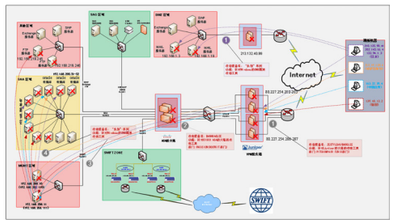
2020 年 6 月 29 日 (总第 236 期 试行)
邮箱：antiynews@antiy.cn

（上接第三版）

维，利用多源威胁情报和私有化生产的内部情报，赋能客户，协助客户开展网络安全防御体系的构建和防御能力的持续提升。



▲“方程式组织”对 EastNets 网络的总体攻击过程复盘（2019）

2019 年，安天接连捕获到多批针对南亚多国军事、政府和教育等实体的攻击样本，且样本之间存在一定关联，攻击者带有明显窃密意图，受害者集中于巴基斯坦等南亚国家。这些攻击样本来自被安天命名为“幼象”的组织（考虑到组织攻击手法简单、载荷还不成熟等特点，因此将其命名为“幼象”），其手法和装备与“白象”组织有一定差异，并于 2020 年 1 月 15 日正式发布《“折纸”行动：针对南亚多国军政机构的网络攻击》。

这十年，安天 CERT 分析了大量的 APT 事件，在分析以及追踪溯源过程中，遇到过挫折，也获得了经验。在与 APT 和 A^{2}PT 攻击分析对抗中，逐渐**开始将“敌已在内”作为基础的敌情想定，认识到防御方应充分考虑防御措施失效的情况，以“面向失效的设计”为基本原则指导防御。在合理网络结构上叠加纵深布防的防御措施、监测措施是限制、阻断、延缓攻击行动的有效方法。**

总结（威胁动态演进，安天砥砺前行）

当前网络空间领域的斗争已经是大国博弈和地缘安全中的常态化存在，网络空间更是政治、军事、经济等领域斗争的首发战场。我国所面临的全球和地缘安全风险，既以大国竞合为主旋律，同时又围绕地缘安全热点展开，地缘利益竞合方众多，多种矛盾复杂交织。网络安全威胁不是单纯的技术风险，其风险和事件研判也不是单纯的领域内研判，这与攻击发起方和潜在对手的战略意图、技术能力和综合国力等综合因素息息相关。过去的安全威胁是单点威胁，例如病毒、木马、DNS 攻击、网站篡改等。如今随着信息技术越来越先进、信息体系越来越复杂、信息资产越来越庞大，安全威胁也在不断发展演进。我们对过去遭遇到的网络入侵攻击，往往将其作为单纯的网络安全事件看待，而未结合总体国家安全的多个方面进行综合分析，对对手意图的分析深度不足。未来，需要对网络攻击行为给我国政治安全、军事安全、科技安全等带来的综合影响后果全面加强研判，实现综合分析、全面量损、有效止损。

未来的网络安全工作应遵循“网络安全是整体的而不是割裂的”、“是动态的而不是静态的”、“是开放的而不是封闭的”、“是相对的而不是绝对的”、“是共同的而不是孤立的”的主要特点，在进一步的投入中提升系统性、及时性和针对性，解决不平衡不充分的安全建设导致的国家安全能力短板和失衡。

面对安全威胁，必须形成有效的防御能力。在信息化发展中，很多存量系统在建设时大多没有充分考虑到网络安全问题，需要投入大量的“补课”成本。随着数字经济的蓬勃发展，云计算、5G、人工智能、IoT 等技术的进步，在新一代信息技术演化生成的基础设施、支撑传统基础设施转型升级以及创新基础设施为代表的新基建内涵更加丰富，涵盖范围更加广泛，更能体现数字经济的特性，更好的推动中国经济转型升级，同时也对安全防护有更高的要求，在发展新基建的过程中，更需要网络安全同步规划、同步建设、同步运维的一套方法体系和相应的预算保障，也需要通过规划指引全面提升防御能力，通过预算投入支撑网络安全领域的能力建设，才能满足新基建的防御能力需求，保障承载中国数字经济的基础建设。

当前的网络安全防护水平和技术能力还有较大提升空间，以国土安全为视角，以应对信息战为要求，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。这个跟进的过程将是复杂、艰巨、且富有挑战的，不仅需要我们有“只争朝夕”的紧迫感，更需要我们“不负韶华”的努力。

微信扫描二维码关注公众号查看原文

谷歌删除了 106 个 Chrome 浏览器恶意扩展

周四，谷歌从 Chrome 网上应用店中删除了 106 个 Chrome 浏览器扩展，以回应有报道称这些扩展被用来窃取敏感用户数据。在同样于周四发布的研究报告中，Awake Security 声称数百万 Chrome 用户已成为威胁者的目标。攻击者不仅使用谷歌 Chrome 浏览器扩展来窃取数据，还在企业网络上建立了持久的立足点。浏览器扩展是免费的，设计用来提醒用户有问题的网站或文件转换器。据 Awake Security 估计，这些扩展总共被下载了 3200 万次。

（原文链接：https://threatpost.com/google-yanks-106-malicious-chrome-extensions/156731/）

研究人员开发语音检测技术以防止语音欺骗攻击

英联邦科学与工业研究组织（CSIRO）的 Data61 与三星研究公司（Samsung Research）和韩国成均馆大学（Sungkyunkwan University）共同开发了一种解决方案，可以保护消费者免受语音欺骗攻击。语音活性检测（Void）被设计成嵌入智能手机或语音辅助软件中，用于识别实时人声和通过扬声器回放的语音之间的差异，从而检测黑客是否试图欺骗系统。根据 Data61 的说法，与其他使用深度学习模型的语音欺骗技术不同，Void 依赖于从频谱图（频谱的可视化表示）中获得的洞察力来检测语音的“活性”。

（原文链接：https://www.zdnet.com/article/csiros-data61-develops-voice-detection-technique-to-prevent-voice-spoofing-attacks/）

攻击者可利用 AMD 的 Mini PC 漏洞执行任意代码

AMD 上周表示，它正在为一个漏洞准备补丁，该漏洞会影响使用某些笔记本电脑和嵌入式处理器的系统所附带的统一可扩展固件接口（UEFI）的系统管理模式（SMM）。该漏洞是由安全研究人员 Danny Odler 在 AMD 的 Mini PC 中发现的，并跟踪为 CVE-2020-12890，该漏洞是 4 月报告的三个问题之一，攻击者可以在避免检测的同时操纵安全固件和执行任意代码。

（原文链接：https://www.securityweek.com/amd-preparing-patches-uefi-smm-vulnerability）

安天周观察
安天官方微博　安天官方微信
主办：安天　2020 年 6 月 29 日 (总第 236 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

从反恶意代码到对抗高级威胁（下）

逐鹿十年——高级威胁 10 年分析回顾

2010 年随着震网事件曝光，网络攻击背后的网空国家 / 地区行为体开始浮出水面。其具备体系化作业能力，巨大成本的承受力，和坚定的作业意志。战略利益化促进了木马向攻击武器发展，从广泛覆盖到精准打击。2010 年至 2012 年安天投入大量的人力和时间对震网（Stuxnet）、Duqu（毒曲）、火焰（Flame）等进行马拉松式的分析，但部分分析成果却仅能覆盖不足 5% 的病毒模块，此事触发了安天对这种逐个逆向样本模块堆砌式分析的反思和自我批判，提出了要以工程体系对抗思维来看待 APT 分析工作。**2013 年开始，安天逐步从单纯的样本模块分析走向攻击装备的整体分析，进入到高级恶意代码体系分析阶段，并在有关专家的指导下引入威胁框架，努力从“只见树木，不见森林”的瓶颈中挣脱出来。**

●以样本分析视角启动 APT 时代分析（2010~2012）

2010 年 7 月 15 日，安天捕获到震网蠕虫 APT 的首个变种，并于 9 月 27 日发布了《对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告》，这是国内第一份针对该蠕虫的深度技术分析报告，成为国内公众了解“震网”攻击真相和细节的重要参考资料。2011 年，毒曲浮出水面后，安天工程师经过分析提出了毒曲和震网可能存在同源性的猜测。2012 年 5 月，“火焰”被发现，火焰是一个模块比震网更多的复杂组件化木马，且可能与震网存在关联。**该恶意代码被卡巴斯基称为“迄今为止最复杂的计算机病毒”**。安天成立了针对火焰的分析小组，开始了为期数月的马拉松式分析，发布了近 100 页的《Flame 蠕虫样本集分析报告》。但分析成果覆盖范围依旧非常狭窄，也触发了我们的反思和自我批判。

2010 年，随着震网重挫伊朗核进程，APT 成为热点话题，由于 APT 广泛使用 0day 漏洞、隐蔽通信、签名仿冒，加之攻击者承担成本能力之强大、攻击意志之坚决，前所未有，导致其对安全体系的冲击和造成的心理恐慌都到达了空前的程度。这种压力**驱动了传统反病毒厂商进行产品和技术的改进。安天基于业内产品经验逐步开始探索传统网络侧检测设备与沙箱结合的产品形态，**其核心价值不仅是将可执行对象直接投放到设备附带的虚拟环境中运行，进行行为判定，更重要的是利用这个虚拟环境实现利用不同的解析器版本，诱发文件格式溢出。基于这个理念安天推出了**追影威胁分析系统**。

虽然时隔多年，但震网事件一直在我们的研究视野，2019 年安天对震网事件进行了全面的复盘和反思，发现我们缺少一种真正意义上的框架化方法。在相关专家的指导下，我们对网空博弈、敌情想定有了新的体悟，逐渐从威胁框架视角进行方法论切换，实现自我能力的完善。也希望通过威胁框架这一视角来解读“震网”这场看起来依然高度复杂的“昨天的战争”。安天于 2019 年 9 月正式发布报告《震网事件的九年再复盘与思考》，此次复盘我们希望聚焦一个具体的问题：**高级恶意代码对检测引擎和威胁情报的挑战。**由于传统的威胁情报存在诸多短板，安天自 2016 年起开始研发下一代威胁检测引擎，深化了安天传统引擎格式识别、深度解析等特点，继承对海量恶意代码精准的分类到变种的识别能力。同时，以没有可信的格式和对象为前提，形成对检测对象的全格式识别，对更多重点格式形成深度解析能力。不只为调用环节输出判定结果，同时也可以将检测对象的向量拆解结果结构化输出，形成支撑产品场景和态势感知场景研判分析、关联与追溯的数据资源。探索检测引擎与威胁情报更好的结合，建立起更为可靠的基础标识能力与响应机制，更有效的支撑 TTP，乃至人员组织相关的情报，建立起更完善的知识工程运营体系，这对我们来说，将是一个需要长期努力的方向。

●走向高级恶意代码体系分析（2013~至今）

自 2013 年起，安天 CERT 逐渐从单一的模块化样本分析走向系统化的攻击装备整体分析，始终警惕地监测、分析、跟踪着各种针对中国的 APT 攻击活动。结合安天 TID 威胁情报平台和追影威胁分析系统等产品展开大量分析工作，谨慎地披露了**“海莲花”(APT-TOCS)、“白象”（White Elephant）、“方程式”（Equation）**等攻击组织的活动或攻击装备分析，同时也对更多的攻击组织和行动形成了持续监测分析成果。

2013 年 7 月，安天开始陆续捕获来自南亚某国的网络攻击样本，并持续对其进行跟踪分析，经过追踪溯源和关联分析，**我们将这一系列网络攻击组织和行动称为——“象群”，**发布多篇分析报告对这一系列针对我国教育、军事、科研的定向攻击事件进行披露。持续的攻击反映出**我国一直对利益竞合国家和地区对我方科技成果的获取和抄袭模仿关注度较低，对于更为纵深的整体供应链安全关注度也十分不足。我国关键基础设施体系面临着严峻**

（下转第三版）

每周安全事件

类 型	内 容
中文标题	带有恶意 slk 文件的电子邮件针对 Microsoft 365 用户
英文标题	200M+ Users At Risk: New Malicious .slk Files Are Bypassing Microsoft 365 Security
作者及单位	Avanan’s Security
内容概述	本周，Avanan 的安全分析人员发现，在针对 Microsoft 365 用户的攻击中，.slk 文件的使用量显著增加。在这种攻击中，黑客发送一个带有 .slk 附件的电子邮件，其中包含一个恶意宏 (MSI exec 脚本) 来下载和安装远程访问木马。这是一种非常复杂的攻击，具有多种专门设计用来绕过 Microsoft 365 的混淆方法。
链接地址	https://www.informationsecuritybuzz.com/news/200m-users-at-risk-new-malicious-slk-files-are-bypassing-microsoft-365-security/

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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft Windows OLE 安全漏洞（CVE-2020-1281）	高	当 Microsoft Windows OLE 无法正确验证用户输入时，会触发远程代码执行漏洞。攻击者可以利用此漏洞以执行恶意代码。要利用此漏洞，攻击者必须诱使用户在网页或电子邮件中打开经特殊设计的文件或程序。
	Microsoft Windows 和 Windows Server 安全漏洞（CVE-2020-1299）	高	Windows 系统如果处理了 .LNK 文件，则会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。
	Microsoft Office 安全漏洞（CVE-2020-1321）	高	当 Microsoft Office 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的上下文中执行操作。例如，文件可以代表登录用户使用与当前用户相同的权限执行操作。
较为活跃样本家族	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan/Win32.Blamon	中	此威胁是一种可以窃密类木马家族。该家族木马运行后会窃取用户账户信息，记录键盘击键等，造成用户敏感信息泄露。
	Trojan/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan/Win32.Autoit	中	此威胁是一种由 Autoit 脚本编写的木马类家族。该家族木马具有多种功能，可以窃取用户信息、接受远程控制、下载并安装其它恶意代码等。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan/Android.Fakeapp	中	此威胁是一种伪装类木马家族。该家族样本通常伪装为主要应用程序（Fackbook 等），诱导用户输入账号密码，通过 firebase 联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗。
	Trojan[SMS]/Android.FakeInst	低	此威胁是一种伪装类木马家族。该家族样本通常伪装为主流应用程序（Opera、Skype 等），运行后向相关付费号码发送短信，造成用户资费消耗。

（上接第一版）

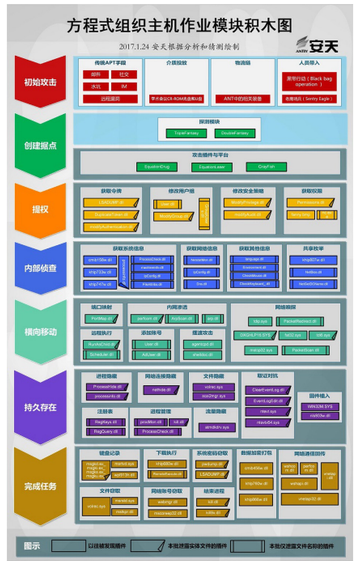
的挑战，网络空间安全视角需要转化为“维护国家主权、安全、发展利益”，更加注重“科技安全”。

2015 年 5 月 27 日，安天发现一例针对中方政府机构的准 APT 攻击事件，鉴于这个攻击与 Cobalt Strike 平台的关系，安天将此攻击事件命名为 APT-TOCS（海莲花）。2018 年安天陆续捕获到多例针对中国用户的恶意宏文档攻击样本，并于 2019 年 3 月发布报告《海莲花组织发布针对中国 APT 攻击的最新样本的分析》。这一系列事件提醒我们，网络攻击技术具有极低的复制成本的特点。随着商业渗透攻击测试平台以及网络军备商业扩散的出现，**“通过分析曝光的方式迫使 APT 攻击组织行为收敛”的效果已经大打折扣，应该放弃简单的敲山震虎，就可以让敌人退避三舍的幻想，全面建设必要的网络安全防御能力，形成动态综合的网络安全防御体系。**

▲安天对 APT-TOCS 攻击的可视化复现（2015）

2015 年 12 月，乌克兰电力部门遭受到恶意代码攻击。安天、四方继保与复旦大学于 2016 年 1 月成立联合分析小组，正式启动对此次事件的分析，2016 年 2 月正式发布《乌克兰电力系统遭受攻击事件综合分析报告》。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，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、方程式等攻击显著降低，但同样直接有效。该事件提醒我们要**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、防火墙、终端防护产品、安全服务等综合方式提升纵深防御能力。**

从 2013 年起，安天从样本分析中，逐步发现存在一个拥有全平台载荷攻击能力的攻击组织，并逐步关联分析了其多个平台的样本。在这个过程中，安天感到一个大至无形的超级攻击组织的存在，但并未找到其攻击背景。截至 2017 年，安天连续发布了四篇关于方程式组织的分析报告，并基于分析成果，根据有关专家建议，形成了一个方程式组织主机作业的模块积木图。初步按照“原子化”拆分的模块组合的拼装，揭示超高网空威胁行为体的模块化作业模式。**在过去的数年间，针对方程式组织的持续跟踪分析，是安天了解超高级别攻击者（即 A^2PT）的极为难得的经历。深入研究这种具有超级成本支撑和先进理念引领的超级攻击者，对于改善和增强安天探海、智甲、追影等高级威胁检测和防御产品的防御能力也非常关键。我们警惕，但并不恐惧。对于一场防御战而言，除了扎实的架构、防御和分析工作之外，必胜的信念是最大的前提。无形者未必无影，安天追影，画影图形。**



▲方程式组织主机作业模式积木图（2017）

2018 年，安天一年的时间内持续每月更新“美国网络空间攻击与主动防御能力”专题报告，刊登在《网信军民融合》杂志两会专刊中，为期 12 期共计 30000 多字。该专题层次化地揭示美国在网络空间中信息获取、进攻与防御能力，尽可能清晰地展现美国在网络空间安全领域的能力体系，为我国网络空间安全发展提供有益参考和借鉴。

▲美方网空作业技术流程与部分工程和装备作用的映射（2018）

2018 年 9 月，安天根据近期掌控的攻击线索结合历史储备，对高级攻击组织绿斑进行了深度分析，发布了《“绿斑”行动——持续多年的攻击》，在该组织的攻击中，反复使用陈旧漏洞，在侵入主机后，通过加密和动态加载等技术手段，试图达成进入目标并在目标机器内长期潜伏而不被发现的效果。**安天此前反复强调，APT 攻击组织使用相关漏洞的攻击窗口期，如果与可能被攻击目标的未进行对应漏洞修复的攻击窗口期重叠，就不是简单的漏洞修复问题，而是深入的排查和量损、止损问题。**

2019 年 6 月，安天基于多年持续跟踪分析超高能力网空威胁行为体的分析成果，结合影子经纪人所泄露的信息，以态势感知视角，完整复盘方程式组织攻击中东最大 SWIFT 服务商 EastNets 的整个过程。按照威胁框架将整个攻击过程的动作逐一进行精细化拆解，通过回放每个攻击分解步骤，分析每个攻击步骤中防御方在基础结构安全工作、防御纵深设置、事件采集与留存、系统配置策略、安全产品布防等方面的不足。**在 A^2PT 级别的攻击的背景下，需要在“实战化”安全运行环境中检验和持续提升防御能力。以资产安全运维平台明晰资产底数，形成网空地形，建立统一安全补丁、统一安全策略分发调整，实现有效的资产安全加固。通过端点侧、网络侧、分析侧的有效数据采集、情报生产，建设态势感知平台系统进行数据汇聚和分析，形成有效安全策略，指控响应行动。安天正在研发的战术型态势感知平台，在安天全线产品体系支撑下通过全面监测和发现、自动化甄别与研判威胁，辅助资产安全运**

（下转第四版）