泛在电力物联网感知终端安全管控与主动防御机制

启明星辰集团 朱少敏

电力网络安全形势

2017年6月12日，安全厂商ESET公布一款针对电力变电站系统进行恶意攻击的工控网络攻击武器-win32/Industroyer(ESET命名)，ESET表示该攻击武器可以直接控制断路器，可导致变电站断电。

• 不要轻易打开来源不明的电子邮件。

• 定期在不同的存储介质上备份您系统业务和个人数据。

2.5 针对工业控制系统的新型攻击武器 Industroyer 专题分析（来源：启明星辰公司）

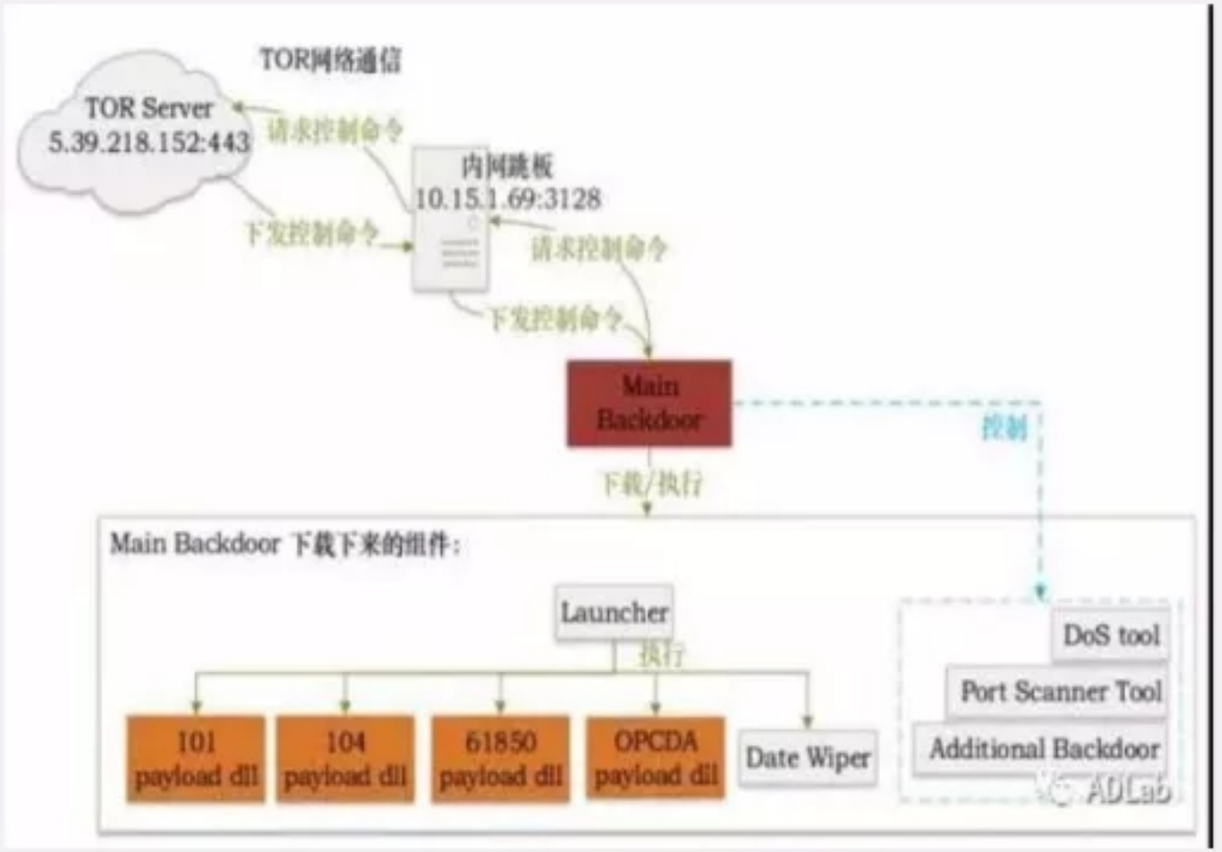
2017年6月12日，安全厂商ESET公布一款针对电力变电站系统进行恶意攻击的工业控制网络攻击武器Win32/Industroyer（ESET命名），该攻击武器可以直接控制断路器，导致变电站断电。启明星辰公司ADLab第一时间对该攻击武器进行深度分析。Industroyer恶意软件目前支持4种工业控制协议：IEC 60870-5-101、IEC 60870-5-104、IEC 61850以及OLE for Process Control Data Access（简称OPC DA）。这些协议广泛应用在电力网络、发电控制系统以及能够对电力进行控制的行业，例如轨道交通、石油石化等重要基础设施行业，尤其是OPC协议作为与工业控制系统无缝的通用接口，更广泛地应用在各个工业控制行业。

与2015年袭击乌克兰电网的攻击中使用的恶意软件（BlackEnergy、KillDisk等）相比，这款恶意软件的破坏性更大。它可以直接控制开关和断路器。Industroyer身后的幕后团队在攻击技术深度还是从对目标工业控制系统的研究深度都远远超过2015年打瘫乌克兰电网攻击背后的幕后团队。可以说，目前Industroyer恶意软件是继Stuxnet、BlackEnergy 2以及Havex之后第4款针对工业控制系统进行攻击的工业控制威胁。

2.5.1 Industroyer 恶意软件

Industroyer恶意软件由一系列的攻击模块组成。根据目前所公开的信息以及ESET捕获的样本来看，Industroyer恶意软件模块在10个以上。其中存在一个主后门模块，它被用于连接C&C下载并执行另外一些模块。这些模块分别为：实现"DLL Payload"模块下载执行的加载器模块，实现数据及痕迹清理的tasks模块，实现扫描已经授的port模块以及利用实现西门子SIPROTEC设备漏洞（CVE-2015-5374）进行DoS攻击的拒绝服务攻击模块。"DLL Payload"模块又包含有：实现IEC 101工业控制协议的101.dll模块，实现IEC 104工业控制协议的104.dll模块，实现IEC 61850协议的61850.dll/61850.exe模块以及实现OPC DA协议的OPC.exe/OPCClientDemo.dll模块等。表2-19列出Industroyer样本及其功能。

摘自：《2017年中国互联网网络安全报告》



Industroyer攻击路径

物联网安全形势

启明星辰

根据Gartner预测，到2020年，25%的企业安全事件都将会和物联网相关

Gartner

The compound spend on IoT security relating to government, utility, building and facility automation, and manufacturing amounted to $249 million in 2015 and will grow to $526 million in 2020. Although not all this spend is directly linked to such initiatives, we expect these elements to drive the majority of investments.

Demand Factors

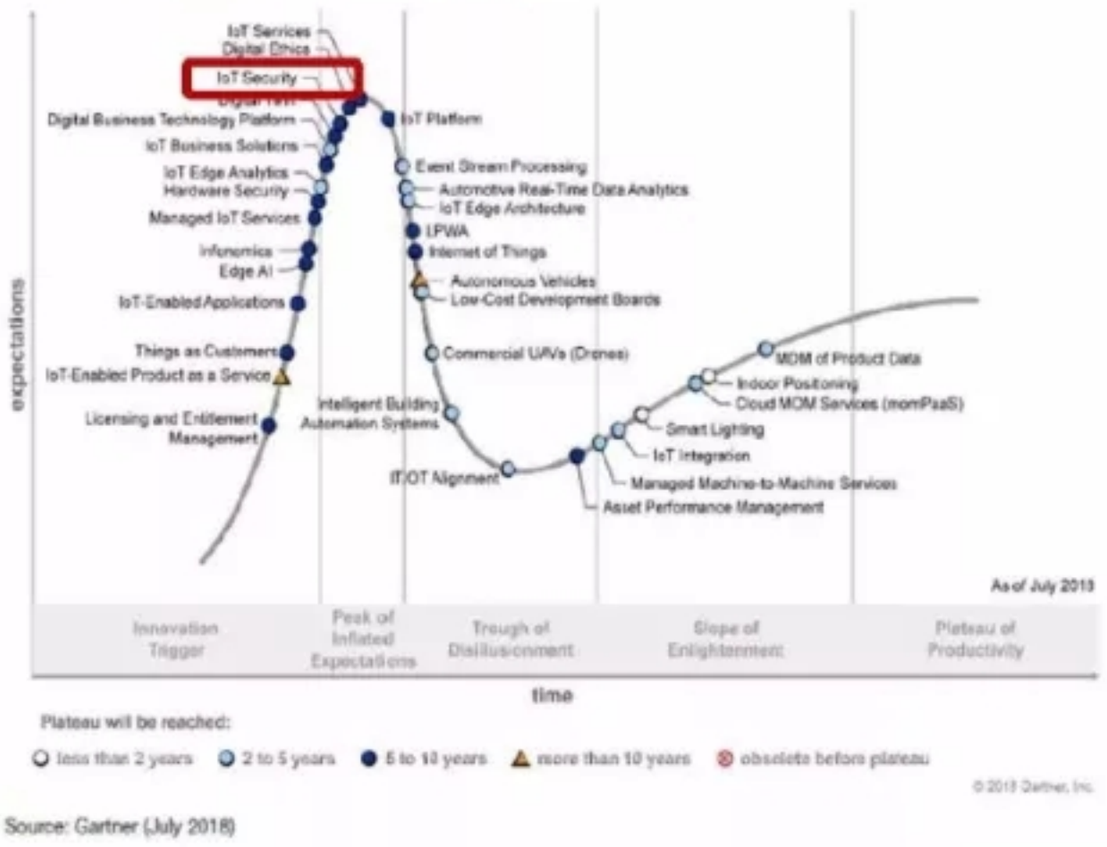
New IoT-Based Vulnerabilities

By 2020, over 25% of identified attacks in enterprises will involve IoT, although IoT will account for less than 10% of IT security budgets.

The exploit market and hacking community have been focusing on the low-hanging fruit and most prevalent systems, which is why Microsoft has been a bigger target than Apple. The increasing opening up of OT systems, as well as the popularity of IoT initiatives (such as smart cities), along with expected growth of mobile threats, will bring a new dimension to cybersecurity.

Gartner 物联网安全预测

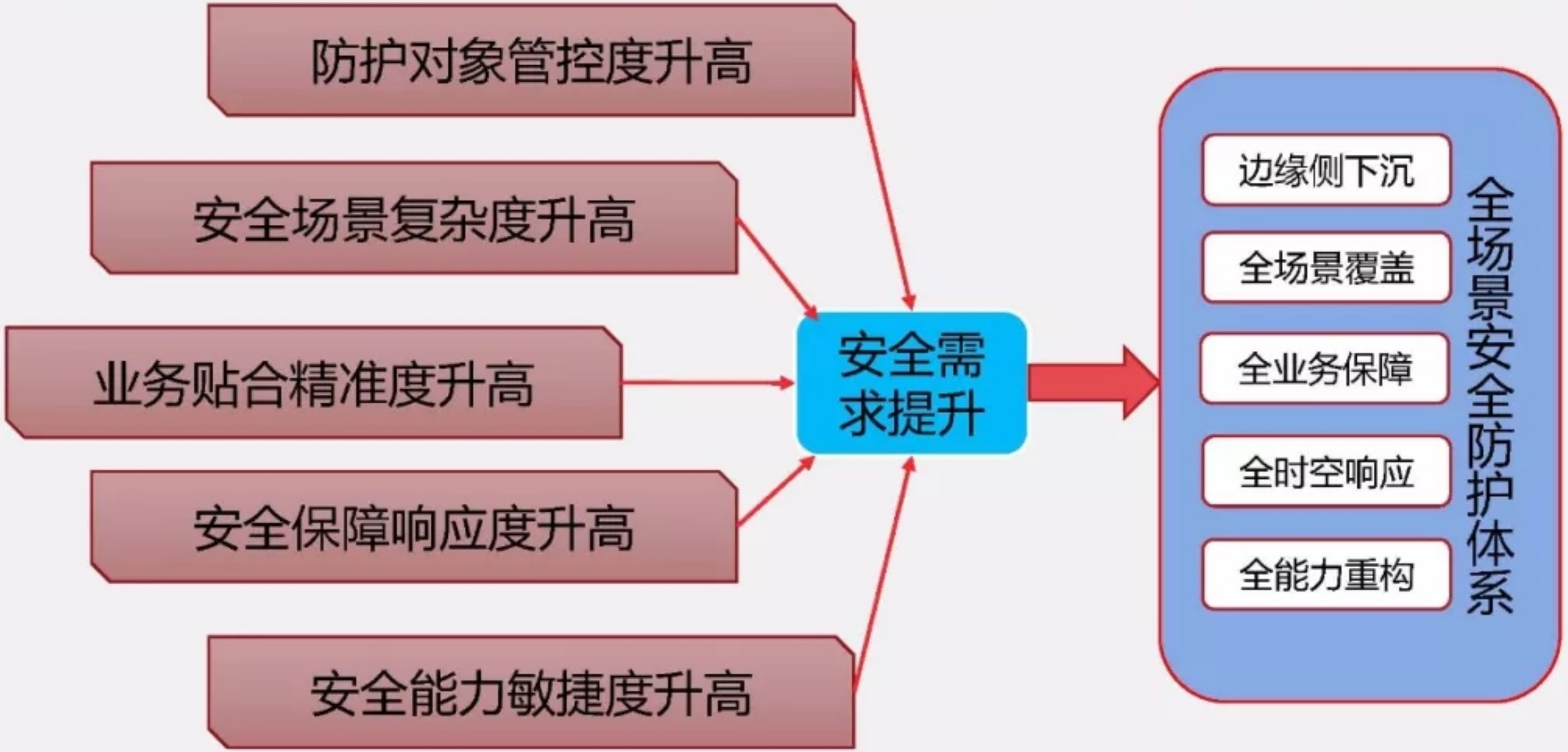
Figure 1. Hype Cycle for the Internet of Things, 2018



Source: Gartner (July 2018)

Gartner2018 物联网技术成熟度曲线

泛在电力物联网安全需求



目录

1 • 泛在电力物联网安全风险与安全需求

2 • 感知终端层安全风险分析

3 • 动态安全管控与主动防御机制

感知终端可信接入

该部分终端**硬件及软件**系统均**无法定制改造**，具备网络通讯接口（或通过其它接口可转换）。定制微小型**密盒串接**实现安全认证、传输。

该部分终端具有**智能系统**以及标准**TF接口**，具备网络通讯能力（多为4G）。植入安全定制**APP**，加配**国密TF卡**，实现安全认证、传输加密。

该部分终端具有**桌面操作系统**以及标准USB**接口**，具备网络通讯能力（多为网线）。植入安全定制**客户端**，加配**国密USBKey卡**，实现安全认证、传输加密。

该部分涉及**公共WIFI**接入场景，可为外网巡检场所，也可以为内网机房巡检区。通过部署**安全AP及AC**的方式，实现WIFI安全接入。

感知终端持续监测

基于设备指纹库的审批机制及检测

通过网络发现建立起一套指纹库，经过管理员审批后，一旦设备被冒用，会自动发现并禁入（串联、旁路均可），支持与交换机联动；

基于行为建模的异常行为分析

对终端行为逻辑基于自学习进行建模，对异常行为进行分析；

基于协议白名单的访问控制

物联网私有协议内容结构深度自定义，PAYLOAD级别过滤自定义匹配，实现网络传输内容的白名单化；

基于PKI的强身份认证、加密接入（终端集成软件时）

与终端软件配合，对可安装客户端的终端可实现进一步的强接入控制；

积极安全研究成果

华为首次将IoT设备安全纳入到漏洞奖励计划中，多家安全实验室和高校参与了此次终端IoT奖励计划上线活动，**仅启明星辰ADLab提交的漏洞符合本次活动要求，发现并协助华为修复了IoT产品中的多个严重安全问题，为其终端IoT产品安全提供了有力的支持。**

- 智能摄像头
- 智能插座
- 智能家电
- 无线门锁/报警器
- 其他智能设备……

Venustech

THANKS!

谢谢观看

启明星辰集团