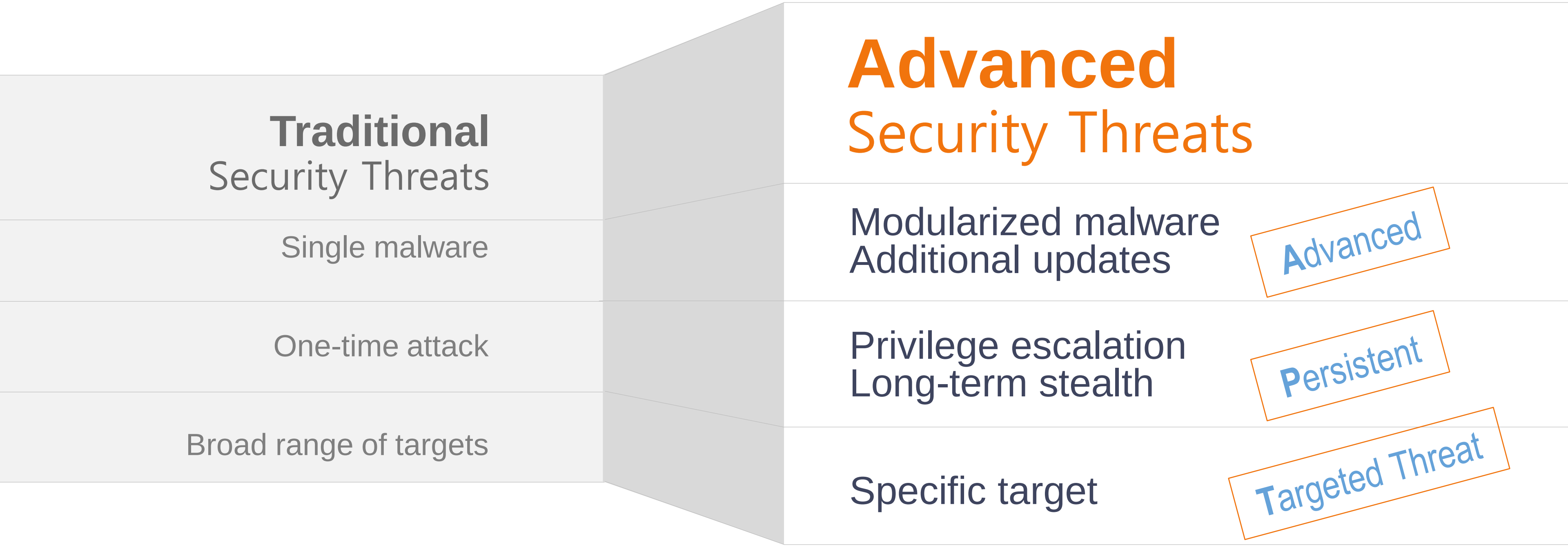
拦截未经许可的
程序执行等于安全

只要限制网络连接
即可以防止侵入

从无法预测的路径感染的恶意代码会破坏系统，造成信息泄露

完全改变的攻击方式

高级持续性威胁 - APT (Advanced Persistent Threat)



Traditional Security Threats	**Advanced** Security Threats	
Single malware	Modularized malware Additional updates	Advanced
One-time attack	Privilege escalation Long-term stealth	Persistent
Broad range of targets	Specific target	Targeted Threat

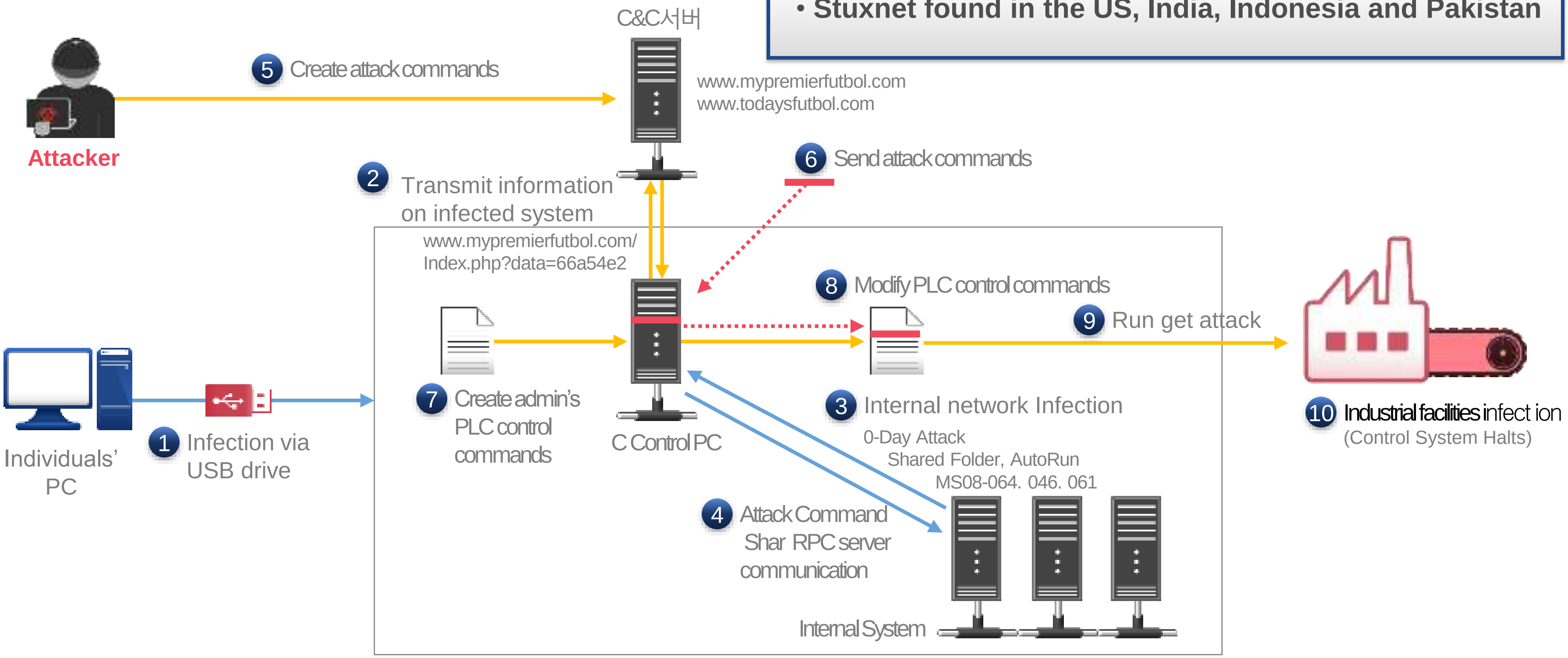
StuxNet证明了这些.

Stuxnet; targeting industrial systems

Stuxnet is specially-designed malware to target the SCADA system.
While other targeted attacks are usually geared towards financial gain, Stuxnet is designed to infect only the SCADA control system[1] to run out of control.

Incidents caused by Stuxnet

- **Iran's SCADA-controlled nuclear facilities attacked** (Jan. to Sep. '10)
  - Stuxnet penetrated Iran's nuclear facility to sabotage the country's uranium enrichment program
- **Stuxnet wreaked havoc in China** (Jul. '10)
  - 6 million PC in China infected by Stuxnet
- **Stuxnet found in the US, India, Indonesia and Pakistan**



Stuxnet is a sophisticated worm that infiltrates even "closed" networks to inflict severe damages to specific industrial control systems.

[1] Siemens WinCC/Step7 system

对公共基础设施的攻击比电影更危险

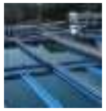
核电站

火力发电厂

水库

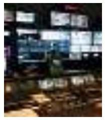
交通系统

防灾系统


自来水设施

监控

军事系统


电视台

通信设施

最近的攻击在一般PC上也几乎不可防御

- 在使用中的 AV 测试后以无法感知的方式攻击

- 虽有以与Anti-Exploit相同的方式来阻止，但由于使用于多种用途会影响性能

专用系统反而可以防御

Attack Surface Reduction

攻击表面最小化

- 程序弱点防御
- 外部储存设备管理
- 除允许的 IP/端点外全部阻止

Malware Prevention

恶意代码诊断

- 服务器为基础通过AV的终端恶意代码诊断

Restricted Applications

只可以执行允许的程序

- 阻止不被允许的程序执行

为了这些工作能有效化而开发

AhnLab

Whitelist-based Hybrid Solution, AhnLab EPS

1 Malware Detection & Prevention

2 Application Whitelisting

3 Easy Control & Manage

4 Centralized Management

AhnLab EPS

EPS

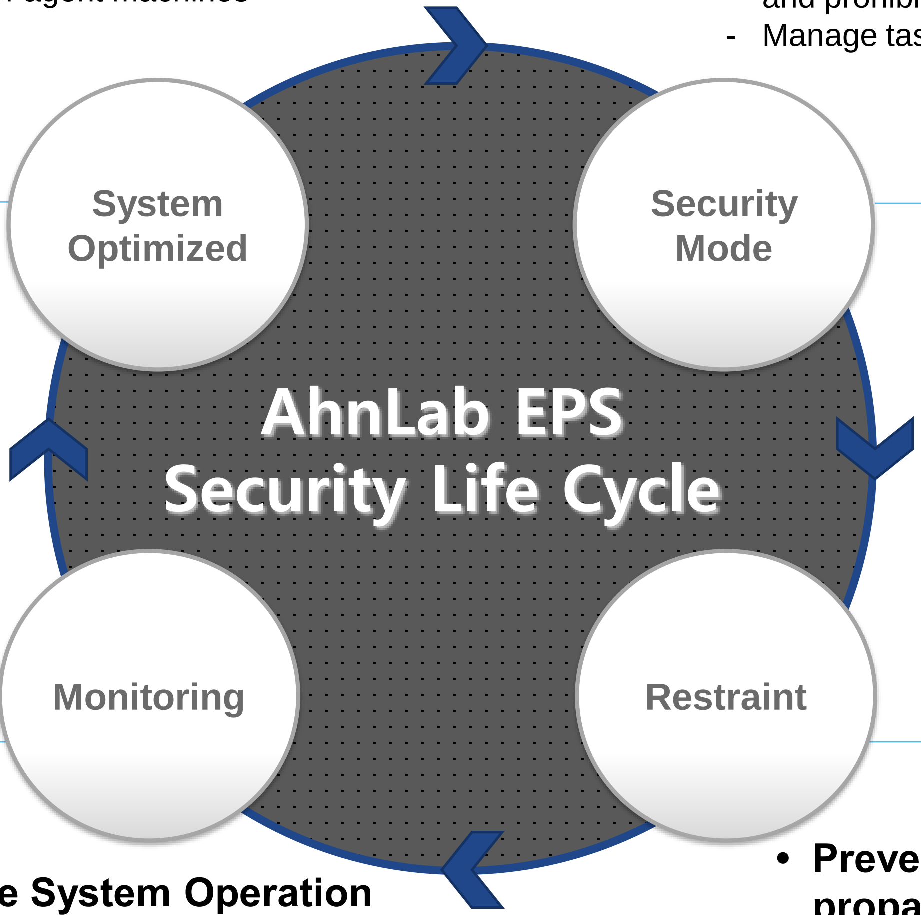
AhnLab EPS的业务流程

- **System Optimization**

- Analyze system operation
- Control non-grouped and non-agent machines
- Optimize system
- Repair malware

- **Manage and Control system**

- Manage system based on whitelist
- Manage external drive control, remote control and prohibited program execution
- Manage tasks using account privileges



- **Analyze and Manage System Operation**

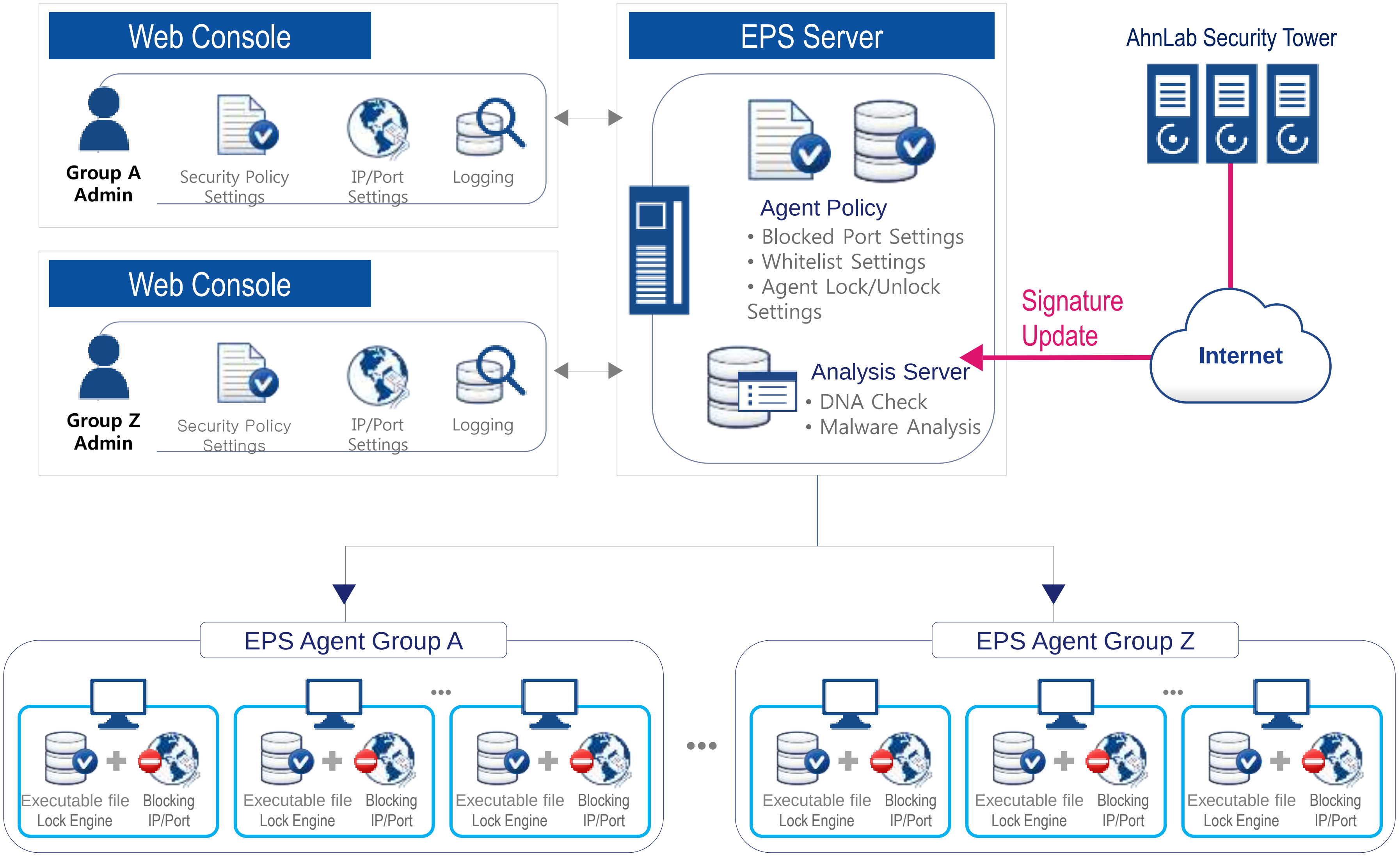
- Monitor all groups and agents
- Manage group/agent logs
- Respond promptly to issues via intuitive screen

- **Prevent and control malware propagation**

- Scan and control malware in real-time
- Block ARP spoofing and network attacks
- Block network IPs and ports

AhnLab EPS 配置和部署

AhnLab



AhnLab EPS 优点

01 在不影响系统资源和业务连续性的前提下控制恶意代码

02 限制非业务活动，提高生产线效率

03 阻止恶意代码或员工引起的数据流出

04 便利的远程管理系统

05 通过灵活的策略配置，进而有效管理

06 预防感染引起的系统中断

AhnLab EPS 会不断的进化

Thank you.

DESIGN YOUR SECURITY

演讲人：金起荣

部　门：融合产品开发室

职　位：室长

http://www.ahnlab.com