

网络安全

你的 ICS 被侵入过吗？

漏洞一般定义为系统或程序“缺陷”，它利用系统的漏洞使系统易受攻击和恶意刺探，以 ICS 为攻击对象的恶意软件是一种手写代码，专门攻击 ICS 系统。

文 | Chris Sistrunk, Mandiant 资深 ICS 安全顾问

许多人都知道企业网络有安全漏洞，但是为什么没有听说许多工业控制系统（ICS）被侵入？其实有时系统已被突破，但企业经营者并不知道，因为他们自己没有安全工具和安全人员。

自从 2010 年 Stuxnet 出现以来，工业控制系统（ICS）漏洞研究、恶意刺探和恶意软件报告越来越多。而且，越来越

越多控制系统已经联网，这使攻击者有机可乘，所有这些只需一个有目的的攻击者！

根据 NCCIC/ICS-CERT 的 2014 年回顾（来自国家网络、通信集成中心和美国国土安全部的工业控制系统网络应急响应小组），攻击者看起来好像越来越猖獗了。去年，ICS 经营者共报告了 245

起网路事故，其中 79 起发生在能源部门。攻击者肯定不关心你是否已经升级到北美电力可靠性公司，他们只关心他们想要的东西，他们是有组织、有资金支持的专业人士。如果你把他们击退，他们马上就会回来。

如果 ICS 这么不堪一击，为什么我们没有发现更多攻击呢？可能因为我们根本没注意到！IT 领域可能有人盯着企业网络，但是大多数企业并不是经常关注控制系统网络流量模式和日志。如果一家公司有一个安全运行中心（SOC），但它未必和 ICS 相连，这意味着公司只能预防一部分业务免受攻击。所以，面对层出不穷的 ICS 漏洞和恶意软件、安全性不高的 ICS 设备、不放过每一个部门的攻击和不可避免的侵入，以及越来越多的政府法规，ICS 运营者还能怎么做？本文解释了工业控制系统网络安全监控（NSM）怎样帮助探测攻击和对攻击做出响应，这样你就无须按照法律要求硬着头皮学习这些东西了。

网络安全监控

网络安全监控即“收集、分析、升级警报迹象来发现并应对侵入，NSM 是一个在侵入者对企业造成损失前就能发

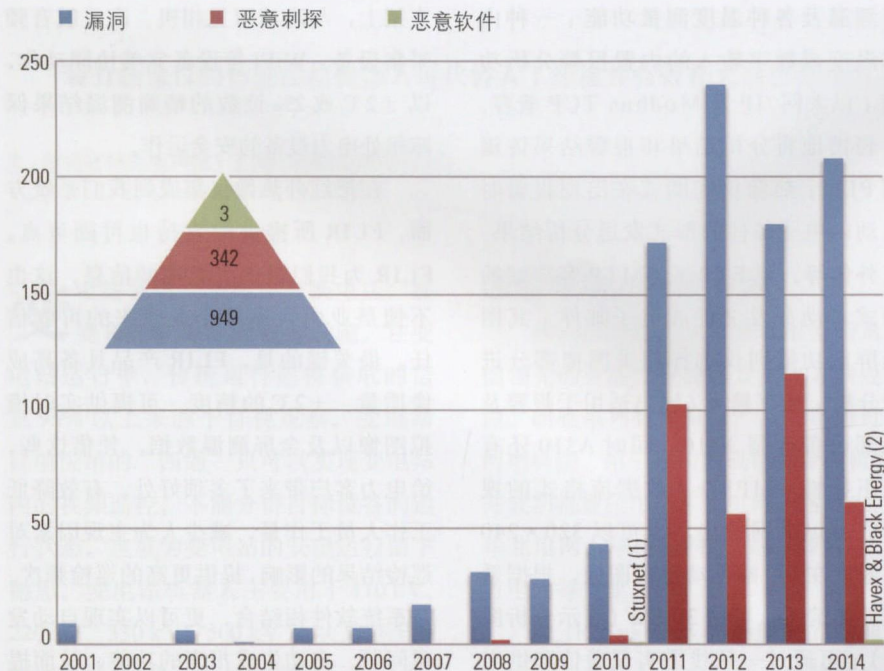


图 1 众所周知的 ICS 漏洞、刺探和恶意软件，该图表的数据是截止于 2014 年 12 月 31 日的年度全球数据，由作者汇总而成

现网络侵入者的方法。” Richard Bejtlich (FireEye 首席安全战略官) 的《网站安全监控实践》中有这样一句话。

1986 年，劳伦斯伯克利国家实验室的一名系统管理员，即前宇航员 Cliff Stoll 使用监测技术来寻求一个从国家实验室盗取信息，并卖给克格勃的黑客。Stoll 和其他一些人在 1988 年的劳伦斯利弗莫尔国家实验室 Todd Heberlein 及其团队完成了一项重要发明，这篇文章的目的是说明这些工具和技术可以用来防止 ICS 受到攻击。

NSM 的成功取决于两个要素。至少有一个以质疑的态度和适当的工具来收集、分析数据，同时追踪攻击者。收集日志和数据、检测异常、进行异常分析，这是一个 NSM 周期。安全分析师的日常工作就是盯着侵入的异常迹象不放，目标是使发生和发现侵入之间的间隔尽量缩短。

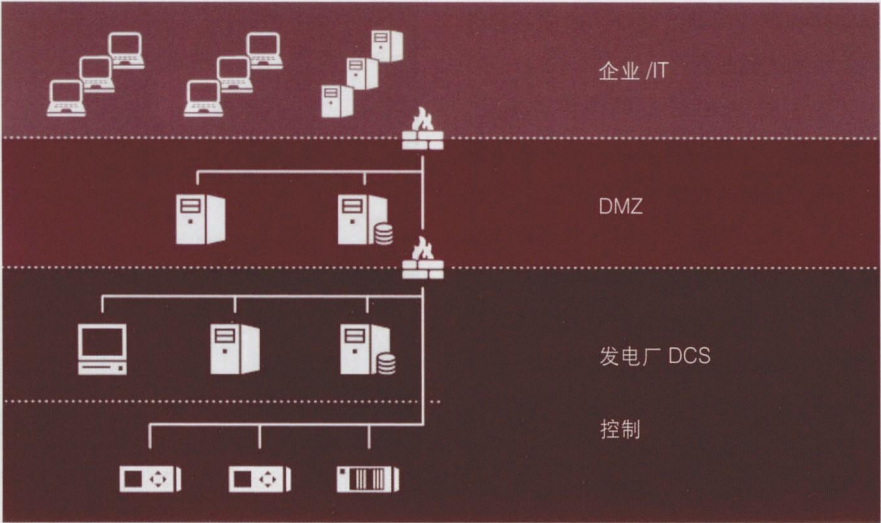


图 2 发电厂架构图示例

隔尽量缩短。

必须了解 NSM 对 ICS 系统进行的 是被动收集，而不是主动扫描，因为我们知道后者会导致严重后果。在主动扫

描时，系统使用软件来探测网络，发现设备、开放端口，甚至漏洞。但如果不能正常完成任务，主动扫描方式可能导致控制系统设备故障。被动收集是监测

GET IN TOUCH



拥有百年历史的德国RAFI公司作为人机界面的创新引领者，从按钮开关等电子元件到整个操作控制系统，我们一直以客户为中心，为其在全球范围内提供优秀的解决方案。

RAFI产品一直以其优秀的质量品质和安全性能著称，并广泛应用于机械制造业，自动化控制，汽车工业，轨道交通，起重和传动，电器设备，医疗器械等行业。

针对亚洲市场，RAFI公司于2008年在上海成立了其独立子公司，纳安斐电子（上海）有限公司，我们遵照集团理念，针对亚太市场和客户的不同需求，为您提供合适的解决方案。

RAFI

纳安斐电子（上海）有限公司
上海市虹梅路1535号星联科研大厦1号楼606-608室

电话：+86-21-5178 2528
传真：+86-21-5178 2527

电邮：info@rafi-electronics.cn
网址：www.rafi-electronics.cn

▲反馈服务编码M5115

以太网和串行网络的流量，这样不会影
响控制系统设备。

为了对 NSM 进行网络被动监测，
至少需要一个网络传感器，将网络流量
复制到传感器。许多组织已经在正常 IT
网络上开发了网络传感器，但这些传感
器并不一定始终适合控制系统环境。

如果你正在考虑在 ICS 上安装一部
NSM 传感器，我强烈建议你从实验室环
境开始，而且和所有重要的 ICS 利益相
关者合作，例如安全操作部门、工厂业
务部门、工程部门，甚至 ICS 供应商。
ICS 环境的 NSM 传感器必须考虑流量和
速度、物理环境以及传感器需要加入的
协议。

传感器的软件平台对于满足这些
需求来说必不可少。市场上有一些针对
ICS 新开发的商用平台，它们能收集数
据，并显示在仪表板上，供分析师进行
分析，对 ICS 协议进行深层数据包检测，
甚至绘制一幅网络图。

位置传感器非常重要，这样分析师
才能看到 ICS 网络的周边和重要的内部
系统网络。传感器应该连接一个有镜像
功能的原有交换机端口，或安装一个专
用网络。甚至可以被动监控基于串口的
流量。最后，别忘了保证传感器和收集
到的数据的安全。

功能最全的一种 NSM 传感器是一
个完整的数据包捕获类 (PCAP)，它像
一个电话录音机。通过它的记录，你能
弄清到底发生了什么事。因为许多 ICS
网络与 IT 系统相比，带宽较低。接下
来的数据是会话数据，就像话费账单记
录，上面记录着谁是主叫和每次通话时
长。会话数据对存储空间利用要少于
对 PCAP 的利用。

ICS 网站安全监控的优势

在他的书中，Bejtlich 谈到几个在 IT
网络中执行 NSM 的缺点，例如需要高带
宽、加密和移动设备。事实证明，ICS 网
络中不存在这些缺点，因为 ICS 通常带
宽较低，使用静态设备，流量不加密。

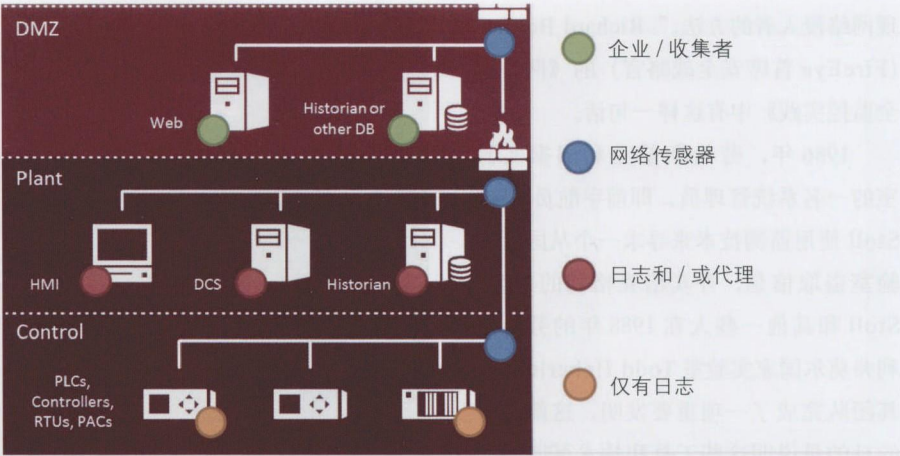


图 3 配有网站安全监控系统的发电厂网络架构图

发电厂经营者面临一些问题，包括
控制系统组件老化，安全性很低或完全
没有补丁或升级很难执行。NSM 是监测
和保护重要控制系统组件的最好方法。
当设备最后成功升级，NSM 仍然可以被
用来监控新一代更安全的设备，因为我
们知道，可能还会有我们不知道的漏洞
存在。

预期你的 ICS 将被侵入，这比试图
预防每个漏洞更有用。图 2 是一个典型
的网络体系结构。最上面是企业 IT 基
础设施，包括业务系统、个人电脑和
笔记本电脑。接下来是发电厂非军事
区 (DMZ)，其中防火墙用来保护发电
厂数据，例如 Plant Historian。深入核
电站，我们看到一个网络分布式控制
系统 (DCS)，用于涡轮控制、发电厂
平衡、水力发电厂、连续排放监测和
Historian。

攻击者可能会企图从公司网络通过
一个钓鱼邮件，获得发电厂 DCS 的访
问权，侵入一台有时会连到 DCS 组件的
工程笔记本、一个受感染的 USB 驱动器或
通过一个第三方连接通道，例如供货商。
一旦攻击者获得 DCS 的访问权，如果你
没有监控网络，那么你可能不知道你被
攻击。即使后来发现了，也于事无补。

明察企业网络的秘密

你已经选择了一个 NSM 传感器平台，

并在 DCS 组件实验室环境中对它进行了
测试，而且已安排专人负责网络监控。要
收集什么数据，从哪里收集？你开始监
控一些 NERC/CIP 发电厂，还是所有发电
厂？让我们用一个网络图举例说明，而
且我们要在图上添加 NSM。你要决定是
否将 NSM 的数据发送到现有的企业 SOC
或一个用于监控控制系统的新 SOC。

在 DMZ 这个例子中，有一个 Web
服务器和一个 Historian，它们很可能运
行在能运行杀毒软件或设置白名单的现
代服务器中，甚至安全代理端点保护软
件上。所有这些都曾用于 IT 系统，所以
必须收集所有的日志。接下来我们用网
络传感器来捕获和分析每个网站的流量。
在工厂网站的 DCS 部分，服务器可能只
提供 Windows 日志或 Syslog。你可能需
要安装一些设备的端点保护，但这通常
需要供应商的批准。最后，如果 PLC 和
其他控制器上保存着任何日志，也需要
收集起来。

今天，你可以执行网络安全监控，
而且不会影响工厂运营。有许多免费工
具能帮你开始监控 ICS 和寻找异常。人
是防御系统中最重要的部分，可以收集
数千兆的字节和成千上万的 IDS 警报，
但没人进行说明的话，他们一无是处。
记住，敌人是“人”而不是“东西”，
他们不在乎你是否满足 NERC/CIP，不
要等到惹上法律麻烦才开始监控你的工
厂。MM