

乌克兰电力系统 BlackEnergy 病毒分析与防御

王勇, 王钰茗, 张琳, 张林鹏

(上海电力学院计算机科学与技术学院, 上海 200090)

摘要: 2015年12月, 乌克兰电力系统遭到 BlackEnergy 病毒攻击, 导致伊万诺—弗兰科夫斯克州地区发生多处同时停电的事故, 该病毒也威胁到我国电力系统安全。通过获取不同版本的 BlackEnergy 病毒样本, 构建了分析环境, 发现了 BlackEnergy 攻击方式, 并给出了防御方法。

关键词: BlackEnergy 病毒; 病毒分析; 入侵防御

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00139

Analysis and defense of the BlackEnergy malware in the Ukrainian electric power system

WANG Yong, WANG Yu-ming, ZHANG Lin, ZHANG Lin-peng

(School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China)

Abstract: Ukrainian electric power system suffered BlackEnergy virus attacks in December 2015, resulting in blackout accident occurred simultaneously at multiple areas in Ivano-Frankovsk region, the malware also pose a threat to the electric power system security in China. Based on different versions of samples of BlackEnergy acquired, the attack mode was analyzed and the prevention of the virus was provided under the proper analysis environment.

Key words: BlackEnergy virus, virus analysis, intrusion prevention

1 引言

2015年12月14日, 乌克兰的伊万诺—弗兰科夫斯克州地区^[1]发生多处同时停电的事件, 黑客控制了电力系统, 并远程关闭了电网。紧接着, 2015年12月27日, 乌克兰电力公司网络系统再次遭到黑客攻击, 这是首次由黑客攻击行为导致的大规模停电事件, 据统计, 此次影响导致成千上万的乌克兰家庭无电可用。乌克兰的国家安全

局(SBU)表示, 这起停电是由黑客以恶意软件攻击电网所造成, 2016年1月4日, 安全公司 iSight Partners^[2]表示乌克兰电力系统感染了名为 BlackEnergy 的恶意软件, 并且已取得造成该起大规模停电的恶意程序代码。

在此事件发生后的第一时间, 由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与复旦大学创建的联合分析小组正式启动, 哈尔滨安天科技股份有限公司^[3]对乌克兰电力运行系统

收稿日期: 2016-10-14; 修回日期: 2016-12-30。通信作者: 王钰茗, bubugab@163.com

基金项目: 上海科委地方能力建设基金资助项目(No.15110500700); 上海市浦江人才计划基金资助项目(No.16PJ1433100); 上海自然科学基金资助项目(No.16ZR1436300); 上海科委中小企业创新基金资助项目(No.1601H1E2600)

Foundation Items: The Project of Shanghai Science and Technology Committee(No.15110500700), Shanghai Pujiang Program(No.16PJ1433100), Shanghai Municipal Natural Science Foundation(No.16ZR1436300), Shanghai Science and Technology Innovation Fund for Small and Medium Enterprises(No.1601H1E2600)

和相关样本进行分析后指出，这次乌克兰停电事故是以 BlackEnergy 病毒为主要攻击手段，通过 BOTNET 体系进行前期的资料采集和环境预置的有目的网络攻击事件；将恶意代码通过电子邮件传播，通过远程控制下达断电指令来操控和毁坏 SCADA 系统；同时以 DDoS 服务电话作为干扰，最终感染了至少 3 个地区^[4]电力部门的基础设施，导致发电设备产生故障，引起公众恐慌。

就我国电力系统情况而言，在电力系统中应用最为广泛的 SCADA 系统多以相对封闭网络为主，通过横向隔离装置^[4]进行单比特的校验和单比特的回送确认，像 BlackEnergy 这样的恶意代码很难渗入到电力二次系统。但是，目前国内的电力系统仍然有许多潜在风险，安全威胁主要来自外部与内部 2 个方面：1) 外部威胁，如非授权用户进入控制系统，访问内部资源，造成机密信息泄露、系统控制权被夺取等无法挽回的影响；2) 内部威胁主要集中在自身故障、授权用户对系统的攻击等方面。对此次乌克兰事件，如果在攻击者病毒中加入所需要的控制指令或攻击代码，只要设法将病毒带入系统环境，那么在访问文件或者调用动态链接库时，就会触发病毒，再加入相关的定时器代码，与本地时钟同步后，就可以对电厂发起定时攻击，危害电力系统的运行。

本文通过对 BlackEnergy 样本的分析，简述其攻击过程、恶意破坏行为以及造成的后果，概括了 BlackEnergy 的演变过程及每一代 BlackEnergy 的特点，给出了 BlackEnergy 的漏洞封堵和防御措施。

2 BlackEnergy 病毒简介

BlackEnergy 的雏形最早形成于 2007 年，是一种近年来颇为流行的攻击工具，广泛用于实施网络犯罪活动。

BlackEnergy 已经形成了僵尸网络 (botnet) 体系，它是采集目标节点相关信息的有力工具，通过配置 build_id^[5]的值来甄别受感染的目标，再从中选取较为容易攻破的系统进行内网纵深攻击。经过不断发展，BlackEnergy 开始支持 Rootkit 的技术、组件技术、远程代码执行、采集信息等一列功能，更具有威胁的是，BlackEnergy 可以针对

不同攻击目标，由黑客选择特定的组件组合使用。其更进一步的升级包括支持代理服务器、越过用户账户便能够认证 (UAC) 技术，以及针对 64 bit Windows 系统的签名驱动等。

2.1 BlackEnergy 1

最早的 BlackEnergy 主要用于 DDoS 攻击。它配有一套完整的生成器^[6]，被触发后就会自动生成客户端程序和基于 C&C (指挥和控制) 服务器的命令生成脚本。攻击者使用它建立僵尸网络，只需在 C&C 服务器端下达简单指令，僵尸网络受害主机便会统一地执行这一指令。与众不同的是，这种 bot 并不与僵尸网络 IRC 通信，也看不到任何从这个服务器上发起的攻击。不同于传统的 IRC，这是一个小 (小于 50 kB) 二进制的 Windows 平台使用的简单程序。

2.2 BlackEnergy 2

BlackEnergy 2^[5]依然是一个 DDoS 类僵尸网络程序，但在新的样本中发现增加了加密程序，以欺瞒病毒软件。驱动文件释放后以名为服务方式注入系统进程，随后远程连接服务器，下载攻击插件，根据配置文件对目标发起 DDoS 攻击。

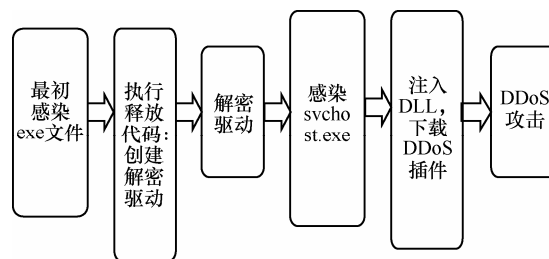


图 1 BlackEnergy 2 工作原理

任何可以接触到 BlackEnergy 2 的人都可以非常容易地利用它发起攻击，而不需要复杂的部署和管理。黑客利用支持升级的组件更容易修改和扩展其功能，只要远程控制中心发布命令，就可以快速实现组件的安装和升级。

BlackEnergy 2 的 3 个主要功能组件是 SYN、HTTP 以及 DDoS 攻击组件^[5]，样本将下载后的攻击组件加载到内存中执行，实现对服务器的远程控制。BlackEnergy 利用 Windows Installer 安装包，将自身的安装程序伪装成名为 msixexec.exe 的系统进程。此版本的最核心功能位于主 DLL 组件。该组件可以根据攻击者的目标定制一个维护

僵尸网络的框架,用于与 C&C 进行通信,同时它本身被隐藏在驱动组件中,文件系统无法察觉。但是主 DLL 组件只提供了一个最小的命令集合。

表 1 为乌克兰病毒变种所支持的命令集合。主 DLL 组件通过一系列的 API 调用和组件进行通信,它为插件产生一些函数调用,同时,插件也依赖导出 2 个函数才能工作。

表 1 乌克兰病毒变种所支持的命令集合

命令	描述
Rexec	Download and execute a binary 下载并执行一个二进制文件
Lexec	Execute a shell command 执行一个 shell 命令
Die	Uninstall 卸载
Getpl	Load a plugin 加载一个插件
Turnoff	Quit (will start again after reboot) 退出 (重启后仍会再启动)
Chprt	Add/remove/set active command and control server 添加/删除/激活 C&C 服务器

2.3 BlackEnergy 3

根据 2014 年 9 月 F-Secure^[7]发布的报告,BlackEnergy 又出现了新的变种,BlackEnergy2 的代码几乎全部被重写而且采用不同的格式对配置数据进行保存。该变种不再使用驱动组件,但目前对该版本的攻击事件还比较稀少。

BlackEnergy3 安装程序的文件名仍为 msisexec.exe,它的释放器会在前台打开一个看似无害的文件,从而悄然释放病毒文件并执行。曾经检测到样本伪装成一个 Adobe Flash 安装程序,它不使用任何欺骗性的文档或应用层程序,而且重启后便不再运行。此版本实现了代理服务器技术、使用 Windows 64 bit 环境下绕过 UAC 和驱动程序签名的相关技术。随着不断地演化,BlackEnergy 不仅可以向 Windows 计算机发起攻击,还对基于 ARM 或 MIPS 架构的路由器和 Linux 系统造成破坏。

3 BlackEnergy 样本分析

3.1 样本获取

在撰写本文时,笔者无法准确得知受害者是如何接收到 BlackEnergy 恶意软件的,但可以合理地推测出是他们在接收包含恶意附件的邮件时感染了该恶意软件。在各方面的努力下,笔者获取了一些 BlackEnergy 样本,通过对其进行分析和

筛选,选择具有典型代表的 BlackEnergy 1 样本和 BlackEnergy 3 样本,并对其分析过程进行详述。BlackEnergy 1 样本带有一个构建器 (builder) 应用程序,生成感染受害者机器的客户端,同时该工具还配备了服务器端脚本,用于构建命令及控制 (C&C) 服务器。这些脚本也提供了一个接口,攻击者可以通过接口控制僵尸机。该工具具有简单易用的特点,即任何人只要能接触到这个工具,就可以利用它来构建自己的僵尸网络。

3.2 分析环境

由于 BlackEnergy 可以影响 Windows 2000、Windows XP、Windows7、Vista 等众多平台,本文对各个平台下的实验结果进行了对比和总结,并简要概括具有代表性的 Windows 平台下的实验过程和结果。为了更好地对 BlackEnergy 样本进行监测,本文所涉及的测试都是在 vmware 虚拟机 Windows XP、Windows 7 系统上进行的。

3.3 BlackEnergy 病毒分析

图 2 为 BlackEnergy 病毒 1.7 版本的生成器界面;修改 Web 服务文件,如图 3 所示;登录 C&C 服务器,界面如图 4 所示;Web 服务器运行界面如图 5 所示。

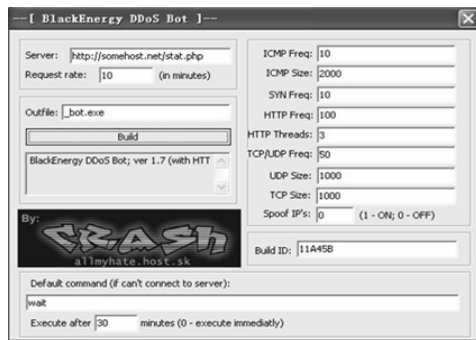


图 2 BlackEnergy 病毒 1.7 版本生成器界面



图 3 Web 服务文件



图 4 Web 服务器登录界面



图 5 Web 服务器运行界面

该 Web 版本服务器将受害者机器相关信息 Base 64 编码后回传到 C&C 服务器中，可以看出 Base 64 解码后的内容就是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，用来甄别受感染个体。Base 64 加密和解密分别如图 6 和图 7 所示。

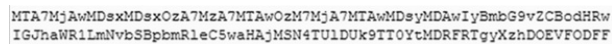


图 6 Base 64 加密

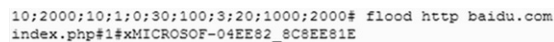


图 7 Base 64 解密

程序在执行后，首先会查看当前系统是否安

装病毒自身。如果没有，程序运行后会释放文件到系统目录下，名为 `mssrv32.exe`，并创建一个互斥量来确保只运行一个程序，并删除自身程序，创建新的线程注入到 `SVCHOST.EXE` 中，联网访问服务器页面。

图 8 为释放文件到系统目录下并创建互斥量的代码。在文件的 `.bdata` 节中，存放着 Base64 编码数据。解码后得到的是生成器的配置信息。如图 9 所示。

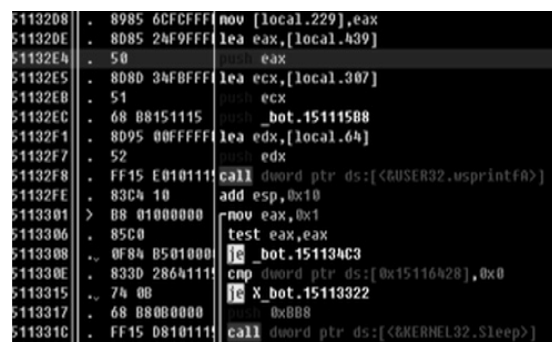


图 8 Ollvdbg 分析结果 1

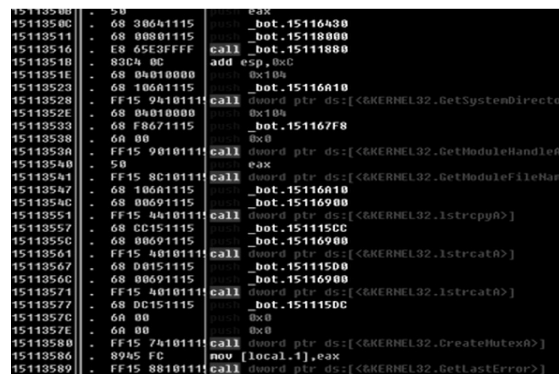


图 9 Ollydbg 分析结果 2

病毒创建一个名为 Microsoft defender update service 的服务，如图 10 所示。使用该名称来欺骗用户启动看似正常的系统安全服务程序，通过该服务程序启动病毒复制自身到 Windows 目录下的 svchost.exe 文件，如图 11 所示，启动命令行的是 svchost.exe -service。



图 10 创建 Microsoft security update service 服务

```

call    ds:strcmpA
push    offset aSvcHost_exe ; "\\svchost.exe"
lea     ecx, [ebp+var_108]
push    ecx
call    ds:strcmpA
lea     edx, [ebp+var_118]
push    edx
lea     eax, [ebp+var_160]
push    eax
push    0
push    0
push    4
push    0
push    0
push    0
lea     ecx, [ebp+var_108]
push    ecx
push    0
call    ds:CreateProcessA
test    eax, eax
jnz     short loc_15112658

```

图 11 Windows 目录下的 svchost.exe 文件

程序运行后会释放文件到系统目录下, 名为 mssrv32.exe, 并创建一个互斥量来确保只运行一个程序, 并删除自身程序, 创建新的线程注入到 svchost.exe 中, 联网访问服务器页面。如图 12 和图 13 所示。

然后, 该 BlackEnergy 客户端通过 HTTP 与 C 和 Cserver 沟通。它使用 HTTP POST 请求 stat.php 页, 如图 14 所示。POST 请求数据然后登录到“统计”表中, 信息发送的 HTTP POST 请求消息包括 ID 和建立 ID 参数。

ID 参数是一个组合的 SMB 主机名和 C:\被感染机器的卷信息。DDoS 攻击的 BlackEnergy 僵尸网络可以启动控制的“洪水”命令的参数, 如下。

icmp: 一个基于 icmp ping 洪水。

syn: 基于 TCP syn 洪水。

udp: 基于 udp 流量洪水。

http: http GET 请求洪水。这个命令格式的洪水如下。

URI http <主机名> <可选>, 如“洪水 http www.li-da.org index.php”。



图 12 成功创建并设置为自启动服务

```

[511364B] . 83C4 0C      ADD ESP,0C
[511364E] . 68 00901115  PUSH _bot.15119000
[5113653] . E8 001E0000  CALL _bot.15115460
[5113658] . 83C4 04      ADD ESP,4
[511365B] . 50          PUSH EAX
[511365C] . 68 30741115  PUSH _bot.15117430
[5113661] . 68 00901115  PUSH _bot.15119000
[5113666] . E8 05E2FFFF  CALL _bot.151118F0
[511366B] . 83C4 0C      ADD ESP,0C
[511366E] . 68 04010000  PUSH 104
[5113673] . 68 10701115  PUSH _bot.15117910
[5113678] . FF15 9C101115 CALL DWORD PTR DS:[<&KERNEL32.GetSystem
[511367E] . 68 04010000  PUSH 104
[5113683] . 68 F3771115  PUSH _bot.151177F8
[5113688] . 6A 00       PUSH 0
[511368B] . FF15 94101115 CALL DWORD PTR DS:[<&KERNEL32.GetModul
[5113690] . 50          PUSH EAX
[5113693] . FF15 94101115 CALL DWORD PTR DS:[<&KERNEL32.GetModul
[5113697] . 68 10701115  PUSH _bot.15117910
[511369C] . 68 00791115  PUSH _bot.15117900
[51136A1] . FF15 44101115 CALL DWORD PTR DS:[<&KERNEL32.istr
[51136A7] . 68 EC151115  PUSH _bot.151115E0
[51136AC] . 68 00791115  PUSH _bot.15117900
[51136B1] . FF15 40101115 CALL DWORD PTR DS:[<&KERNEL32.istr
[51136B7] . 68 F0151115  PUSH _bot.151115F0
[51136BC] . 68 00791115  PUSH _bot.15117900
[51136C1] . FF15 40101115 CALL DWORD PTR DS:[<&KERNEL32.istr
[51136C7] . 68 FC151115  PUSH _bot.151115FC
[51136CC] . 6A 00       PUSH 0
[51136CF] . 68 00       PUSH 0
[51136D0] . FF15 7C101115 CALL DWORD PTR DS:[<&KERNEL32.CreateMut
[51136D6] . 89MS FC     MOV DWORD PTR SS:[EBP+4],EAX
[51136D9] . FF15 20101115 CALL DWORD PTR DS:[<&KERNEL32.GetLastEr
[51136DE] . 50          PUSH EAX
[51136E0] . 68 44151115  PUSH _bot.15111544
[51136E3] . 8B95 E4FEFFFF MOV EDI,DWORD PTR SS:[EBP-11C]
[51136E8] . 52          PUSH EDI
[51136EB] . FF15 00111115 CALL DWORD PTR DS:[<&WININET.HttpOpenRequestA]
[51136F0] . 8945 F4     MOV DWORD PTR SS:[EBP-C],EAX
[51136F4] . 837D F4 00  CMP DWORD PTR SS:[EBP-C],0
[51136F8] . 75 02       JNZ SHORT _bot.15112F0C
[51136FA] . 5B         POP EBX
[51136FB] . 745 FC 4C15 MOV DWORD PTR SS:[EBP-4],_bot.1511154C
[51136FD] . 8B45 0C     MOV EAX,DWORD PTR SS:[EBP+C]
[51136FE] . 50          PUSH EAX
[5113700] . 68 50101115  PUSH _bot.15117900
[5113703] . 50          PUSH EAX
[5113706] . 8B4D 0C     MOV ECX,DWORD PTR SS:[EBP+C]
[5113709] . 51          PUSH ECX
[511370B] . 8B45 FC     MOV EDI,DWORD PTR SS:[EBP-4]
[511370E] . 52          PUSH EDI
[5113710] . FF15 50101115 CALL DWORD PTR DS:[<&KERNEL32.lstrlenA]
[5113713] . 50          PUSH EAX
[5113716] . 8B4D 0C     MOV ECX,DWORD PTR SS:[EBP+C]
[5113719] . 51          PUSH ECX
[511371B] . 8B45 FC     MOV EDI,DWORD PTR SS:[EBP-4]
[511371E] . 52          PUSH EDI
[5113720] . FF15 50101115 CALL DWORD PTR DS:[<&KERNEL32.lstrlenA]
[5113723] . 50          PUSH EAX
[5113726] . 8B45 FC     MOV EDI,DWORD PTR SS:[EBP-4]
[5113729] . 50          PUSH EAX
[511372B] . 8B4D F4     MOV ECX,DWORD PTR SS:[EBP-C]
[511372E] . 51          PUSH ECX
[5113730] . FF15 04111115 CALL DWORD PTR DS:[<&WININET.HttpSendRequestA]
[5113733] . 50          PUSH EAX
[5113736] . 50          PUSH EAX
[5113738] . 50          PUSH EAX
[511373A] . 50          PUSH EAX
[511373C] . 50          PUSH EAX
[511373E] . 50          PUSH EAX
[5113740] . 50          PUSH EAX
[5113742] . 50          PUSH EAX
[5113744] . 50          PUSH EAX
[5113746] . 50          PUSH EAX
[5113748] . 50          PUSH EAX
[511374A] . 50          PUSH EAX
[511374C] . 50          PUSH EAX
[511374E] . 50          PUSH EAX
[5113750] . 50          PUSH EAX
[5113752] . 50          PUSH EAX
[5113754] . 50          PUSH EAX
[5113756] . 50          PUSH EAX
[5113758] . 50          PUSH EAX
[511375A] . 50          PUSH EAX
[511375C] . 50          PUSH EAX
[511375E] . 50          PUSH EAX
[5113760] . 50          PUSH EAX
[5113762] . 50          PUSH EAX
[5113764] . 50          PUSH EAX
[5113766] . 50          PUSH EAX
[5113768] . 50          PUSH EAX
[511376A] . 50          PUSH EAX
[511376C] . 50          PUSH EAX
[511376E] . 50          PUSH EAX
[5113770] . 50          PUSH EAX
[5113772] . 50          PUSH EAX
[5113774] . 50          PUSH EAX
[5113776] . 50          PUSH EAX
[5113778] . 50          PUSH EAX
[511377A] . 50          PUSH EAX
[511377C] . 50          PUSH EAX
[511377E] . 50          PUSH EAX
[5113780] . 50          PUSH EAX
[5113782] . 50          PUSH EAX
[5113784] . 50          PUSH EAX
[5113786] . 50          PUSH EAX
[5113788] . 50          PUSH EAX
[511378A] . 50          PUSH EAX
[511378C] . 50          PUSH EAX
[511378E] . 50          PUSH EAX
[5113790] . 50          PUSH EAX
[5113792] . 50          PUSH EAX
[5113794] . 50          PUSH EAX
[5113796] . 50          PUSH EAX
[5113798] . 50          PUSH EAX
[511379A] . 50          PUSH EAX
[511379C] . 50          PUSH EAX
[511379E] . 50          PUSH EAX
[51137A0] . 50          PUSH EAX
[51137A2] . 50          PUSH EAX
[51137A4] . 50          PUSH EAX
[51137A6] . 50          PUSH EAX
[51137A8] . 50          PUSH EAX
[51137AA] . 50          PUSH EAX
[51137AC] . 50          PUSH EAX
[51137AE] . 50          PUSH EAX
[51137B0] . 50          PUSH EAX
[51137B2] . 50          PUSH EAX
[51137B4] . 50          PUSH EAX
[51137B6] . 50          PUSH EAX
[51137B8] . 50          PUSH EAX
[51137BA] . 50          PUSH EAX
[51137BC] . 50          PUSH EAX
[51137BE] . 50          PUSH EAX
[51137C0] . 50          PUSH EAX
[51137C2] . 50          PUSH EAX
[51137C4] . 50          PUSH EAX
[51137C6] . 50          PUSH EAX
[51137C8] . 50          PUSH EAX
[51137CA] . 50          PUSH EAX
[51137CC] . 50          PUSH EAX
[51137CE] . 50          PUSH EAX
[51137D0] . 50          PUSH EAX
[51137D2] . 50          PUSH EAX
[51137D4] . 50          PUSH EAX
[51137D6] . 50          PUSH EAX
[51137D8] . 50          PUSH EAX
[51137DA] . 50          PUSH EAX
[51137DC] . 50          PUSH EAX
[51137DE] . 50          PUSH EAX
[51137E0] . 50          PUSH EAX
[51137E2] . 50          PUSH EAX
[51137E4] . 50          PUSH EAX
[51137E6] . 50          PUSH EAX
[51137E8] . 50          PUSH EAX
[51137EA] . 50          PUSH EAX
[51137EC] . 50          PUSH EAX
[51137EE] . 50          PUSH EAX
[51137F0] . 50          PUSH EAX
[51137F2] . 50          PUSH EAX
[51137F4] . 50          PUSH EAX
[51137F6] . 50          PUSH EAX
[51137F8] . 50          PUSH EAX
[51137FA] . 50          PUSH EAX
[51137FC] . 50          PUSH EAX
[51137FE] . 50          PUSH EAX
[5113800] . 50          PUSH EAX
[5113802] . 50          PUSH EAX
[5113804] . 50          PUSH EAX
[5113806] . 50          PUSH EAX
[5113808] . 50          PUSH EAX
[511380A] . 50          PUSH EAX
[511380C] . 50          PUSH EAX
[511380E] . 50          PUSH EAX
[5113810] . 50          PUSH EAX
[5113812] . 50          PUSH EAX
[5113814] . 50          PUSH EAX
[5113816] . 50          PUSH EAX
[5113818] . 50          PUSH EAX
[511381A] . 50          PUSH EAX
[511381C] . 50          PUSH EAX
[511381E] . 50          PUSH EAX
[5113820] . 50          PUSH EAX
[5113822] . 50          PUSH EAX
[5113824] . 50          PUSH EAX
[5113826] . 50          PUSH EAX
[5113828] . 50          PUSH EAX
[511382A] . 50          PUSH EAX
[511382C] . 50          PUSH EAX
[511382E] . 50          PUSH EAX
[5113830] . 50          PUSH EAX
[5113832] . 50          PUSH EAX
[5113834] . 50          PUSH EAX
[5113836] . 50          PUSH EAX
[5113838] . 50          PUSH EAX
[511383A] . 50          PUSH EAX
[511383C] . 50          PUSH EAX
[511383E] . 50          PUSH EAX
[5113840] . 50          PUSH EAX
[5113842] . 50          PUSH EAX
[5113844] . 50          PUSH EAX
[5113846] . 50          PUSH EAX
[5113848] . 50          PUSH EAX
[511384A] . 50          PUSH EAX
[511384C] . 50          PUSH EAX
[511384E] . 50          PUSH EAX
[5113850] . 50          PUSH EAX
[5113852] . 50          PUSH EAX
[5113854] . 50          PUSH EAX
[5113856] . 50          PUSH EAX
[5113858] . 50          PUSH EAX
[511385A] . 50          PUSH EAX
[511385C] . 50          PUSH EAX
[511385E] . 50          PUSH EAX
[5113860] . 50          PUSH EAX
[5113862] . 50          PUSH EAX
[5113864] . 50          PUSH EAX
[5113866] . 50          PUSH EAX
[5113868] . 50          PUSH EAX
[511386A] . 50          PUSH EAX
[511386C] . 50          PUSH EAX
[511386E] . 50          PUSH EAX
[5113870] . 50          PUSH EAX
[5113872] . 50          PUSH EAX
[5113874] . 50          PUSH EAX
[5113876] . 50          PUSH EAX
[5113878] . 50          PUSH EAX
[511387A] . 50          PUSH EAX
[511387C] . 50          PUSH EAX
[511387E] . 50          PUSH EAX
[5113880] . 50          PUSH EAX
[5113882] . 50          PUSH EAX
[5113884] . 50          PUSH EAX
[5113886] . 50          PUSH EAX
[5113888] . 50          PUSH EAX
[511388A] . 50          PUSH EAX
[511388C] . 50          PUSH EAX
[511388E] . 50          PUSH EAX
[5113890] . 50          PUSH EAX
[5113892] . 50          PUSH EAX
[5113894] . 50          PUSH EAX
[5113896] . 50          PUSH EAX
[5113898] . 50          PUSH EAX
[511389A] . 50          PUSH EAX
[511389C] . 50          PUSH EAX
[511389E] . 50          PUSH EAX
[51138A0] . 50          PUSH EAX
[51138A2] . 50          PUSH EAX
[51138A4] . 50          PUSH EAX
[51138A6] . 50          PUSH EAX
[51138A8] . 50          PUSH EAX
[51138AA] . 50          PUSH EAX
[51138AC] . 50          PUSH EAX
[51138AE] . 50          PUSH EAX
[51138B0] . 50          PUSH EAX
[51138B2] . 50          PUSH EAX
[51138B4] . 50          PUSH EAX
[51138B6] . 50          PUSH EAX
[51138B8] . 50          PUSH EAX
[51138BA] . 50          PUSH EAX
[51138BC] . 50          PUSH EAX
[51138BE] . 50          PUSH EAX
[51138C0] . 50          PUSH EAX
[51138C2] . 50          PUSH EAX
[51138C4] . 50          PUSH EAX
[51138C6] . 50          PUSH EAX
[51138C8] . 50          PUSH EAX
[51138CA] . 50          PUSH EAX
[51138CC] . 50          PUSH EAX
[51138CE] . 50          PUSH EAX
[51138D0] . 50          PUSH EAX
[51138D2] . 50          PUSH EAX
[51138D4] . 50          PUSH EAX
[51138D6] . 50          PUSH EAX
[51138D8] . 50          PUSH EAX
[51138DA] . 50          PUSH EAX
[51138DC] . 50          PUSH EAX
[51138DE] . 50          PUSH EAX
[51138E0] . 50          PUSH EAX
[51138E2] . 50          PUSH EAX
[51138E4] . 50          PUSH EAX
[51138E6] . 50          PUSH EAX
[51138E8] . 50          PUSH EAX
[51138EA] . 50          PUSH EAX
[51138EC] . 50          PUSH EAX
[51138EE] . 50          PUSH EAX
[51138F0] . 50          PUSH EAX
[51138F2] . 50          PUSH EAX
[51138F4] . 50          PUSH EAX
[51138F6] . 50          PUSH EAX
[51138F8] . 50          PUSH EAX
[51138FA] . 50          PUSH EAX
[51138FC] . 50          PUSH EAX
[51138FE] . 50          PUSH EAX
[5113900] . 50          PUSH EAX
[5113902] . 50          PUSH EAX
[5113904] . 50          PUSH EAX
[5113906] . 50          PUSH EAX
[5113908] . 50          PUSH EAX
[511390A] . 50          PUSH EAX
[511390C] . 50          PUSH EAX
[511390E] . 50          PUSH EAX
[5113910] . 50          PUSH EAX
[5113912] . 50          PUSH EAX
[5113914] . 50          PUSH EAX
[5113916] . 50          PUSH EAX
[5113918] . 50          PUSH EAX
[511391A] . 50          PUSH EAX
[511391C] . 50          PUSH EAX
[511391E] . 50          PUSH EAX
[5113920] . 50          PUSH EAX
[5113922] . 50          PUSH EAX
[5113924] . 50          PUSH EAX
[5113926] . 50          PUSH EAX
[5113928] . 50          PUSH EAX
[511392A] . 50          PUSH EAX
[511392C] . 50          PUSH EAX
[511392E] . 50          PUSH EAX
[5113930] . 50          PUSH EAX
[5113932] . 50          PUSH EAX
[5113934] . 50          PUSH EAX
[5113936] . 50          PUSH EAX
[5113938] . 50          PUSH EAX
[511393A] . 50          PUSH EAX
[511393C] . 50          PUSH EAX
[511393E] . 50          PUSH EAX
[5113940] . 50          PUSH EAX
[5113942] . 50          PUSH EAX
[5113944] . 50          PUSH EAX
[5113946] . 50          PUSH EAX
[5113948] . 50          PUSH EAX
[511394A] . 50          PUSH EAX
[511394C] . 50          PUSH EAX
[511394E] . 50          PUSH EAX
[5113950] . 50          PUSH EAX
[5113952] . 50          PUSH EAX
[5113954] . 50          PUSH EAX
[5113956] . 50          PUSH EAX
[5113958] . 50          PUSH EAX
[511395A] . 50          PUSH EAX
[511395C] . 50          PUSH EAX
[511395E] . 50          PUSH EAX
[5113960] . 50          PUSH EAX
[5113962] . 50          PUSH EAX
[5113964] . 50          PUSH EAX
[5113966] . 50          PUSH EAX
[5113968] . 50          PUSH EAX
[511396A] . 50          PUSH EAX
[511396C] . 50          PUSH EAX
[511396E] . 50          PUSH EAX
[5113970] . 50          PUSH EAX
[5113972] . 50          PUSH EAX
[5113974] . 50          PUSH EAX
[5113976] . 50          PUSH EAX
[5113978] . 50          PUSH EAX
[511397A] . 50          PUSH EAX
[511397C] . 50          PUSH EAX
[511397E] . 50          PUSH EAX
[5113980] . 50          PUSH EAX
[5113982] . 50          PUSH EAX
[5113984] . 50          PUSH EAX
[5113986] . 50          PUSH EAX
[5113988] . 50          PUSH EAX
[511398A] . 50          PUSH EAX
[511398C] . 50          PUSH EAX
[511398E] . 50          PUSH EAX
[5113990] . 50          PUSH EAX
[5113992] . 50          PUSH EAX
[5113994] . 50          PUSH EAX
[5113996] . 50          PUSH EAX
[5113998] . 50          PUSH EAX
[511399A] . 50          PUSH EAX
[511399C] . 50          PUSH EAX
[511399E] . 50          PUSH EAX
[51139A0] . 50          PUSH EAX
[51139A2] . 50          PUSH EAX
[51139A4] . 50          PUSH EAX
[51139A6] . 50          PUSH EAX
[51139A8] . 50          PUSH EAX
[51139AA] . 50          PUSH EAX
[51139AC] . 50          PUSH EAX
[51139AE] . 50          PUSH EAX
[51139B0] . 50          PUSH EAX
[51139B2] . 50          PUSH EAX
[51139B4] . 50          PUSH EAX
[51139B6] . 50          PUSH EAX
[51139B8] . 50          PUSH EAX
[51139BA] . 50          PUSH EAX
[51139BC] . 50          PUSH EAX
[51139BE] . 50          PUSH EAX
[51139C0] . 50          PUSH EAX
[51139C2] . 50          PUSH EAX
[51139C4] . 50          PUSH EAX
[51139C6] . 50          PUSH EAX
[51139C8] . 50          PUSH EAX
[51139CA] . 50          PUSH EAX
[51139CC] . 50          PUSH EAX
[51139CE] . 50          PUSH EAX
[51139D0] . 50          PUSH EAX
[51139D2] . 50          PUSH EAX
[51139D4] . 50          PUSH EAX
[51139D6] . 50          PUSH EAX
[51139D8] . 50          PUSH EAX
[51139DA] . 50          PUSH EAX
[51139DC] . 50          PUSH EAX
[51139DE] . 50          PUSH EAX
[51139E0] . 50          PUSH EAX
[51139E2] . 50          PUSH EAX
[51139E4] . 50          PUSH EAX
[51139E6] . 50          PUSH EAX
[51139E8] . 50          PUSH EAX
[51139EA] . 50          PUSH EAX
[51139EC] . 50          PUSH EAX
[51139EE] . 50          PUSH EAX
[51139F0] . 50          PUSH EAX
[51139F2] . 50          PUSH EAX
[51139F4] . 50          PUSH EAX
[51139F6] . 50          PUSH EAX
[51139F8] . 50          PUSH EAX
[51139FA] . 50          PUSH EAX
[51139FC] . 50          PUSH EAX
[51139FE] . 50          PUSH EAX
[5113A00] . 50          PUSH EAX
[5113A02] . 50          PUSH EAX
[5113A04] . 50          PUSH EAX
[5113A06] . 50          PUSH EAX
[5113A08] . 50          PUSH EAX
[5113A0A] . 50          PUSH EAX
[5113A0C] . 50          PUSH EAX
[5113A0E] . 50          PUSH EAX
[5113A10] . 50          PUSH EAX
[5113A12] . 50          PUSH EAX
[5113A14] . 50          PUSH EAX
[5113A16] . 50          PUSH EAX
[5113A18] . 50          PUSH EAX
[5113A1A] . 50          PUSH EAX
[5113A1C] . 50          PUSH EAX
[5113A1E] . 50          PUSH EAX
[5113A20] . 50          PUSH EAX
[5113A22] . 50          PUSH EAX
[5113A24] . 50          PUSH EAX
[5113A26] . 50          PUSH EAX
[5113A28] . 50          PUSH EAX
[5113A2A] . 50          PUSH EAX
[5113A2C] . 50          PUSH EAX
[5113A2E] . 50          PUSH EAX
[5113A30] . 50          PUSH EAX
[5113A32] . 50          PUSH EAX
[5113A34] . 50          PUSH EAX
[5113A36] . 50          PUSH EAX
[5113A38] . 50          PUSH EAX
[5113A3A] . 50          PUSH EAX
[5113A3C] . 50          PUSH EAX
[5113A3E] . 50          PUSH EAX
[5113A40] . 50          PUSH EAX
[5113A42] . 50          PUSH EAX
[5113A44] . 50          PUSH EAX
[5113A46] . 50          PUSH EAX
[5113A48] . 50          PUSH EAX
[5113A4A] . 50          PUSH EAX
[5113A4C] . 50          PUSH EAX
[5113A4E] . 50          PUSH EAX
[5113A50] . 50          PUSH EAX
[5113A52] . 50          PUSH EAX
[5113A54] . 50          PUSH EAX
[5113A56] . 50          PUSH EAX
[5113A58] . 50          PUSH EAX
[5113A5A] . 50          PUSH EAX
[5113A5C] . 50          PUSH EAX
[5113A5E] . 50          PUSH EAX
[5113A60] . 50          PUSH EAX
[5113A62] . 50          PUSH EAX
[5113A64] . 50          PUSH EAX
[5113A66] . 50          PUSH EAX
[5113A68] . 50          PUSH EAX
[5113A6A] . 50          PUSH EAX
[5113A6C] . 50          PUSH EAX
[5113A6E] . 50          PUSH EAX
[5113A70] . 50          PUSH EAX
[5113A72] . 50          PUSH EAX
[5113A74] . 50          PUSH EAX
[5113A76] . 50          PUSH EAX
[5113A78] . 50          PUSH EAX
[5113A7A] . 50          PUSH EAX
[5113A7C] . 50          PUSH EAX
[5113A7E] . 50          PUSH EAX
[5113A80] . 50          PUSH EAX
[5113A82] . 50          PUSH EAX
[5113A84] . 50          PUSH EAX
[5113A86] . 50          PUSH EAX
[5113A88] . 50          PUSH EAX
[5113A8A] . 50          PUSH EAX
[5113A8C] . 50          PUSH EAX
[5113A8E] . 50          PUSH EAX
[5113A90] . 50          PUSH EAX
[5113A92] . 50          PUSH EAX
[5113A94] . 50          PUSH EAX
[5113A96] . 50          PUSH EAX
[5113A98] . 50          PUSH EAX
[5113A9A] . 50          PUSH EAX
[5113A9C] . 50          PUSH EAX
[5113A9E] . 50          PUSH EAX
[5113AA0] . 50          PUSH EAX
[5113AA2] . 50          PUSH EAX
[5113AA4] . 50          PUSH EAX
[5113AA6] . 50          PUSH EAX
[5113AA8] . 50          PUSH EAX
[5113AAA] . 50          PUSH EAX
[5113AAC] . 50          PUSH EAX
[5113AAE] . 50          PUSH EAX
[5113AB0] . 50          PUSH EAX
[5113AB2] . 50          PUSH EAX
[5113AB4] . 50          PUSH EAX
[5113AB6] . 50          PUSH EAX
[5113AB8] . 50          PUSH EAX
[5113ABA] . 50          PUSH EAX
[5113ABC] . 50          PUSH EAX
[5113ABE] . 50          PUSH EAX
[5113AC0] . 50          PUSH EAX
[5113AC2] . 50          PUSH EAX
[5113AC4] . 50          PUSH EAX
[5113AC6] . 50          PUSH EAX
[5113AC8] . 50          PUSH EAX
[5113ACA] . 50          PUSH EAX
[5113ACC] . 50          PUSH EAX
[5113ACE] . 50          PUSH EAX
[5113AD0] . 50          PUSH EAX
[5113AD2] . 50          PUSH EAX
[5113AD4] . 50          PUSH EAX
[5113AD6] . 50          PUSH EAX
[5113AD8] . 50          PUSH EAX
[5113ADA] . 50          PUSH EAX
[5113ADC] . 50          PUSH EAX
[5113ADE] . 50          PUSH EAX
[5113AE0] . 50          PUSH EAX
[5113AE2] . 50          PUSH EAX
[5113AE4] . 50          PUSH EAX
[5113AE6] . 50          PUSH EAX
[5113AE8] . 50          PUSH EAX
[5113AEA] . 50          PUSH EAX
[5113AEC] . 50          PUSH EAX
[5113AEE] . 50          PUSH EAX
[5113AF0] . 50          PUSH EAX
[5113AF2] . 50          PUSH EAX
[5113AF4] . 50          PUSH EAX
[5113AF6] . 50          PUSH EAX
[5113AF8] . 50          PUSH EAX
[5113AFA] . 50          PUSH EAX
[5113AFC] . 50          PUSH EAX
[5113AFE] . 50          PUSH EAX
[5113B00] . 50          PUSH EAX
[5113B02] . 50          PUSH EAX
[5113B04] . 50          PUSH EAX
[5113B06] . 50          PUSH EAX
[5113B08] . 50          PUSH EAX
[5113B0A] . 50          PUSH EAX
[5113B0C] . 50          PUSH EAX
[5113B0E] . 50          PUSH EAX
[5113B10] . 50          PUSH EAX
[5113B12] . 50          PUSH EAX
[5113B14] . 50          PUSH EAX
[5113B16] . 50          PUSH EAX
[5113B18] . 50          PUSH EAX
[5113B1A] . 50          PUSH EAX
[5113B1C] . 50          PUSH EAX
[5113B1E] . 50          PUSH EAX
[5113B20] . 50          PUSH EAX
[5113B22] . 50          PUSH EAX
[5113B24] . 50          PUSH EAX
[5113B26] . 50          PUSH EAX
[5113B28] . 50          PUSH EAX
[5113B2A] . 50          PUSH EAX
[5113B2C] . 50          PUSH EAX
[5113B2E] . 50          PUSH EAX
[5113B30] . 50          PUSH EAX
[5113B32] . 50          PUSH EAX
[5113B34] . 50          PUSH EAX
[5113B36] . 50          PUSH EAX
[5113B38] . 50          PUSH EAX
[5113B3A] . 50          PUSH EAX
[5113B3C] . 50          PUSH EAX
[5113B3E] . 50          PUSH EAX
[5113B40] . 50          PUSH EAX
[5113B42] . 50          PUSH EAX
[5113B44] . 50          PUSH EAX
[5113B46] . 50          PUSH EAX
[5113B48] . 50          PUSH EAX
[5113B4A] . 50          PUSH EAX
[5113B4C] . 50          PUSH EAX
[5113B4E] . 50          PUSH EAX
[5113B50] . 50          PUSH EAX
[5113B52] . 50          PUSH EAX
[5113B54] . 50          PUSH EAX
[5113B56] . 50          PUSH EAX
[5113
```


意程序。office2007 系列组件是一个主要的漏洞攻击载体。

iSIGHT Partners 厂商^[9]宣称发现, 新的 Oday 被俄罗斯黑客用在针对北约的名为“SandWorm”的 APT 攻击中, 该漏洞首次被发现。经过初步分析, CVE-2014-4114 漏洞也能被 BlackEnergy 利用, 其触发的核心在于 office 系列组件加载 Ole 对象, Ole 对象可以通过远程下载, 在加载 Ole 包时, 会下载 2 个文件, 一个为 inf 文件, 一个为 gif (实质上是可执行病毒文件)。将下载的 gif 文件的后缀名改为 exe 并加入到开机启动项, 此病毒文件就是 BlackEnergy。随后调用 C:\Windows\System32\InfDefaultInstall.exe 执行下载下来的 inf 文件, 从而造成了远程任意代码执行。

4.2 攻击步骤

攻击者首先将恶意代码嵌入电子邮件的 office 附件中, 入侵目标主机后, 利用漏洞 CVE-2014-4114 迷惑目标主机执行病毒 exe 程序, 远程连接 C&C 服务器进行交互, 将目标主机的关键信息发送给攻击者。

宏病毒利用工控 HMI (人机界面) 远程执行漏洞 (CVE-2014-0751^[10]) 对内网发起攻击, 远程攻击者可通过向 TCP 10212 端口发送特制报文利用该漏洞执行任意代码, 从而控制内网的 HMI。

攻击者将 BlackEnergy 嵌入内网 HMI, BlackEnergy 开启 DropbearSSH^[11]后门, SSH 服务器连接端口 6789。在被感染的内网运行 SSH, 攻击者可以进退自如。

攻击者启动 BlackEnergy 的 KillDisk 组件, 该组件的主要目的是破坏原有数据, 用随机数据覆盖原文件, 并且让系统无法重启。

4.3 防御措施

通过对 BlackEnergy 和乌克兰事件各方面的分析可以看出, SCADA 系统很大程度上仍受制于所采用操作系统自身的漏洞和缺陷。因此本文从以下几个方面对 SCADA 系统进行安全防护。虽然过去的工控系统相对封闭, 但是随着移动互联网的发展, 很多工控的采集点^[11]都已经暴露在互联网上, 可以轻易被攻击, 并以此为基础进入管理系统, 因此加强系统与互联网之间的安全防护级别至关重要, 尽量避免把系统任何部分直接暴

露在互联网上。对工控系统采用的国外产品进行全面的安全检查, 以避免可被利用的后门存在的风险, 同时监测第三方供货商提供任何管理员级别账户的动作, 删除或重命名系统默认账户; 安装工控系统专用防火墙, 对各部分通信行为进行严格监管, 禁止外接设备, 使用专用的安全 U 盘, 阻断潜在的攻击路径。关闭系统中不必要的应用和服务, 安排专人对工控设备做定时的升级和打补丁操作。

从此次乌克兰电力系统遭受黑客攻击导致停电的事件中, 可以看到如下问题: 存在安全防护体系方面的漏洞, 工控系统与网络直接相连没有任何隔离措施; BlackEnergy 病毒入侵工控系统后存在一定的潜伏期, 但由于网络安全监控不到位并未发现任何病毒入侵异常; 攻击者通过发送伪装邮件的方式致使乌克兰方面的工作人员打开了恶意植入程序, 虽然在此之前国际安全机构曾向其发出过预警信息, 但由于网络信息安全防范方面的意识薄弱, 并未得到重视。

5 结束语

本文概括地介绍了 BlackEnergy 病毒的发展历程, 将 BlackEnergy 三代病毒分别进行了初步分析, 通过对现有样本模拟攻击以及反汇编原理的分析, 得出了 BlackEnergy 的入侵方法, 分析推测得出乌克兰事件 BlackEnergy 的攻击过程, 以及此病毒对系统漏洞的利用从而逐步感染电力系统的过程。同时根据 BlackEnergy 的行为特点和乌克兰事件所造成严重的后果指出了目前 SCADA 系统在网络信息安全方面存在的隐患及不足。同时也给出了在电力安全工控系统当中, 针对网络安全方面的一些可防护入侵措施。

但本文只是在理论分析层面以及 BlackEnergy 的入侵步骤等基础方向进行了初步分析, 所给出的预防措施也没有根据我国国情具体考虑在不同地区不同领域实际的可行性。未来的研究方向是, 通过此次乌克兰事件收集更多可用的信息, 找到最新的病毒版本进行分析, 获取 BlackEnergy 病毒的源代码, 并且构建一套完整的模拟电力工控系统的体系, 进行实际的病毒入侵实验, 在实际操作过程中确认防护入侵措施的

有效性、可行性, 从而进一步完善电力工控系统的安全性措施。

参考文献:

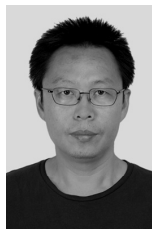
- [1] Brian Prince(2014). Researchers go inside black energy malware[EB/OL]. <http://www.securityweek.com/researchers-go-inside-blackenergy-malware>.
- [2] John Hultquist(2014). Sandworm team – targeting SCADA systems[EB/OL]. <https://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/>.
- [3] 安天实验室. 乌克兰停电事件启示录[J]. 中国信息安全, 2016(4):48-53.
Antiy Lab. Revelation of blackout in Ukraine[J]. China Information Security, 2016(4):48-53.
- [4] 绿盟科技(2016). 从乌电事件看我国电力安全[EB/OL]. <http://www.aiweibang.com/yuedu/82697112.html>.
NSFOCUS.(2016). Power safety in China from Ukraine's power grid incident[EB/OL]. <http://www.aiweibang.com/yuedu/82697112.html>.
- [5] 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. 乌克兰电力系统遭受攻击事件综合分析[J]. 信息安全研究, 2016(3):243.
Harbin Antiy Tech. Co. Ltd., Beijing Sifang Automation Co. Ltd., Fudan University Network Space Management Research Center. Comprehensive analysis of Ukraine's power grid incident[J]. Journal of Information Security Research, 2016(3):243.
- [6] 安天实验室安全研究与应急处理中心. BlackEnergy 简报[EB/OL]. <http://www.antiy.com/response/BlackEnergy/BlackEnergy.html>.
Antiy CERT. BlackEnergy briefing[EB/OL]. <http://www.antiy.com/response/BlackEnergy/BlackEnergy.html>.
- [7] F-secure. (2014) BLACKENERGY & QUEDAGH: the convergence of crimeware and APT attacks[EB/OL]. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf
- [8] CVE 通用漏洞与披露(2014). Microsoft Windows OLE 远程执行代码漏洞 (CNNVD-201410-268)[EB/OL]. <http://cve.scap.org.cn/CVE-2014-4114.html>.
CVE Common vulnerabilities and disclosures(2014). Windows OLE remote code execution vulnerability (CNNVD-201410-268) [EB/OL]. <http://cve.scap.org.cn/CVE-2014-4114.html>.
- [9] 翰海源安全(2014). Windows 任意代码执行 0day (CVE-2014-4114) 分析报告[EB/OL]. <http://www.freebuf.com/news/46956.html>.
Nanjing Vulnhunt Information Security Inc. Analysis report of Windows arbitrary code execution of 0day (CVE-2014-4114) [EB/OL]. <http://www.freebuf.com/news/46956.html>.
- [10] CVE 通用漏洞与披露(2014). GE intelligent platforms proficy HMI/SCADA-CIMPLICITY 目录遍历漏洞(CNNVD-201401-524) [EB/OL]. <http://cve.scap.org.cn/CVE-2014-0751.html>.

CVE Common vulnerabilities and disclosures. GE Intelligent platforms proficy HMI/SCADA-CIMPLICITY directory traversal vulnerability (CNNVD-201401-524) [EB/OL]. <http://cve.scap.org.cn/CVE-2014-0751.html>.

- [11] 王得金. 从乌克兰电网被攻击事件看我国基础电网面临的安全风险及处置建议[J]. 中国信息安全, 2016(3): 91-93.

WANG D J. Security risks faced by China's basic power grids and suggestions on disposal from the attacked events in Ukraine power grid[J]. China Information Security, 2016(3): 91-93.

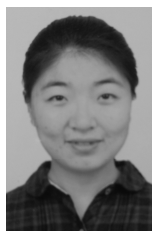
作者简介:



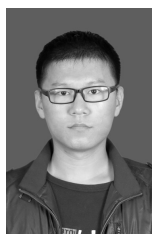
王勇 (1973-), 男, 河南驻马店人, 博士, 上海电力学院教授, 主要研究方向为电力系统攻防试验床、病毒分析、入侵检测。



王钰茗 (1994-), 女, 山东烟台人, 上海电力学院本科生, 主要研究方向为病毒分析。



张琳 (1995-), 女, 黑龙江绥化人, 上海电力学院本科生, 主要研究方向为病毒分析。



张林鹏 (1991-), 男, 河北邢台人, 上海电力学院硕士生, 主要研究方向为电力系统防火墙。