一、网络空间中的对抗

1.1 APT的典型事件之——“震网病毒”

- 目标系统：工控系统
- 潜伏渗透：感染了伊朗境内60%的PC
- 突破物理隔离：U盘(病毒检测到宿主机插上U盘则主动向U盘感染病毒)
- 技术水平：同时利用多个0day(微软和西门子工控系统)，体现了APT的高级性
- 攻击者：极有可能是敌对关系的政治势力
- 攻击持续性：C2服务器2005.11就完成注册,可能长达6~7年

1.2 APT攻击的概念

- 起源
    - 由美国一名空军上校2006年提出
- 何时引起关注、高潮
    - 2010伊朗震网病毒、2013美国"棱镜门"事件
- 定义
    - 知名第三方机构
        - 维基百科、Mandiant、赛门铁克、Damballa、TechTarget
            - 1.特性：高级、持续、威胁、针对。
              2.目标动机：政治、情报、数据、经济利益
              3.APT目标：国防、制造业、金融、科研
    - 奇安信威胁情报中心
        - 不是一个纯粹的技术概念，泛指有组织，有计划针对特定目标的一系列攻击
        - 组织
            - 国家或者政府(精神支持和物质基础)
            - 情报机构、网络间谍活动的攻击组织
            - 经济实体、犯罪组织、恐怖主义组织
        - 能力：攻击不计成本(技术成本,比如系统0day)
        - 技术特点：针对性、高度隐藏(潜伏渗透周期长)、不以经济利益为直接目的、掌握0day
        - 重大安全事件不一定是APT
            - 重大损失的，也不一定是APT
                - 2016年美国东部互联网瘫痪
                  2018年Facebook数据泄露
                  国内酒店大量住户信息泄露
            - 影响范围大的，也不一定是APT
                - 2017年WannaCry勒索病毒
            - 针对性强的，也不一定是APT
                - 2008年8月俄罗斯对格鲁吉亚的军事行动
    - APT 与威胁情报
        - 威胁情报：安全机构所掌握的、针对特定组织机构的各种网络威胁信息，而该组织机构自身可能并不知道相关威胁的存在或细节
            - 威胁情报的主要方面
                - 源头、目标、动机、工具、指标、表象、影响、方案

1.3 相关研究

- 在全球范围内，APT研究美国和俄罗斯两国属世界一流，中国属全球第二梯队的排头兵
- 行业领域：军队与国防、政府、金融、外交、能源、科研、医疗、传媒、电信
- 目标地域：全球绝大部分的国家和地区。韩国、中东、美国、俄罗斯、巴基斯坦等国家APT最为活跃

二、APT攻击的对象

2.1 工控系统

- 乌克兰圣诞大停电事件
  - 核心攻击方式：BlackEnergy 后门程序、攻击者可远程访问并操控电力控制系统
- 沙特阿拉伯大赦之夜攻击事件
  - 核心攻击方式：Shamoon(Disttrack)，能够导致目标网络完全瘫痪(通过当前的权限来访问活动目录、相同域及局域网其他主机进行横向移动)
    - 投放器(Dropper)
    - 通信组件(Communications)
    - 擦除组件(Wiper)
- 美国电网承包商攻击事件
  - 核心攻击方式：渗透网站，向网站上传恶意程序，利用恶意程序跟踪网站访问者，获得相关人员的账号密码，利用该账号发送大量钓鱼邮件

2.2 金融系统

- 多国银行被盗事件
  - 核心攻击方式：
    获得银行SWIFT权限，利用SWIFI向其他银行发送转账指令、篡改MT9XX报文清除证据
- ATM 机盗窃事件
  - 核心攻击方式：
    1.针对性入侵金融机构员工的计算机或银行网络，进行视频监控，查看和记录负责转账系统的银行员工屏幕。获取足够的信息后，模仿银行员工的行为进行恶意操作。
    2.插入特别制造的芯片(EMV)卡，植入恶意程序，吐钞的同时让计算机断网
    3.入侵其他资产，通过资产内代理进行授权交易
    4.入侵内部网络、获得ATM控制权限
    5.通过光驱、USB接口等直接对ATM机进行操作
- 黄金眼(国内APT组织)行动事件
  - 核心攻击方式：以合法软件开发公司伪装，以不当盈利作为目的，长期从事敏感金融交易信息窃取活动。（该组织攻击水平和反侦察能力均达到国际水平)

2.3 地缘政治

- DNC邮件泄露、美国大选
  - 希拉里邮件门事件，利用私人电子邮件向家里私人服务器发送大量涉及国家机密的绝密邮件，大约6万封。
  - 相关细节：希拉里竞选团队主席被钓鱼攻击上钩，泄露邮箱密码，从而获取邮箱中的邮件，同样的攻击方法在团队其他成员中也相继成功。钓鱼邮件使用了(Bitly)短链接技术来进行伪装。
- 法国总统大选
  - 攻击组织：APT-28
    文档:Trump's_Attack_On_Syria_English.docx

核心攻击技术：
CVE-2017-0262(Word远程代码执行)
CVE-2017-0263(Windows本地权限升级)

2.4 教育、科研系统

- 国内顶尖大学、研究院
- 国内海事、电信、能源、国防、军工业

三、APT攻击的技术手段

3.1 APT攻击的目标

- 敏感情报信息
  - PC敏感文件扩展名
    - doc,docx,ppt,pptx,xls,xlsx,rtf,wps,et,dps,pdf,txt,dwg,rar,zip,7z,exe,eml
  - 移动端敏感文件
    - 音频、照片、通话录音、录像、通话记录、通讯录、短信、手机基本信息、地理位置信息
  - 敏感情报信息窃取方式
    - 核心思想：选择性窃取（攻击者如果活动太频繁，木马与C&C服务器的通信次数越多越容易暴露）。故APT组织一般只收集特定目录下的文件或者有特殊文件名的文件。
    - 文件直接回传、Socket通信、 电子邮件
- 敏感文件
- 经济利益
- 持续监控
- 破坏
- 攻击目标平台
  - Windows、Android、MacOS、iOS
  - 跨平台的水坑攻击
    - 带有恶意程序的伪造Flash升级包

3.2 APT攻击的武器搭载系统

- 鱼叉攻击(Spear Phishing)
  - 目的：不通过授权访问机密数据
  - 手段：最常见的方式是通过电子邮件发送给特定的攻击目标，诱使目标打开附件，这种方式就是鱼叉邮件。
    - 钓鱼邮件：这个概念和鱼叉邮件类似。不过，钓鱼多是针对普通人的攻击，针对性较弱，精确度较低。
  - 实施过程：前期准备->邮件制作->邮件投放->情报回收
  - 防护方法：稍微有点安全意识即可，认真查看邮件来源，附件扩展名，病毒扫描，虚拟机，沙箱等。
- 水坑攻击(Water Holing)
  - 攻击概述：攻击者通过分析攻击目标的网络活动规律，寻找攻击目标经常访问的网站的弱点，先攻下该站点并植入攻击程序，在攻击目标访问该站点时实施攻击
  - 以海莲花APT组织的水坑攻击举例

        - A方式
            - 替换目标网站的可信程序(捆绑即时通、证书驱动)
            - 对目标网站插入恶意JavaScript程序(伪装成Adobe Flash更新程序)
        - B方式
            - 替换目标网站站点指定链接
- PC跳板
- 第三方平台
    - APT组织通过社交网络来下发C&C指令，APT组织的专用木马会读取文章中的程序指令来完成指定的攻击操作
    - 微博、Twitter、Facebook、...
- 恶意硬件中间人劫持
    - 在目标网络环境中部署物理硬件设备，通过中间人方式劫持用户网络流量，替换更新包等软件
        - 输入法软件、聊天软件、下载软件、影音软件、安全软件、微软系统软件
    - 例子：火焰病毒

3.3 APT攻击的武器装备

- 专用木马
    - 开机自启动
        - 修改快捷方式
        - DLL(动态链接库)劫持
        - 修改注册表、服务、计划任务
        - APT组织为何放弃开机自启动?
            - 特定场景下需要一次性攻击
                - 火力侦察判断目标是否为真实目标时、目标防护能力很强时（都是为了隐藏自己的攻击
            - 依赖原始母体文件运行
            - 用其他方法启动木马
                - 注入到其他进程、或者捆绑到其他软件
                - 利用漏洞劫持篡改网络流量
    - 加密与自加密
    - 木马升级换代
- 1day \ nday
    - 出于攻击技术成本考虑、目标系统存在大量已知漏洞但未修复
    - 相关例子
        - CVE-2012-0158
            - 微软Office漏洞(非常稳定)，远程攻击者诱使目标打开一个经过特殊构造的RTF文件，在符合漏洞条件下，即可在目标机器上执行任意指令。
        - CVE-2015-0097
            - 微软Office的一个逻辑漏洞，可导致目标通过HTA文件下载恶意程序到本机并执行
        - Android 漏洞
- 0day
    - Office 文档漏洞
    - Windows 提权漏洞

    - Flash 漏洞
    - 其他0day
- APT组织武器使用成本原则(0day、或者技术成本较高的攻击手段)
    - 攻击目标具有足够的攻击价值
    - 一般的专用木马攻击无效或者无法达到预期目的
    - 利用1day、nday攻击依然无法达到目的或者无效
- APT武器研发趋势
    - 特别关注点：RAT(Remote Access Trojan)文件,远程访问木马的文件格式、文件形态、功能形态、恶意程序寄宿位置的变化
    - 相关武器研发趋势
        - 从PE到非PE，从有实体到无实体
        - 小众编程语言日渐流行(Delphi\GCC\NSIS\AutoIt
        - 模块互动，云控技术渐成主流
        - 恶意程序寄宿位置越藏越深：从常见的系统目录到难以追踪的MBR, VBR, 磁盘固件, EFI, BIOS, 移动存储设备的隐藏分区
        - 独立研发与委托定制成主流
            - 使用公开的RAT，目的是自我隐藏和嫁祸他人
            - 绝大部分的APT组织都是在相对独立的环境下完成攻击代码的开发工作
            - 不排除委托第三方组成协助定制开发的可能性

3.4 APT攻击的 C&C(Command and Control)

- 主要作用：
  1.向感染了目标机的木马程序发送控制命令，提供下载资源(新木马，木马模块，配置文件等)
  2.回收木马程序收集到的情报信息，包括文件、邮件等
- 地域分布
    - 美国最多、其次中国、俄罗斯，西班牙，德国并列第三(2015年)
        - 一个APT组织可能拥有数十个，或者几个分布于不同地域的C&C服务器
- 注册机构
    - 国内外APT组织均使用或部分使用境外服务商动态域名，ChangIP,DynDNS,No-IP,Afraid(FreeDNS),dnsExit
        - 动态域名的好处：
          1.相关注册信息不对外公开(无whois信息)
          2.需要域名持有者的权限才能查询相关信息
- 注册偏好
    - 模仿邮箱类
        - 126mailserver 、mail163等
    - 模仿杀毒软件类
        - safe360、rising等
    - 模仿互联网公司类
        - 360sc2、sohu、sogou、sina等

四、APT攻击的战术布阵

4.1 情报收集

- 重要性：APT组织发动一次攻击，绝大部分时间都会消耗在情报收集环节上。为了达到攻击目的，攻击者必须尽可能地全面的收集攻击目标相关的情报信息，从认知水平到掌握水平。
- 公开情报收集
  - 官方网站、行业网站、学术期刊、行业会议、新闻报道等
- 地下情报收集
  - 地下黑市购买社工库
  - 入侵第三方网站以获取目标人员、组织的情报信息
  - 向其他APT组织购买情报信息

4.2 火力侦察

- 目的：收集攻击目标网络或设备的基本信息、判断攻击目标的真伪(是否为虚拟机)、防御能力、攻击价值。以及方便后期横向移动的准确性。
- 主机信息：操作系统信息、主机名称、本地用户名等
- 网络信息：主要是IP地址、网关信息
- 应用程序信息及相关版本信息，微软Office、微软Internet Explorer
- 磁盘信息、当前进程信息等

4.3 供应链攻击

- 攻击原理
  - 当攻击目标本身的防御措施特别完善时，或初始攻击无法达到效果，对目标相关的周边企业、人员、供应链进行攻击，有可能取得较好的效果。
- 典型案例
  - 震网病毒、Havex

4.4 假旗行动

- 概述
  - 也叫伪旗行动，是隐蔽行动的一种。通过使用其他组织的旗帜、制服等手段误导公众、使公众认为该攻击是其他攻击组织执行。
    - 相关战术术语：拟态、诱饵、混淆、伪装、干扰
- 类型
  - 预设陷阱
    - 样本文件、C&C服务器域名、特殊字符串、上线密码、诱饵文档属性信息等
  - 事后掩盖
    - 攻击成功后，对域名whois、IP地址等信息进行伪装
- 冒充对象
  - 冒充其他APT组织
  - 冒充普通用户
- 国家级情报机构对该行动的观点
  - 五眼联盟
    - 与欺骗相关的策略：暗区(DarkSpace)、蜜罐(Honeypot)、蜜令(Honeytoken)、蜜网(Honeynet)、假旗行动(False Flag)、效果(Effects)
  - 五眼联盟对假旗行动的观点：1.有意制造攻击目标与被嫁祸国或组织间紧张的敌对气氛，以实现某种政治或经济目的 2.更好地隐藏自己，避免暴露，收获更大利益。

4.5 周期性袭扰

- 周一、二（工作日处理邮件、文件高峰期）
- 大型节日（如国庆节、春节等）

4.6 横向移动

- 目的：
  1.进一步在感染的目标机器上获取更多有价值的信息
- 借助受感染的机器，探测周边其他设备的情况或直接向周边设备发动攻击
- 横向移动攻击步骤
  - 侦察和识别网络拓扑、获取域计算机信息、当前计算机相关主机信息、网卡信息、路由信息等
  - 查看远程计算机服务及状态、获取指定IP共享信息、共享目录、扫描内网机器远程端口等
  - 补充原有木马没有的功能、窃取本机更多信息、向周边其他设备发动攻击
  - 常用命令：net view、ipconfig /all、netstat -a/n、nbstat -A、systeminfo、tracert -w 1000 8.8.8.8、ping、telnet、利用PowerShell远程加载木马或者上传情报信息到C&C服务器

4.7 伪装术

- 社会工程学伪装
  - 邮件内容伪装
  - 邮件身份伪装
- 文件视觉伪装
  - 文件名
  - 文件扩展名
  - 文件图标
- 快捷方式伪装
  - 将攻击代码文件和一个指向攻击代码的快捷方式文件打包成一个压缩包，同时，快捷方式的命名具有迷惑性
- 捆绑合法程序
  - AWVS7
    - 针对网络安全行业
  - 办公软件
    - 政府单位、事业单位
  - 即时通、证书驱动
    - 政府机构
  - 微软更新程序
  - Microsoft Visio Professional 2013
- 压缩包外壳
  - 将木马程序进行压缩，以压缩包的形式传播

4.8 反侦察术

- 一些APT组织的攻击木马会判断自身所处的环境、发现杀软时、会选择放弃执行后续的功能代码、或者设法绕过杀软的监测。
- 一些APT组织会对安全研究人员进行反向侦察工作，比如海莲花组织向AWVS的破解版中插入了木马。

五、APT攻击的监测与防御

5.1 如何发现APT攻击

- 大数据技术
  - 数据采集、数据分析、数据呈现
- 威胁情报技术
  - "标志"(Indicator of Compromise,IOC),也叫入侵指示器：通常包括主机活动中出现的文件、进程、注册表键值、系统服务、网络上的域名、URL、IP等
  - 分类
    - 战术情报
      - 标记攻击者使用工具相关的特纸值及网络基础设施信息、可直接用于设备、实现对攻击活动的监控，IOC即是一个典型
    - 作战情报
      - 描述攻击者的工具、技术和过程，即TTP
    - 战略情报
      - 描述当前对于特定组织的威胁类型和对手现状、指导安全投资的大方向。使用者为CSO(Chief Security Officer), CISO(Chief Information Security Offier)
  - 威胁情报的利用
    - ~在准备阶段、检测与分析阶段、隔离，清除，与恢复阶段、事后复盘阶段的作用
    - 安全运营团队会遇到的问题
      - 如何高效地发现攻击和入侵活动，评估影响面
      - 如何获取、处置与已经发现安全事件相关的活动
      - 如何基于对对手的了解、设置各个环节上的安全控制措施、以阻止相同对手或类似攻击手法的入侵
      - 理解目前安全威胁的全貌、实现有效的安全投资
- 流量威胁检测技术
  - 流量威胁分析
  - 流量日志存储
  - 威胁回溯分析
- 网络检测响应技术(Network-based Detection and Response,NDR)
- 终端检测响应技术(Endpoint Detection and Response,EDR)
  - 基于终端大数据分析的新一代终端安全产品，能对终端行为数据进行全面采集、实时上传、对终端进行持续检测和分析、增强对内部威胁事件的深度可见性，结合相关威胁情报中心推送的情报信息(IP、URL、文件Hash等)能帮助企业快速发现，精确定位高级威胁入侵

5.2 如何分析APT攻击

- 网络杀伤链模型(Cyber Kill Chain)
  - 侦察
    - 攻击者选择目标、进行研究、搜集目标弱点
  - 武器化
    - 攻击者创建针对一个或多个漏洞定制的远程访问恶意程序武器，比如病毒或蠕虫
  - 散布
    - 将网络武器包向目标投放
  - 恶用
    - 在受害者系统上运行代码
  - 设置

        - 在目标位置安装恶意程序
    - 命令和控制
        - 为攻击者建立可远程控制目标系统的路径
    - 目标达成
        - 攻击者远程完成其预期效果
- 钻石模型
    - 攻击者
        - 分清攻击者有利用了解其目的、归属、适应性和持久性
    - 能力
        - 事件中使用的工具或技术
    - 基础设施
        - 攻击者用来传递能力的物理或逻辑结构，如IP地址、域名、邮件地址、USB设备等
    - 受害者
        - 以社会-政治为支点的安全分析中，受害者作用重大
- 自适应安全架构(Adaptive Security Architecture,ASA)
    - 由美国安全公司Gartner于2014年提出的面向未来的下一代安全架构，从预测、防御、检测、响应四个维度，强度安全防护是一个持续处理、循环的过程，是细粒度、多角度、持续化地对安全威胁进行实时动态分析
    - 目的：为了解决当前企业的安全防护功能难以应对高级定向攻击的问题
    - 最终效果：达到网络安全的可管、可控、可视、可调度、可持续

5.3 协同联动的纵深防御体系

- 高级安全威胁的判定
    - 结合多源头威胁情报应用、沙箱动态行为发现、关联引擎分析
- 安全威胁的处置
    - NDR与EDR联动

六、APT攻击技术(趋势)

6.1 技术越发高超

- 非PE文件文件攻击
    - 文件无需长期驻留磁盘
    - 核心Payload存放在网络或注册表
    - 通过系统进程执行Payload
- 开源工具和自动化攻击框架
    - PowerShell自动化攻击框架
    - CobaltStrike
        - Shellcode
        - Beacon
    - Koadic
- "Living off the land"技术

6.2 国际冲突地区的APT攻击更加活跃

- 能源资源、工业、持有不同政见者
- 这类APT组织：黄金鼠、人面狮、APT33、APT34等

6.3 网络空间已成为大国博弈新战场

- 影响面：政治、经济、军事谈判等

6.4 针对基础设施的破坏性攻击日益活跃

- “互联网+”、5G、万物互联等新兴技术的兴起
- 涉及行业：能源、交通、制造、金融、通信等领域
- 现状：很多基础设施和生产系统的网络安全体系建设还基本为零

6.5 针对个人移动终端攻击显著增加

- iOS、Android
- 系统漏洞、社会工程学
- 典型例子：“三叉戟漏洞”

七、典型的APT组织机构

方程式、索伦之眼、APT28、Lazarus、Group123

八、国家APT组织网络攻击

从作用意义上看，“震网”事件开辟了国家间APT攻击的先例，也展现了国家支持的有组织网络攻击的巨大战略效应。透过“震网”攻击事件整个过程，我们可以发现，国家APT组织网络攻击体现了**跨域协同**的鲜明特征，这也是其有效发挥作用的主要支撑条件。按照由低到高的层次，国家APT行动组织的跨域协同主要体现在四个维度。

8.1 行动维度，“人+工具”的跨专业协同

在“震网”事件中，“人+工具”的跨域协同动作主要体现在两个方面。

一是“工控系统专家和病毒开发人员”专业协同。在病毒研制阶段，首先，美国和以色列情报部门针对伊核电站进口的德国西门子工业控制系统进行了全面剖析，掌握各种控制器件的拓扑结构和指控传输方式，为病毒的摆渡传播奠定基础。同时，利用截获的利比亚同款离心机，开展拆解研究，以开发针对性破坏病毒代码，为病毒武器能够实质发挥作用提供了试验和效果验证目标环境。

二是“内鬼和工具投放”的技战术协同。据雅虎新闻披露，“震网”病毒的投送是通过伊朗核设施的内鬼完成的。在美国中央情报局和以色列情报机构摩萨德的要求下，由荷兰情报机构招募的一名伊朗工程师提供了关键数据，帮助美国开发人员将代码对准纳坦兹的系统。并在需要使用USB闪存驱动器将“震网”病毒植入这些系统时，由这个内应提供了急需的内部访问，在此基础上，震网病毒利用工控系统漏洞实现了对隔离网站的进一步入侵与破坏攻击。

8.2 供应链维度，实现了多领域的跨行业协同

此次雅虎新闻网站披露，德国西门子公司在“震网”事件中提供了生产所用工业控制系统的技术规范和知识，这些系统在伊朗工厂用于控制旋转离心机，法国提供了类似的情报，并且“震网”病毒利用了四个0day漏洞对伊朗核设施进行长期而隐蔽的破坏行动，在系统硬件、软件和漏洞利用多个行业领域实施了跨域协同。另外，荷兰情报机构AIVD以及美国和英国的情报机构，渗透了巴基斯坦科学家阿卜杜勒·卡迪尔汗的欧洲顾问和前线公司的供应网络，这些公司帮助在伊朗和利比亚建立核计划。

这种渗透不仅涉及特工手段，而且还采用了黑客行动，这些多行业多领域协同行动为获取伊朗核设施的研发计划和技术进程提供了必要的情报支持。从病毒攻击过程看，首先，病毒入侵环节，用于嵌入工控系统和离心机的电子设备，发现并定位攻击的具体部位，这取决于对入侵目标机理的充分掌握。其次，病毒破坏环节，美国、以色列研发的病毒武器能够对核设施的核心控制程序如电机、阀门、开关、电路实施针对性破坏性操作。

8.3 政治维度，“实体空间与网络空间”跨域协同

“震网”病毒作为美国“奥运会”工程秘密行动的重要组成，其目的不是为了彻底摧毁伊朗的核计划，而是将其暂时搁置一段时间，以便为制裁和外交生效腾出时间。从效果上看，该战略成功地帮助伊朗进入谈判桌，并最终在2015年与该国达成协议。而在“震网”病毒的研制过程中，美西方国家政治方面举措也为“震网”病毒的精心设计准备提供了充足的时间。

早在2000年，伊朗在纳坦兹计划建造一座可容纳5万台旋转离心机用于浓缩铀气的设施时，AIVD就入侵了伊朗一个重要国防组织的电子邮件系统，以获取更多有关伊朗核计划的信息。并在接下来的两年里，以色列和西方情报机构一直在秘密监视纳坦兹核项目的进展，直到2002年8月，一个持不同政见的伊朗团体使用情报机构提供的信息，在华盛顿举行的新闻发布会上公开曝光了伊朗的核项目，国际原子能机构核查人员要求进入纳坦兹，伊朗被迫同意停止在纳坦兹的一切活动。2004年全年和2005年的大部分时间，伊朗一直处于暂停状态。在此期间，“震网”病毒攻击代码进行了长时间的开发，于2006年对离心机进行了一次破坏试验，将试验结果提交给了当时美国总统乔治•布什，由此批准了“震网”攻击计划，并根据情况，后续对攻击代码进行了多次修改编辑，为真正实施攻击作好了武器和政策准备。

8.4 国际维度，实现了跨国跨部门的国家间协同

美国、以色列在网络空间广泛存在的同盟机制，成为其实施国家间跨域协同的重要保障。“奥运会”工程是一个多国多部门参与的国际性网络空间攻击破坏行动，主要是美国和以色列联合实施，涉及美国国家安全局、中央情报局和以色列摩萨德、国防部、SIGINT国家部队(相当于以色列的国家安全局)。另外，美国和以色列还得到了荷兰、德国、法国其他三个国家的援助，因此使用了“奥运会”工程代号，标志着五环国家。从作用上看，美国、以色列主导了整个攻击活动组织以及病毒武器开发，德国、法国提供了供应链上情报支撑，荷兰提供有关伊朗从欧洲采购非法核计划设备活动的关键情报和有关离心机本身的信息，以及特工渗透的实际行动支撑。除了在研发针对性病毒攻击代码过程中，多个国家协同行动之外，在截获其他国家同款离心机以及在荷兰发展伊朗间谍的关键行动过程中，多个国家也互相协同，促成了有关行动任务的顺利达成。

九、震网传播方式

震网的传播主要包括两种方式，一种是移动设备感染，利用LNK漏洞或者通过autorun.inf文件进行传播；另一种是网络传播，涉及WinCC数据库感染、网络共享传播、打印机后台处理程序漏洞传播、Windows服务器漏洞传播等多种方式。这两种传播方式虽然不同，但最终都会释放主DLL文件，进行后续的安装和执行操作。震网感染目标系统后，会启动RPC服务器监听网络，将网络上其他感染计算机都连接到RPC服务器，并查询远程计算机安装的震网版本，以执行对等通信和更新，如果远程计算机上的震网版本较新，则本地计算机就会请求新版本并自我更新，如果远程机器上的震网版本较旧，则本地计算机上的震网就将自身副本发送给远程机器。这样，震网可以在任何感染机器上更新并最终传播到所有机器。

十、安全建议

此次攻击事件凸显了两个问题：

- 即便是物理隔离的专用局域网，也并非牢不可破；
- 专用的软件系统，包括工业控制系统，也有可能被攻击。

因此，我们对有关部门和企业提出下列安全建议：

- 加强主机（尤其是内网主机）的安全防范，即便是物理隔离的计算机也要及时更新操作系统补丁，建立完善的安全策略；
- 安装安全防护软件，包括反病毒软件和防火墙，并及时更新病毒数据库；
- 建立软件安全意识，对企业中的核心计算机，随时跟踪所用软件的安全问题，及时更新存在漏洞的软件；
- 进一步加强企业内网安全建设，尤其重视网络服务的安全性，关闭主机中不必要的网络服务端口；
- 所有软件和网络服务均不启用弱口令和默认口令；
- 加强对可移动存储设备的安全管理，关闭计算机的自动播放功能，使用可移动设备前先进行病毒扫描，为移动设备建立病毒免疫，使用硬件式U盘病毒查杀工具。

十一、攻击事件的特点

相比以往的安全事件，此次攻击呈现出许多新的手段和特点，值得特别关注。

11.1 专门攻击工业系统

Stuxnet蠕虫的攻击目标直指西门子公司的SIMATIC WinCC系统。这是一款数据采集与监视控制（SCADA）系统，被广泛用于钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域，特别是国家基础设施工程；它运行于Windows平台，常被部署在与外界隔离的专用局域网中。
一般情况下，蠕虫的攻击价值在于其传播范围的广阔性、攻击目标的普遍性。此次攻击与此截然不同，最终目标既不在开放主机之上，也不是通用软件。无论是要渗透到内部网络，还是挖掘大型专用软件的漏洞，都非寻常攻击所能做到。这也表明攻击的意图十分明确，是一次精心谋划的攻击。

11.2 利用多个零日漏洞

Stuxnet蠕虫利用了微软操作系统的下列漏洞：

- RPC远程执行漏洞（MS08-067）
- 快捷方式文件解析漏洞（MS10-046）
- 打印机后台程序服务漏洞（MS10-061）
- 尚未公开的一个提升权限漏洞

后三个漏洞都是在Stuxnet中首次被使用，是真正的零日漏洞。如此大规模的使用多种零日漏洞，并不多见。
这些漏洞并非随意挑选。从蠕虫的传播方式来看，每一种漏洞都发挥了独特的作用。比如基于自动播放功的U盘病毒被绝大部分杀毒软件防御的现状下，就使用快捷方式漏洞实现U盘传播。
另一方面，在安天捕获的样本中，有一部分实体的时间戳是今年3月。这意味着至少在3月份，上述零日漏洞就已经被攻击者掌握。但直到7月份大规模爆发，漏洞才首次披露出来。这期间要控制漏洞不泄露，有一定难度。

11.3 使用有效的数字签名

Stuxnet在运行后，释放两个驱动文件：

- %System32%\drivers\mrxcls.sys
- %System32%\drivers\mrxnet.sys

这两个驱动文件使用了RealTek的数字签名（图11）以躲避杀毒软件的查杀。目前，这一签名已经被颁发机构吊销，无法再通过在线验证，但目前反病毒产品大多使用静态方法判定可执行文件是否带有数字签名，因此有可能被欺骗。