第113篇：俄乌网络战之一，沙虫APT组织致乌克兰第1次大停电事件复盘 | CTF导航

Archived: 2026-04-05 14:54:32 UTC

第113篇：俄乌网络战之一，沙虫APT组织致乌克兰第1次大停电事件复盘

Part1 前言

大家好，我是ABC_123。好久没有和大家分享“画出整张流程图”的APT攻击事件了。结合当前俄乌战争题材，今天和大家分享俄乌网络战中的APT攻击事件导致乌克兰3次大停电的第一次事件。关于其中的技术细节，网上的各种文章说法不一，部分文章还有错误。这次ABC_123参考了赛门铁克、ESET等国外安全公司的几十篇分析报告，综合整理形成此篇文章，希望能给大家带来一些对网络战的一些启示。

第113篇：俄乌网络战之一，沙虫APT组织致乌克兰第1次大停电事件复盘

Part2 技术研究过程

- ### 乌克兰第一次大停电攻击流程图

在参考几十篇APT分析报告之后，ABC_123总结出如下流程图。2015年12月23日，当地时间15时左右，**沙虫APT组织利用鱼叉式钓鱼攻击，通过投递带有宏恶意代码的Excel邮件附件，成功控制乌克兰国家电网某工作站人员的电脑**。之后在乌克兰电网内部网络潜伏长达6个月至1年，通过植入的恶意软件**BlackEnergy3（黑色能量3）**，远程控制电力系统的SCADA节点，发送指令断开多做变电站的电路连接。与此同时，沙虫APT组织还发动了**电话拒绝服务（TDos）攻击**，导致客户服务电话被占满，受害人群无法及时告知断电情况。

第113篇：俄乌网络战之一，沙虫APT组织致乌克兰第1次大停电事件复盘

这次攻击导致乌克兰首都基辅部分地区及乌克兰西部伊万诺-弗兰科夫斯克地区的**140万人受到停电影响，停电持续约6个小时**。据统计，共有3个地区的电力系统受到恶意软件的破坏，影响范围覆盖全国超过一半的地区。其中，乌克兰Kyivoblenergo电力公司因遭入侵，导致7个110kV变电站和23个35kV变电站发生故障，直接造成约8万用户断电。同一时间，乌克兰境内多家能源公司也遭受了网络攻击，进一步加剧了社会混乱。这次事件成为全球首次具备“信息战”特征的重大停电事故，揭示了网络攻击对关键基础设施的严重威胁。

- **沙虫APT组织发动攻击的背景**

俄罗斯和乌克兰在东部地区的冲突由来已久。2014年，俄罗斯通过军事行动吞并了乌克兰的克里米亚半岛，并随后在当地组织了一场公投，宣布克里米亚加入俄罗斯联邦。这一事件使得乌克兰与俄罗斯的矛盾进一步激化。作为回应，2015年11月22日凌晨，**乌克兰对克里米亚地区实施了全面断电，导致近200万居民的日常生活受到严重影响**。随后，沙虫APT组织对乌克兰境内的电网公司发动攻击，导致140万多万乌克兰居民停电。

- **发动鱼叉式钓鱼攻击**

沙虫（Sandworm）APT组织通过一封主题为“乌克兰总统对部分动员令”的邮件，针对乌克兰境内的电力公司员工实施了鱼叉式钓鱼攻击。**沙虫APT组织将钓鱼邮件的发件人地址伪装成乌克兰议会官员**，欺骗受害者下载并打开了载有BlackEnergy3的恶意代码的Excel宏文档，并根据诱骗提示启用宏功能。当恶意Excel文件被打开之后，内嵌的宏代码会在系统的临时文件目录释放文件vba_macro.exe，然后立即启动执行。vba_macro.exe作为下载器，将BlackEnergy恶意程序释放到目标主机并执行，同时与攻击者的命令与控制（C2）服务器建立连接。该攻击通过社会工程学手段而非软件漏洞实施，旨在诱骗受害者启用宏功能。

如下图所示，2014 年 5 月 12 日星期一，第一次攻击针对乌克兰国家铁路运输管理局管理的所有六条铁路，攻击者对铁路运输领域相关的乌克兰企业发送鱼叉钓鱼攻击。邮件附件是一个可执行的PE文件，图标被伪装成了MS Office Word的图标。**发件人被修改为政府官方的邮件地址，使得正文内容更加可信**。表明早在 2014 年 5 月，即乌克兰地区配电公司的“十二月事件”发生一年半多之前，BlackEnergy2/3 恶意软件就已交付（试图交付）到受攻击的能源设施。这是 BlackEnergy 的轻量级“Lite”版本，除其他外，它能够收集受攻击对象的相关信息，为后续攻击提供支撑。

2014 年 8 月 13 日左右，沙虫APT组织通过包含 0day 漏洞（CVE-2014-4114）的PowerPoint文件，结合BlackEnergy2/3恶意木马实施攻击，这些恶意电子邮件一如既往地使用高度相关且看似可信的内容作为诱饵文档，意图欺骗受害者打开附件并触发漏洞，进一步实现对受害网络的控制。

如下图所示，2015年3月初的钓鱼邮件，针对乌克兰无线电广播公司的攻击，显著的特点是，邮件中的附件为.xls和.pps的恶意文档，需要启用宏去触发恶意代码。

2015 年 3 月底，国外的一份分析报告记录了两封恶意邮件，这些邮件包含的附件与乌克兰西部一家区域配电公司遭受鱼叉式钓鱼攻击有关。

- **僵尸网络内网信息收集**

在乌克兰第一次大停电事故发生的前期，**沙虫（Sandworm）APT组织通过僵尸网络（BOTNET）体系进行前期侦察和信息收集**，对乌克兰境内的电力系统和能源公司开展了大规模的渗透。攻击者通过多轮鱼叉钓鱼攻击，成功获取了多个乌克兰境内关键基础设施单位的内网访问权限，并在内网中进行了深入的

信息收集，包括电力网络的运行状况、电力系统拓扑架构等关键数据。随后提升了权限，在内网进行横向移动。攻击者利用工具Mimikatz收集凭证，包括内网用户的登录信息。通过查找主机文档、提取浏览器保存的凭证、部署键盘记录器等方式，**沙虫APT组织最终获取了电网员工的VPN账号，该VPN账号可以直接访问电力控制系统的人机界面（HMI）**。后续的溯源调查表明，该VPN账号使攻击者在没有触发安全告警的情况下长期访问目标内网，完成对电力系统的远程控制。

- **操控HMI人机界面**

攻击者通过横向移动窃取电网员工的VPN账号和密码，成功获得了对乌克兰电网SCADA系统的远程访问权限。在进入SCADA/ICS内网后，**沙虫APT组织通过HMI界面手动执行断路器关闭操作**。他们远程操作鼠标，逐步点击HMI界面中的选项，断开了30多个变电站的断路器，这些操作通过SCADA系统的控制信号，直接发送到现场设备，导致断路器实际断开，切断了电力输送，导致大范围电力供应中断。后续的溯源调查显示，在断电操作发生时，一名值班人员正在整理桌上的文件，突然注意到计算机屏幕上的光标不受控制地移动。值班人员眼睁睁地看着攻击者逐步完成断电操作，却无能为力。

如下图所示，这是后续乌克兰工程师拍摄的现场沙虫APT组织远程通过鼠标点击的方式，操控SCADA系统发布断电指令的视频片段。

- **部署SSH后门**

攻击者在内网中部署了SSH后门程序dropbear.exe，这一后门基于SSH协议，攻击者可以通过6789端口与受害主机进行通信。

- **改写备用电源UPS固件**

进入SCADA网络之后，攻击者利用BlackEnergy3黑色能量木马实施进一步破坏。他们上传了新的恶意UPS固件，**导致备用电源（UPS）设备无法正常运行**。这使得电力系统的操作员在停电期间无法获得必要的供电支持，无法在短时间内恢复电力系统的正常运行。

- **改写工控网关设备固件**

此外，攻击者还向串口-以太网网关设备上传了特制的恶意固件。该固件使网关设备陷入不可恢复的状态，无法通过常规方式重启或者修复。这一行为有效阻断了远程对现场设备的控制，即使电力公司成功恢复工作站或其他系统，网关设备的瘫痪依然对系统功能造成严重阻碍。

- **投放KillDisk硬盘数据擦除插件**

攻击者通过BlackEnergy3木马上传了破坏性程序KillDisk（硬盘数据擦除插件）。该程序被设计用于彻底破坏目标系统的数据。攻击者利用KillDisk遍历所有硬盘设备，并直接向硬盘前256个扇区写入零。这一操作清除了SCADA系统主机的系统文件和主引导记录（MBR），同时删除了恶意操作的相关日志和记

录，试图掩盖攻击痕迹。受到破坏的主机不断报错、蓝屏，并在尝试重启时无法恢复正常运行。KillDisk的使用直接导致SCADA系统全面瘫痪，严重影响了电网的运行。

- **TDoS电话洪水攻击**

在乌克兰第一次大停电事故中，攻击者还对电力公司的电话客服系统发起了TDoS（电话拒绝服务）攻击。**沙虫APT组织通过自动拨号设备制造了大量虚假呼叫，导致客服电话长时间处于占线状态**。这一攻击造成了双重影响。一方面，受影响的居民无法通过客服渠道向电力部门报告停电情况，延误了问题的上报和响应；另一方面，电力公司工作人员也无法通过电话渠道了解停电区域的具体情况，进一步阻碍了抢修工作的开展。

Part3 总结

1. 乌克兰第一次大停电事故是世界上第一次网络攻击造成大规模停电事件，展现了沙虫APT组织对关键基础设施的精确攻击能力和隐蔽性。

2. TDoS攻击作为技术性与社会工程结合的手段，加剧了此次电网瘫痪事件的影响，体现了攻击者通过多维度干扰来放大关键基础设施故障后果的能力。

3. BlackEnergy3（黑色能量3）是沙虫APT组织攻击工控系统的重要后门程序，它是dll文件插件化的木马程序。

4. 沙虫APT组织前期主要通过鱼叉式钓鱼邮件发动攻击，而且通常伪造邮件来源地址欺骗受害者下载附件，并且启用恶意文档的宏功能，执行恶意代码。

5. 沙虫APT组织实施的第一次乌克兰大停电事件，主要还是通过窃取员工的VPN账号，然后远程操作HMI人机界面，手工操作来实施断电。

6. 沙虫APT组织至少发动过三次大规模的针对乌克兰电力系统的APT攻击，后续ABC_123会继续为大家分享其中的技术细节，敬请期待。

公众号专注于网络安全技术分享，包括APT事件分析、红队攻防、蓝队分析、渗透测试、代码审计等，每周一篇，99%原创，敬请关注。

Contact me: 0day123abc#gmail.com

(replace # with @)

> 原文始发于微信公众号（希潭实验室）：第113篇：俄乌网络战之一，沙虫APT组织致乌克兰第1次大停电事件复盘

Source: https://www.ctfiot.com/224570.html