AhnLab

安全月刊

2016.06 Vol. 43

关键基础设施的安全威胁

揭开攻击社会基础设施的恶意软件实体

去年4月，韩国全罗南道丽水市的某个公交车站的公交车到达信息指南系统被黑客入侵，信息显示屏播放了色情视频近40分钟。最近，美国也发生了类似的事件。德克萨斯州高速公路的电子屏幕被黑客入侵，整个晚上屏幕出现了嘲笑总统候选人特朗普的字样等。这两事件虽然都没有发生经济损失，但是交通设施被黑客攻击这一点需要注目。如果是交通信号等控制系统，或者是机场、铁道、发电站的系统被黑客攻击的话，真是不敢想象会导致什么样的结果。
本文通过国内外主要社会基础设施被攻击事件，研究这些事件对社会基础设施安全给予的启示。

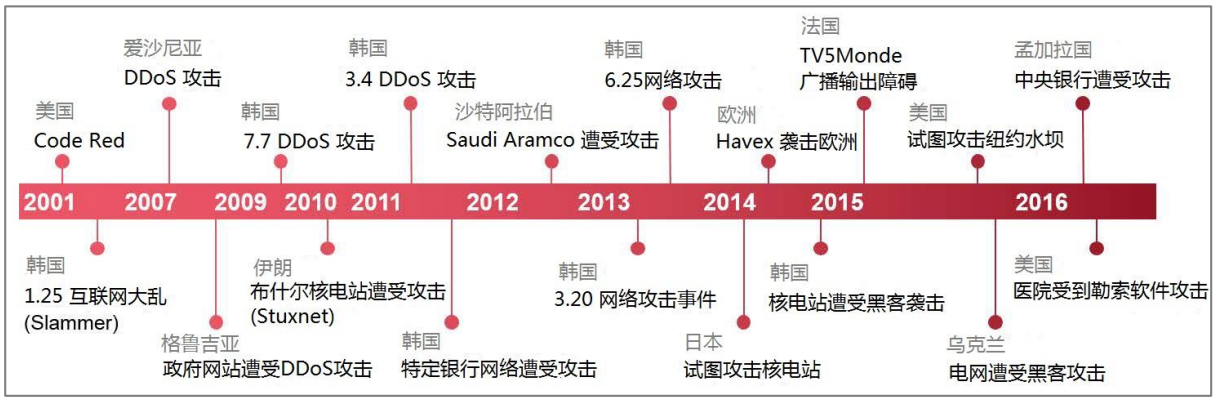
社会基础设施被称为“基础设施”、“社会公共基础设施”等，是指为社会生产和居民生活提供公共服务的物质工程设施，是用于保证国家或地区社会经济活动正常进行的公共服务系统。最近，学校、医院和公园等的社会福利和生活环境相关的设施也被分类到社会基础设施。
这些设施或系统是维持社会的基石，如果被黑客攻击受到损害，导致的问题不仅仅是财产上的损失，而且还引起社会混乱、人民安全受到威胁，进而可能严重威胁到国家安全。2012年，全球最大石油公司沙特阿拉伯国家石油公司（Saudi Aramco）遭受黑客攻击。2015年，乌克兰电网遭受黑客攻击，导致成千上万的家庭供电被迫中断。这两个事件不仅导致了莫大的财产损失，还导致了人们生活极大不便，进而引起了社会混乱。
美国国土安全部（Department of Homeland Security）将社会基础设施分为16个主要领域。其中，食品、农业服务除外的14个领域存在的主要安全风险分类如下【表 1】。

领域	网络安全威胁
化学	• 化学产品工程管理的网络系统
通信	• 攻击通信系统来阻碍国际连接 • 通信基础设施受到影像
主要生产设施	• 控制系统及数据库被攻击
水坝	• 水坝控制系统被攻击
国防工业	• 对安全基地的DDoS攻击 • 系统误操作等泄漏国家安全机密
应急服务	• 应急服务通信系统和网络、GPS被攻击
能源	• 电气：电力电网及运营设施被攻击 • 石油及天然气：能源管理系统被攻击
金融服务	• 泄漏金融信息机关的个人信息 • 金融系统遭受攻击，导致大规模金融损失
政府设施	• 自动安全管理系统及数据库被攻击 • 政府设施系统遭受攻击， 机密和个人信息被泄漏
医疗保健及公共医疗	• 医院处方系统遭受攻击，医疗保险、诊疗记录被泄漏
IT 设施	• IT系统管理、内容、信息、通讯等多种领域信息被泄漏 • 身份验证系统遭受攻击，社会基础系统运营受到威胁
核电及处理设施	• 核设施控制系统被攻击
交通	• 陆、空、海上交通控制系统被攻击
水利资源及水利处理系统	• 水利资源及水利控制系统被攻击

【表 1】美国国土安全部的社会基础设施安全威胁分类

世界主要的社会基础设施遭受攻击事件

2000年初开始就已经存在针对特定国家或社会基础设施的恶意软件。2001年7月，美国白宫网站发生了由 CodeRed 蠕虫引起的 DoS 攻击。韩国在2003年1月25日，发生了 Slammer 蠕虫引起的互联网障碍，该事件被称为“1.25大乱”。



【图 1】世界主要社会基础设施遭受攻击事件

针对社会基础设施的网络攻击白热化从2000年中后期开始出现。2007年4月27日，爱沙尼亚（Estonia）共和国的重要网络基础设施，包括国会、总统府、总理办公室、央行、主要媒体报社等都受到 DDoS 攻击。此次攻击导致了包括总统府的国会、政府机关、银行、移动通信等爱沙尼亚的整个国家系统瘫痪了长达三周的时间。

2008年6月，格鲁吉亚（Georgia）政府网站遭受了大规模的 DDoS 攻击，攻击时间平均2小时15分钟，最长6个小时，导致政府网站、国家银行等许多重要网站24小时中断服务。

2010年开始出现了不是单纯导致服务障碍的攻击，而是针对社会基础设施的直接攻击。最为代表的事例是2010年6月发现的 Stuxnet 病毒。 Stuxnet 蠕虫病毒（超级工厂病毒）是世界上首个专门针对工业控制系统编写的破坏性病毒，能够利用对 windows 系统和西门子 SIMATIC WinCC 系统的7个漏洞进行攻击。特别是针对西门子公司的 SIMATIC WinCC 监控与数据采集（SCADA）系统进行攻击。该病毒在2010年9月造成伊朗核电站瘫痪。

针对能源领域的另一个攻击事例有2012年在沙特阿拉伯发生的 Saudi Aramco 被攻击事件。同年8月27日，媒体报道了卡塔尔天然气公司（RasGas）遭受病毒攻击事件。2015年，乌克兰电网遭受黑客攻击，导致成千上万的家庭供电被迫中断。

就像乌克兰的停电事件，最近由于针对交通、航空和电力设施的网络攻击，导致一般市民的生活不便，甚至有时受到严重损失。巴西南部的一个城市公交车站的电脑系统被黑客入侵，信息显示屏播放色情视屏近15分钟，另旅客侧目。航空设施也不例外。去年6月，波兰国家航空公司的地面计算机系统遭受 DDoS 攻击，飞行计划系统瘫痪5个小时，导致超过1,400位的乘客被迫停留在机场。这是全球首次针对航空公司计算机系统的网络攻击。

【图 2】被黑客入侵的巴西公交车站信息显示屏（*来源：SecurityWeek）

此外，法国电视台 TV5Monde 遭到网络攻击而导致大量的信息传输中断长达数小时的事件，以色列电视台遭受攻击事件，2013年韩国主要银行和电视台网络遭受攻击事件，孟加拉国中央银行遭受攻击事件，美国纽约水坝电网被攻击事件，美国医院受到勒索软件攻击事件等，针对社会基础设施的攻击在各个领域持续发生。

揭开攻击社会基础设施的恶意软件的实体

在前面谈及的事例中，详细解析乌克兰电网被黑事件和 Saudi Aramco 被黑事件，了解实际针对社会基础设施的攻击中利用的恶意软件和攻击方式。

1. 乌克兰电网遭受黑客攻击

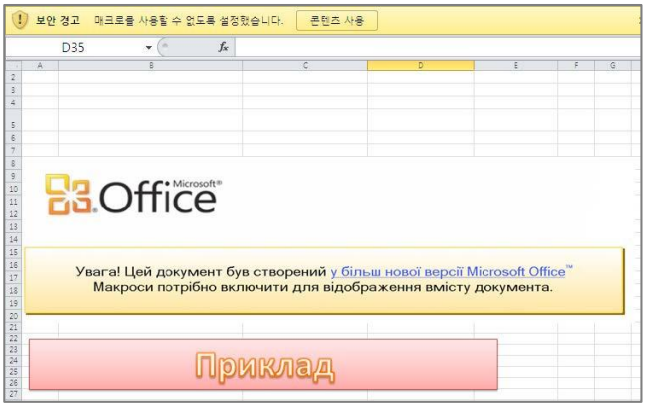
2005年12月23日，乌克兰的 Kyivoblenergo 发电站发生问题，导致当天下午4点35分开始3个小时停电，造成约8万个家庭陷入一片黑暗。这是有史以来首次导致停电的网络攻击。另外在乌克兰西部地区的 Prykarpattyaoblenergo 发电站也发生了问题，同样导致大规模停电事件。甚至通信系统也发生了障碍，无法正常通信。停电后，媒体和乌克兰国家安全部就对两次停电事故谈到了网络攻击的可能性。

网络攻击导致乌克兰连续发生停电事故，美国政府也开始着手相关调查。今年1月，美国国土安全部发表，乌克兰的停电事件是由网络攻击造成的，3月18日公开了附加相关分析报告。根据该报告，攻击者已在6个月前开始入侵到发电所内部系统并收集相关信息，开发恶意的固件(Firmware)等做好彻底的准备后再执行了攻击。

与此相关，SANS ICS 团队和斯洛伐克杀毒软件公司 Eset 表示，本次攻击和被称为黑暗力量（BlackEnergy）的恶意软件有密切关系。另外，停电事件发生一个月前的2015年11月，乌克兰的 CERT 中心曾在乌克兰选举期间谈及过有关 BlackEnergy 恶意软件。因此，可以预想到，针对乌克兰的 BlackEnergy 攻击是从停电事件以前就开始进行的。

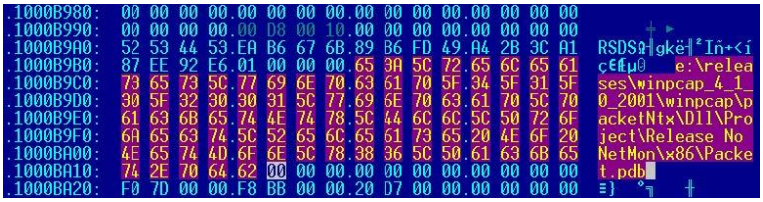
BlackEnergy 并不是最近兴起的新型恶意软件，它最早出现在2007年，由俄罗斯的地下黑客组织开发并广泛使用在 BOTNET，主要用于建立僵尸网络，对特定目标实施 DDoS 攻击 。此后，2008年的格鲁吉亚政府网站被攻击事件也使用了该恶意软件。特征是以驱动程序文件构成，目前也持续出现其变种。

BlackEnergy 恶意软件是由释放恶意软件的 Dropper 和实际执行恶意行为的代码混淆的驱动器文件构成，并创建 FONTCACHE.DAT 等文件。另外，该攻击利用了带宏病毒的 Excel 文档。打开 Excel 文档的用户若选择安全警告信息的“使用内容”选项，宏即被运行。宏代码释放一个 vba_macro.exe 文件到%temp%文件夹。



【图 3】 利用在乌克兰电网攻击的Excel文档的宏功能

Vba_macro.exe 又会创建 FONTCACHE.DAT 文件。该文件伪装成 WinPcap 和相关文件。内部字符串也伪装成 WinPcap 相关文件。



【图 4】 伪装成 WinPcap 相关文件

2. Saudi Aramco 遭受黑客攻击

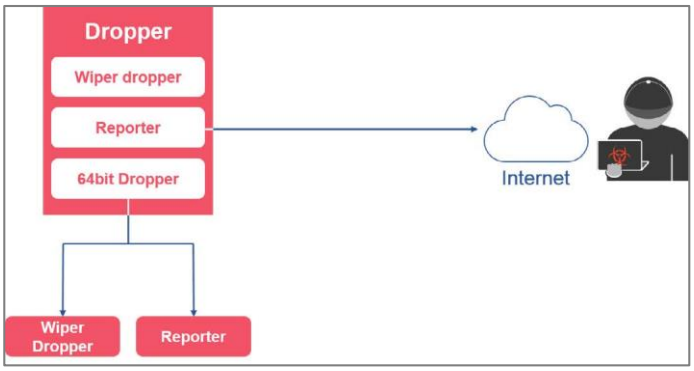
2012年8月15日，世界最大的石油公司沙特 Saudi Aramco 遭受网络攻击，大约3万台的系统发生障碍。当天就有一个自称为“正义之剑(Cutting Sword of Justice)”的团体主张此次攻击是他们所为。

We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.

Cutting Sword of Justice

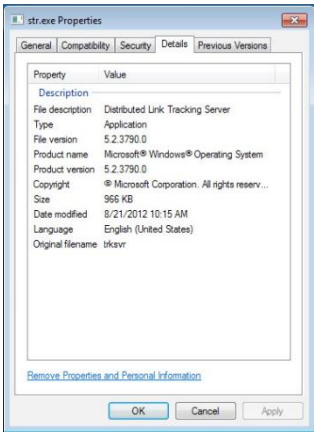
【图 5】 对于 Saudi Aramco 攻击的“正义之剑(Cutting Sword of Justice)”的主张

Saudi Aramco 攻击使用的恶意软件被称为“Shamoon”或“Disttrack”，这种病毒的攻击目标是能源企业或能源部门，它能将受感染 Windows 机器中的数据永久删除。



【图 6】 Shamoon 恶意软件结构

Shamoon 恶意软件的结构如【图 6】所示。Dropper 的作用是将破坏硬盘的恶意软件释放到系统，仅具有删除数据功能和报告功能。查看文件属性，会发现它伪装成微软制作的文档，说明栏显示“Distributed Link Tracking Server”。



【图 7】 Shamoon 恶意软件的 Dropper 登记信息

数据破坏文件具有如 C:\Shamoon\ArabianGulf\wiper\release\wuper.pdb 的PDB信息。从字符串“ArabianGulf”可以猜想是一种具有明确攻击对象的恶意软件。

【图 8】PDB信息包含的特定字符串

当运行数据删除文件，驱动器文件（drdisk.sys）将被生成，得到一个文件列表。此后，以 JPEG 图像覆盖系统存在的所有文件。最后，覆盖硬盘 MBR 使无法使用系统，使用“shutdown -r -f -t 2”结束。该恶意软件还具有报告功能，如报告被害系统数等信息。

有关社会基础设施安全的提示

去年末，包括 AhnLab 在内的很多安全厂商在2016年安全预测中，提出了“网络恐怖行为及国家基础设施安全威胁”是2016年有可能发生的安全威胁。随后2016年初开始发生了一系列基础设施被攻击事件，如“孟加拉国中央银行被攻击”、“韩国公交车站信息显示屏被攻击”等事件。

社会基础设施是形成社会基础的重要的设施，因此要伴随着强有力的安全策略。但是很多时候是“安全人员不足”或“安全人员缺乏专业性”等情况。另外，设施的系统本身就没有考虑安全而设计，或者系统本身就存在漏洞。这些都是基础设施容易成为黑客攻击目标的一个因素。

如要从外部的威胁中安全保护社会基础设施，首先要树立具有现实性的安全策略，使每个成员都可以遵守。与此同时，还要构筑适合企业环境的安全系统，监控和拦截入侵到内部系统的安全威胁，并分析和响应内部扩散的恶意软件。恶意软件入侵到内部系统到扩散、破坏系统、造成恶意结果需要一定的时间。一般，掌握数多的内部系统并一一了解系统需要6个月的时间。因此，为了防止攻击导致的损害，必须对主要系统进行定期检查，迅速掌握异常征兆。这就需要具有专业性的安全专家。另外，还需要具备对合作厂商的强有力的安全方案。因为，攻击者有可能不直接攻击入侵相当麻烦的社会基础设施，而攻击合作厂商后，通过合作厂商再攻击社会基础设施。

参考资料
- Data breach digest. (http://www.verizoneenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf)
- Analysis of the Cyber Attack on the Ukrainian Power Grid (https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)
- 铁道安全及维护管理现状审查结果 (http://gov.seoul.go.kr/archives/86261)
- 审计院，'国家网络安全管理现状 ' (http://www.bai.go.kr/bai/index.do)
- Kang,EnSung，‘网分离是万能药?’ (www.ciokorea.com/news/25437)
- 美国国土安全部 'Sector Risk Snapshots’ (https://www.hsdl.org/?view&did=754033)
- http://www.securityweek.com/hackers-broadcast-porn-tv-screens-brazil-bus-depot
- http://africanspotlight.com/2015/08/08/hackers-broadcast-porn-on-tv-screens-at-brazil-bus-station-photos
- https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=200908100021
- https://en.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War
- http://www.economist.com/node/17147818
- http://money.cnn.com/2015/08/05/technology/aramco-hack
- http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html
- SANS : https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered
- Ukraine CERT: http://cert.gov.ua/?p=2370
- http://www.mta.go.kr/policy/its/management_sign.jsp
- http://www.ittoday.co.kr/news/articleView.html?idxno=42719
- https://securelist.com/blog/incidents/57854/shamoon-the-wiper-copycats-at-work/

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com