（上接第一版）

动管理与资源保障）、Preparation（行动准备筹措）、Engagement（接触目标与进攻突防）、Presence（持久化驻留潜伏）、Effect（致效能力运用）、Ongoing Processes（全程持续支撑作业）为步骤，通常结合人力作业、物流与仓储劫持、供应链攻击、摆渡攻击等多种方式，依托其制式化、全平台、高能力的网空攻击装备体系实现了可针对各种端点设备、网络设备、网络安全设备的全IT场景覆盖。

面对高能力/超高能力网空威胁行为体的网络威胁，在具备有效防御体系的基础上，实施持续常态化威胁猎杀，能够提高保障等级。尤其是在缺失有效防御体系的情况下，更需要针对潜伏的威胁展开“威胁猎杀”（Threat Hunting）行动，从而做到对突防威胁的“找出来”和“赶出去”。

在威胁猎杀的相关理论研究和实践方面，国际上已经有很多前沿探索，其中美国走在世界前列。早在2016年初，美国国防部就已经高度重视威胁猎杀工作，呼吁业界加强对其猎杀工作的支持，并呼吁业界向其提供用于猎杀网络潜在威胁的各种支撑工具。基于网络信息系统的重要程度、安全预算、所面临的威胁等级等因素的综合考量，威胁猎杀可以分为两种：一种是美国国防部所指的常态化的威胁猎杀，适用于各种重要的网络系统，以应对高/超高能力的网空威胁行为体；另一种就是临时化的威胁猎杀，用于应对各种突发性威胁/严重威胁，这种临时化的威胁猎杀更具挑战性。当然，由于威胁猎杀工作往往需要付出极高的成本，“猎杀”范围一般只针对高价值系统。临时化的威胁猎杀往往是无奈之举，在资源充足的情况下，应该进行常态化的威胁猎杀，这也是未来的趋势。

大国博弈背景下的网络战威胁形势日益严峻，威胁猎杀是有助于关键信息基础设施、重要部门和大型政企单位降低网络安全风险隐患的有效应对方法，使其即使面对高能力网空威胁行为体也能达到“防患于未然”的要求。当前最重要的举措，正是开展能力导向建设模式的规划与建设工作，构建针对已知威胁的有效防护能力，支撑猎杀未知威胁的体系化防御措施。本文将就威胁猎杀的重要性以及如何做好威胁猎杀工作，提出一些思考和具体实施方法。

威胁猎杀概述

从防御者视角看，威胁猎杀是积极防御层面一种主动和迭代的威胁检测方法，不同于攻击者已经完成攻击并对业务系统造成严重损害后（即所谓“事后环节”）才采取行动的取证、分析、处置工作，威胁猎杀是针对突防后潜伏状态的威胁，是在“潜伏的事中”、“攻击破坏或盗取信息的事前”。结合“NSA/CSS技术网络空间威胁框架V2”，从攻击者视角看，网络战或网络攻击造成的后果将表现在Effect阶段。Effect阶段是整个威胁攻击过程中决定性的一环，而威胁猎杀所针对的作业阶段是Presence阶段以及Ongoing Processes阶段中的命令与控制、规避等活动。

威胁猎杀整体运行方法

威胁猎杀是一种协同配合的工作方法，基于工作性质、工作重点部位与参与人员组织，安天将威胁猎杀划分为威胁猎杀分析、现场协同与后台支撑服务、现场排查三个层面。这三个层面相应人员在负责各自工作的同时，也会根据其他层次的输入信息进行工作，并生成相应的输出信息给予不同的层面，实现三个层次相互之间的协同联动进而展开威胁猎杀工作。

威胁猎杀分析层：由威胁猎杀分析师完成此部分工作。威胁猎杀初期，需要准备信息采集需求和部署方案，并向现场下发观测信息采集节点部署需求。

现场协同与后台支撑服务层：现场工程师协同系统管理员、控制工程师、安全管理员完成现场协同，逆向分析工程师为现场协同提供后台支撑服务。

现场排查层：基于下发的特征包及其加载指南、专查工具及其使用手册，指挥协调员协同客户系统管理员、安全管理员、控制工程师以及厂商维护工程师完成现场排查工作。

小结

对于像电力基础设施这样的复杂的关键信息基础设施和重要网络信息系统，需要把尝试罗列各种可能的网空威胁并设计零散防御措施进行被动应对的传统式威胁导向建设模型，演化为全面建设必要的网络安全防御能力，并将其有机结合以形成网络安全综合防御体系的能力导向建设模型。安天基于著名网络安全研究机构SANS的“滑动标尺”模型，提出了叠加演进的网络空间安全能力模型。其中基础结构安全类别的能力，来自于在信息化环境的基础设施结构组件以及上层应用系统中所实现的安全机制，兼具安全防护和系统保障的双重意义，主要作用是有效收缩信息化环境中基础设施所存在的攻击面。纵深防御类别的安全能力，来自于附加在网络、系统、桌面使用环境等信息技术基础设施之上综合的体系化安全机制，以“面向失效的设计”为基本原则构建防御纵深，通过逐渐收缩攻击面以有效消耗进攻者资源，从而实现将中低水平的攻击者拒之门外的防御作用。在保障安全能力的“深度结合”、“全面覆盖”基础上，建设以态势感知为核心的威胁情报驱动的动态防御能力体系，做到“掌握敌情”、“协同响应”，重点是在敌情想定的基础上提升网络系统的可弹性恢复水平，特别是依靠具有动态特性的积极防御能力，在威胁情报能力的驱动下，通过全面持续监控发现威胁踪迹，并针对潜伏威胁展开“猎杀”行动，从而发现并消除威胁。

安天已经连续六届、十二年蝉联国家级网络安全应急服务支撑单位资质，是中国网络安全应急体系的重要企业节点。安天CERT基于多年的恶意代码检测、APT攻击对抗与深度分析等技术积累，依托产品体系、支撑体系和威胁情报赋能，为客户提供监测分析、安全保障和应急处置等特色化安全服务。在逆向分析方面，具备依托安天大规模自动化分析处理体系的逆向分析、关联分析、同源分析平台的人机协同能力，及对“白象”等网空威胁行为体追踪溯源到自然人的成功案例。在威胁情报方面，具备对多源异构威胁情报数据的采集、分析、处理能力。这些均为有效开展威胁猎杀提供了基础支撑能力。由安天CERT的威胁猎杀分析师、取证工程师、逆向分析工程师、情报工程师所组建的专业威胁猎杀团队，正在积极开展威胁猎杀实践。

微信扫描二维码阅读全文

安天周观察
安天官方微博 安天官方微信
主办：安天 2019年07月22日(总第192期)试行 本期4版 微信搜索：antiylab 内部资料 免费交流

实战化威胁猎杀 让威胁无处遁形

--“美向俄电网植入恶意代码”等有关报道带来的启示

背景

2019年6月16日，美国《纽约时报》爆料称，美政府官员承认早在2012年就已在俄罗斯电网中植入病毒程序，可随时发起网络攻击。报道随即引发相关国家的高度关注和国际舆论的广泛猜测。尽管美国总统特朗普第一时间否认了《纽约时报》的报道，但世界仍普遍担忧网络冷战甚至热战距离人类越来越近。俄方对此表示，“美国设想对俄发动网络战”的可能性是存在的。据《纽约时报》报道，美方瞄上俄电力系统，是因为“美国网络司令部研究了俄方在2020年美总统选举期间切断选举关键州供电的可能性，并认为美方需有相应的遏制办法”。俄战略规划与预测研究所所长古谢夫则表示，美方（向俄方电力系统）植入恶意代码与“保护2020年美国总统选举”毫无关系，其真实目的就是压制俄罗斯。如果美国确实企图向俄电力系统植入恶意程序代码，则应把该行为视作对俄方的直接威胁。

电力基础设施是关键基础设施至关重要的组成部分。一个国家的电力系统安全不仅关系到电网的稳定运行，也关系到国家能源安全和国计民生，甚至关系到国家的利益和安全。由于电力系统具有结构复杂多样、分布广泛、重要性高的特点，一旦系统瘫痪则影响巨大，因而极易成为网空攻击的首选目标。例如，2015年12月23日，乌克兰电力系统遭受网络攻击，造成大规模停电事故，影响波及8万家庭；2019年3月7日开始，委内瑞拉国内包括首都加拉加斯在内的大部分地区停电超过24小时，委总统马杜罗指出，大规模停电是美方网络攻击造成的，随后连续多日大规模停电造成民众严重恐慌，引发社会秩序混乱；2019年6月16日，阿根廷和乌拉圭因互联电网发生“大规模故障”导致全国性停电，乌拉圭乌特电力公司称“具体故障原因仍有待查明，不排除是网络攻击导致”。

2019年6月21日，根据雅虎新闻报道，美国两名情报官称，美国对伊朗一个网络组织发动了网络攻击。而2019年7月13日，美国纽约发生了大规模停电事故，随后则又开始有攻击来自于伊朗的各种传闻。

上述种种都表明在网络攻防对抗中，对于高能力/超高能力威胁行为体行动的感知普遍有限，溯源十分困难，因而防御工作无法做到有的放矢。而且，这种对涉及国家安全风险的认知缺失或认知错误，极易引发战略上、战术上的误判，甚至可能造成不可挽回的后果。2018年，特朗普已授权美军网络司令部可在未获总统批准的情况下直接实施攻击性网络行动。简化网络攻击授权，凸显了美方所谓的“积极防御”实为先发制人的打击战略，网络进攻性色彩愈加浓厚。作为被美方明确列为的“竞争对手”，我国家关键信息基础设施的网络安全防护形势日益严峻，常态化网络安全防护工作的迫切性日益突显。

针对电力系统等关键信息基础设施面临的突防威胁，应基于叠加演进模型构建动态综合网络安全防御体系，以基础结构安全和纵深防御为主体的综合防御体系为基础，叠加动态的积极防御以应对高级复杂威胁。基础结构安全与纵深防御能力需要具有“深度结合、全面覆盖”的综合防御特点，积极防御与威胁情报能力需强调“掌握敌情、协同响应”的动态防御特点。

但是目前我国关键信息基础设施防护体系尚存在各个方面能力的缺失。以电力设施为例，在基础结构安全方面，为了保障电力系统业务的连续性和稳定性，对系统进行更新升级、打补丁等安全动作有着近乎苛刻的谨慎，大量陈旧漏洞成为暴露在外的威胁敞口，都会给攻击者以可乘之机；在全面纵深防御方面，很多工控网络并没有建立起有效的纵深防御体系，依然采用单纯依赖物理隔离的方式维持网络信息系统安全，而大量事实证明，仅靠物理隔离难以在网络空间有效对抗高能力对手的威胁；在积极防御方面，多数电力企业尚未部署全要素信息采集、异常监控、深度分析等安全系统，无法感知网络安全态势。此外，为了保障电力系统的正常运行，无法采用自动化的威胁响应机制，无防护甚至不安全的远程访问等问题的客观存在均为系统安全埋下了巨大隐患。我方目前普遍存在的网络防护现状不仅防不住高能力网空威胁行为体的攻击，而且无法确定是否“敌已在内”。

在网络攻击方面，美方一直秉承“建立全面的植入和持久化能力”的理念，强调对各种场景的全面穿透能力，为长期的信息窃取和日后可能的网络战做准备。一旦在目标系统达成持久化，攻击者能够实现随时从计算机网络利用（即CNE）到计算机网络攻击（即CNA）的无缝切换，对目标网络进行破坏和摧毁。美方具有全球最强的体系化网络攻击能力。在复杂的组织机构、庞大的人员规模和充沛的预算保障下，美方建设了一系列大型的信号情报获取和作业的工程系统，研发了制式化装备体系，建立了支撑网空情报活动和攻击活动的框架，将情报获取、进攻作业、积极防御等网空能力整合成整体国家能力。在网空作业时，美方以Administration（行

（下接第四版）

每周安全事件

类 型	内 容
中文标题	Hawkeye 活动使用 Visual Basic 打包器反调试技术
英文标题	Anti-Debugging Techniques from a Complex Visual Basic Packer
作者及单位	ZLAB-YOROI
内容概述	Hawkeye Keylogger 是一个在暗网上出售的信息窃取恶意软件，自 2013 年以来，其不断增加新的功能和技术。近期攻击者使用了 Visual Basic 打包程序强制执行的反调试技术。投递文件为 ISO 映像，具有较低的 AV 检测率，其内部有一个 PE 文件伪装的 bat 文件。PE 文件使用 VB 5.0 编写，用于保护恶意软件核心部分，并使分析难度加大。在新分配区域内的上下文切换之后，恶意软件采用“ GetTickCount（） ”反调试技术。其会检索自系统启动以来经过的时间，以毫秒计算，如果高于预设阈值，恶意软件会终止执行。
链接地址	https://blog.yoroi.company/research/anti-debugging-techniques-from-a-complex-visual-basic-packer/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.FakeBank.x[prv,exp,rmt] 2019-07-14	高	该应用程序伪装为银行相关，运行请求激活设备管理器，生成伪随机密码诱导用户使用，联网上传设备信息、短信信息等隐私内容，拦截短信，解析短信指令执行相关操作，私自发送短信，造成用户的资费消耗和隐私泄露，可能造成用户的财产损失，建议卸载。
		G-Ware/Android.Bianlian.a[exp,rog] 2019-07-15	中	该应用程序伪装正常应用，实际联网接收指令，随机变换使用界面，推送第三方贷款、投资理财类产品，该类服务没有安全保障、可能造成用户财产损失，建议卸载。
		RiskWare/Android.FakeSamSungUpdate.a[exp,fra] 2019-07-16	中	该应用程序伪装 SamSung 更新服务，运行频繁推送广告，下载更新会跳转第三方更新平台，该平台通过限速诱导用户选择付费下载，牟取利益，请谨慎使用。
	较为活跃样本	Trojan/Android.Jiakey.a[prv,rmt,spy]	中	该应用程序是一款间谍软件，运行后接收远程控制命令，窃取用户短信、联系人、通话记录、手机基本信息，地理位置，社交软件信息，请求 root 权限，私自拍照、录音、录像，并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.MLogger.a[prv,exp]	中	该应用程序能够隐藏图标，运行收集用户手机的短信、彩信、通话记录和 app 列表等日志信息，并上传至服务器，请用户谨慎使用，非自主安装建议卸载。
		Trojan/Android.huanji.a[exp,prv,bkd]	中	该应用程序包含恶意代码，会联网获取杀毒软件列表逃避检测，模拟点击恶意创建快捷方式，上传用户设备等隐私信息，并且留有后门，能联网下载并静默安装任意应用，恶意刷量，发送大量网络请求，造成用户资费损耗和隐私泄露，建议卸载。
		G-Ware/Android.FakeApp.go[fra,exp]	中	该应用程序伪装正常应用，运行加载色情界面，诱导点击下载色情样本，请注意提示信息，使用健康绿色软件。
		Trojan/Android.Locker.bs[rog,lck]	低	该应用程序运行激活设备管理器，修改锁屏 PIN 码，致使用户手机无法正常使用，建议卸载该应用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows DHCP 服务器远程代码执行漏洞（CVE-2019-0785）	高	当攻击者向 DHCP 故障转移服务器发送经特殊设计的数据包时，Windows Server DHCP 服务中存在内存损坏漏洞。成功利用此漏洞的攻击者可以在 DHCP 故障转移服务器上运行任意代码或者导致 DHCP 服务无响应。
	较为活跃样本	Trojan[Backdoor]/MSIL.Bladabindi	中	此威胁是一种使用 C# 语言编写的具有后门行为的木马家族。该家族的样本为 NJ Rat 远控所生成的被控制端，在执行后会与远程服务器通讯并接收远程服务器的控制。该样本可能具有窃密行为和破坏行为。
		Trojan[SMS]/J2ME.Agent	中	此威胁是一种基于 Java ME 架构的木马。该家族的样本在执行后会在后台发送付费的短信，使用户的财产受到损失。同时该样本还会收集用户设备上的信息并回传。
		RiskWare[NetTool]/MSIL.NetFilter	中	此威胁是一种风险软件家族。该家族的样本在执行后会在启动项添加自身、同时注入其他进程、更改浏览器设置、安装浏览器扩展并添加一个代理设置。
		RiskWare[Server-Proxy]/Win32.Sock4Proxy	中	此威胁是一种具有代理功能的风险软件家族。该家族的样本在执行后会利用远程的服务器作为代理服务器，劫持用户的网络流量。
		GrayWare[AdWare]/Win32.Suppad	低	此威胁是一种基于 Windows 32 位平台的具有广告行为的灰色软件程序。该家族的样本在执行后会在通知区域和浏览器中弹出广告，影响用户的使用体验。

如何识别网络钓鱼

Kelly Sheridan/ 文 安天技术公益翻译组 / 译

先进的网络钓鱼技术和糟糕的用户行为会加剧网络钓鱼攻击成功的威胁。

教导员工如何识别恶意电子邮件，是防止网络钓鱼攻击的众多步骤之一。但是，随着攻击者采用更先进的技术，安全团队除了要识别通过邮件的网络钓鱼行为，还要了解不通过邮件的网络钓鱼，也就是不局限于电子邮件这一个途径。

在第四期《识别网络钓鱼》（Beyond the Phish）年度报告中，Proofpoint 公司的研究人员从 2018 年 1 月 1 日到 2019 年 2 月 28 日之间提交给其安全教育平台的近 1.3 亿份回复中，提取了相关数据。而在 2019 年最新的测试中，该公司采用了新扩展的、更高级的网络安全试题；因此难以将其结果与之前年度的结果进行对比。

模拟通过邮件的网络钓鱼攻击是一种方便的方法，可用于评估用户的一部分弱点，但不能完全反映员工对网络钓鱼的理解程度。毕竟，通过查看他们在模拟的网络钓鱼攻击中是否会上钩，安全团队无法了解其口令安全性、移动设备安全性或机密数据安全性。因此，他们还需要回答问题。

“我们不仅分析网络钓鱼攻击，还会更广泛地分析影响企业网络安全态势的环境和行为。”Proofpoint 公司安全意识和培训策略师格雷泰尔 · 伊根（Gretel Egan）说，“除了电子邮件，还有很多行为和风险会影响企业的网络安全态势。”

今年，员工的测试内容涵盖 14 道题。平均而言，回答错误率是 22%——而 2018 年的错误率为 19%。伊根表示，鉴于测试题目的扩展和问题难度的增加，错误率的上涨并不令人意外。她说，正确率的下降并不意味着员工安全意识的缺乏；而是说明一些企业开始提高测试难度。

“这说明测试题目的复杂程度有所增加，以及员工对网络钓鱼、数据保护以及网络安全相关合规指令的理解上存在细微差距。”她解释道，“这比仅进行电子邮件钓鱼测试更加有效。”

错误率最高的问题是：“识别网络钓鱼威胁”（25%）、“在数据的整个生命周期中加以保护”（25%）、“合规相关的网络安全指令”（24%）以及“保护移动设备和信息”（24%）。而正确率最高的是：“避免勒索软件攻击”（11%）、“口令和账户鉴别”（12%）和“无意和恶意内部人员威胁”（13%）。

在移动设备加密、保护个人身份信息（PII）、阻止社会工程攻击的技术、区分公共数据和私有数据，以及应对可疑物理安全漏洞等问题上，员工表现较为吃力。

而在识别潜在风险通信渠道、旅行时的物理安全保障、识别勒索软件和恶意弹出窗口，以及与蓝牙配对相关的风险等问题上，员工的表现较好。

伊根指出，员工无意识的一些行为会使雇主面临风险并加剧网络钓鱼威胁。例如，在社交媒体上过度分享信息，如员工的一篇帖子说“老板本周出差”可能看起来没什么不妥，但对攻击者而言可能就是有价值的信息。

“我们还发现，对于在本地设备上的行为如何影响企业数据（有时是个人数据）的安全性，员工的了解不够。”她继续道。企业对员工开展了如何使用设备的培训，但是这些培训侧重功能方面，而非安全方面。举例来说，员工让家庭成员使用公司设备，以及使用同一台设备处理个人和公司事务等常见行为，都会导致敏感信息面临风险。

攻击者采用更高级的钓鱼策略

网络安全公司 INKY 在《2019 特殊网络钓鱼报告》指出，随着网络犯罪分子采用更高级的钓鱼策略，对员工开展有关安全行为的培训越来越有必要。

INKY 公司首席执行官戴维 · 巴格特（Dave Baggett）说：“攻击者技术的进化令人震惊。”

“就攻击趋势而言，我们看到了大量的假冒厂商电子邮件，其目标是获取用户凭证。”他继续道。攻击者经常将电子邮件伪装成来自合法的微软或亚马逊账户，诱骗用户在伪造的登录页面上输入凭证。获取用户名和口令之后，他们会尝试登录用户的网银账户或网络邮件账户。

他补充道，很多人认为网络钓鱼攻击都是很复杂的，但实际上很多钓鱼攻击并不复杂。例如，假冒厂商“是非常容易的”，巴格特说。而更高明的攻击者则知道安全电子邮件网关（SEG）是如何运作的以及如何绕过它们。

巴格特说，攻击者的一种隐蔽策略是“隐藏文本”——即将恶意代码隐藏到电子邮件中。如今，大多数电子邮件是使用 HTML 设计的，这种设计很复杂，SEG 很难恰当解析，因此电子邮件客户端很难确定用户会看到什么。这为攻击者提供了将恶意内容“绕过”SEG 的机会。

SEG 经常扫描特定的厂商名或文字，以识别涉嫌假冒厂商的电子邮件。而网络犯罪分子的应对方法是：在字母或短语之间插入用户不可见的随机小号白色（也就是背景颜色）字母，以绕过 SEG 的扫描。通过添加对 SEG 安全系统和最终用户不可见的乱码文本，钓鱼邮件就能绕过 SEG 的监控，进入毫无戒心的用户的收件箱。

一些攻击者创建的电子邮件还有会话，而且不添加附件或链接，以绕过 SEG。使用传统垃圾邮件过滤技术的安全工具，很可能不会阻止假冒 CEO 或供应商的攻击者的邮件。

原文名称	How to Catch a Phish: Where Employee Awareness Falls Short
作者简介	Kelly Sheridan。Kelly Sheridan 是 Dark Reading 的编辑。
原文信息	2019 年 7 月 11 日发布于 Dark Reading。 原文地址 https://www.darkreading.com/risk/how-to-catch-a-phish-where-employee-awareness-falls-short/d/d-id/1335228
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。