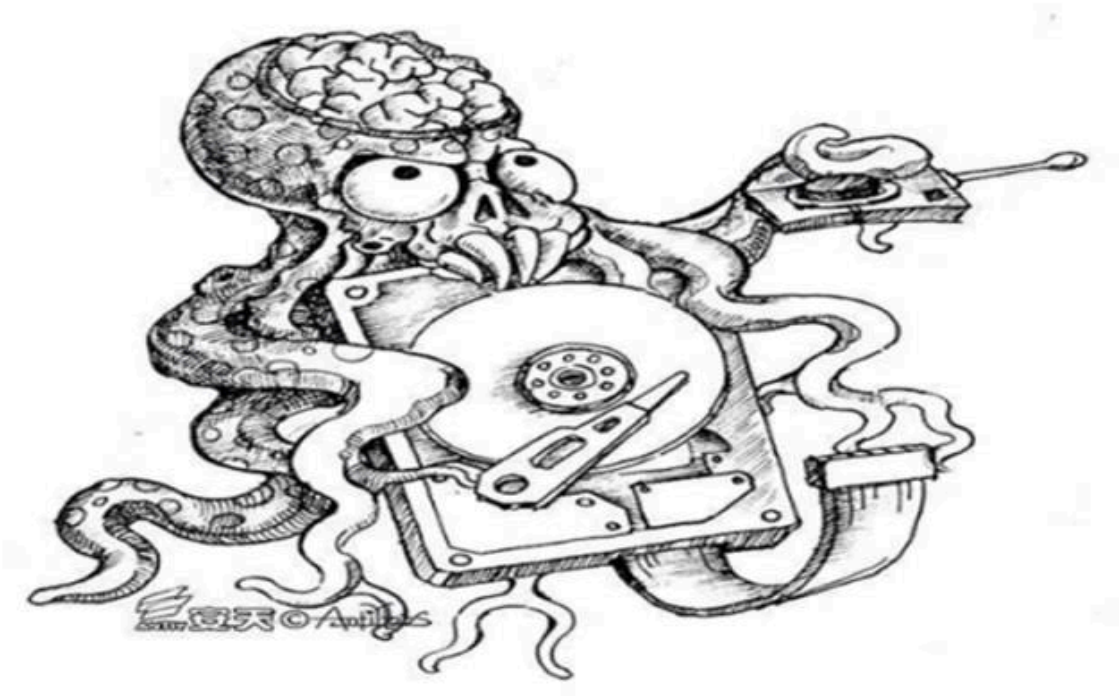
安天发布“方程式组织”攻击中东SWIFT服务商事件复盘分析报告



1

事件背景

网空威胁行为体是网络空间攻击活动的来源，它们有不同的目的和动机，其能力也存在明显的层级差异。根据作业动机、攻击能力、掌控资源等角度，安天将网空威胁行为体划分为七个层级，分别是业余黑客、黑产组织、网络犯罪团伙或黑客组织、网络恐怖组织、一般能力国家/地区行为体、高级能力国家/地区行为体、超高能力国家/地区行为体（参见附件一）。其中，超高能力国家/地区行为体，或称为超高能力网空威胁行为体，拥有严密的规模建制，庞大的支撑工程体系，掌控体系化的攻击装备和攻击资源，可以进行最为隐蔽和致命的网络攻击。安天曾将这种网络攻击称之为A2PT（即高级的高级可持续性威胁）。

“方程式组织”（Equation Group）正是这样一种典型的超高能力网空威胁行为体。2015年2月，由卡巴斯基实验室首次公开披露。卡巴斯基称其已活跃近20年，可能是当前最复杂的APT攻击组织之一[1]。安天多年来持续追踪“方程式组织”的威胁行为，从2015年3月至今，先后发布了四篇分析报告：《修改硬盘固件的木马——探索方程式组织的攻击组件》[2]，分析了其部分木马模块组件和基于硬盘固件持久化的机理；《方程式部分组件中的加密技巧分析》[3]，揭示了其资源的加密方法；《从“方程式”到“方程组”——EQUATION攻击组织高级恶意代码的全平台能力解析》[4]，揭示了其木马载荷的全操作系统平台覆盖能力，并独家曝光了其针对Solaris和Linux的样本；《方程式组织Equation DRUG平台解析》[5]，则形成了对其原子化作业木马的积木拼图。在这些工作中，我们最大的遗憾，莫过于这些分析依然停留在恶意代码分析的视角，我们只能对在已达成攻击目标的现场的有限提取结果，结合基于

威胁情报扩线关联到的样本，来展开分析工作。从业内已发表的分析成果来看，无论对于方程式组织的活动，还是对于同样来自超高能力网空威胁行为体的“震网”[6]、“火焰”[7]、“毒曲”[8]等攻击活动，都基本建立在，对所使用漏洞的原理分析、对样本的逆向分析，以及对样本作用机理的复盘之上。尽管这些工作同样是复杂和艰难的，但并不能掩盖防御者对超高能力网空威胁行为体在战术和过程认知上的不足。这是因为，以“方程式组织”为代表的超高能力网空威胁行为体有一套完整、严密的作业框架与方法体系；拥有大规模支撑工程体系、制式化装备组合，进行严密的组织作业，高度追求作业过程的隐蔽性、反溯源性，使其攻击看似“弹道无痕”，其突破、存在、影响、持续直至安全撤出网络环境或系统的轨迹很难被察觉，导致防护者对其网空行动中实际的攻击技术、战术和过程（TTP）以及相应轨迹知之甚少，包括对于其从研究分析、信息采集、环境塑造、前期侦察，到入口突破、横向移动、持久化、隐蔽对抗、信息获取、长期控制等活动，无法在整个威胁框架视角进行全面的信息掌握和解读。

随着斯诺登的曝光，对于超高能力网空威胁行为体的相关工程体系、装备体系，有了更多可以分析的文献资料。而2017年，影子经纪人的爆料，则让一批攻击装备浮出水面。一方面，这些漏洞利用工具和恶意代码载荷的外泄，被其他低层级的网空威胁行为体快速而广泛的利用，包括酿成了魔窟（WannaCry）蠕虫大爆发等信息灾难；另一方面，这些信息也成为了安全研究者从完整的威胁框架角度去分析超高能力网空威胁行为体的攻击活动全貌的极为宝贵的研究资源。

其中在2017年4月14日，“影子经纪人”曝光的数据中包含一个名为SWIFT的文件夹，完整曝光了“方程式组织”针对SWIFT金融服务提供商及合作伙伴的两起网络攻击行动的详实信息：“JEEPFLEA_MARKET”和“JEEPFLEA_POWDER”。其中，2012年7月至2013年9月期间发起的“JEEPFLEA_MARKET”攻击行动，针对中东地区最大的SWIFT服务提供商EastNets，成功窃取了其在比利时、约旦、埃及和阿联酋的上千个雇员账户、主机信息、登录凭证及管理员账号；“JEEPFLEA_POWDER”攻击行动，主要针对EastNets在拉美和加勒比地区的合作伙伴BCG（Business Computer Group），但此次行动并未成功。

安天CERT将多年对方程式组织的分析进展与这一文件夹中所曝光的各种信息线索进行了组合复盘，还原了“方程式组织”对EastNets网络的攻击过程。通过复盘我们可以看到，这是一起由超高能力网空威胁行为体发起，以金融基础设施为目标；从全球多个区域的预设跳板机进行攻击；以0Day漏洞直接突破两层网络安全设备并植入持久化后门；通过获取内部网络拓扑、登录凭证来确定下一步攻击目标；以“永恒”系列0Day漏洞突破内网Mgmt（管理服务器）、SAA业务服务器和应用服务器，以多个内核级（Rootkit）植入装备向服务器系统植入后门；通过具有复杂的指令体系和控制功能平台对其进行远程控制，在SAA业务服务器上执行SQL脚本来窃取多个目标数据库服务器的关键数据信息的高级持续性威胁攻击事件。

安天分析小组力求以态势感知的工作思路形成过程复盘，对超高能力网空威胁行为体的攻击活动进行初步的抽丝剥茧，对接威胁框架视角的解读，为重要信息系统和关键信息基础设施的规划、建设和运维者，提供关于如何建立有效的防御体系的参考依据。

2

目标资产被攻击情况

SWIFT介绍

SWIFT，全称Society for Worldwide Interbank Financial Telecommunications，中文名为“环球同业银行金融电信协会”，1973年5月，由来自美洲和欧洲的15个国家的239家银行正式组建，总部设在比利时首都布鲁塞尔。该组织运营着世界级的金融报文网络，各国银行和其他金融机构通过其提供的安全、标准化和可信的通道与同行交换报文，从而完成金融交易。除此之外，SWIFT还向金融机构销售软件和服务。截至2015年，SWIFT的服务已经覆盖全球200多个国家和地区的11000多家银行和证券机构、市场基础设施和公司客户，每日处理的报文次数达到1500万。

被攻击的SWIFT服务提供商介绍

经过认证的SWIFT服务提供商（SWIFT Service Bureau）为客户提供了一种高效访问完整SWIFT服务的方法，相当于客户的云提供商，目前全球共有74家。此次攻击行动的目标EastNets是中东地区最大的SWIFT服务提供商。

图2-1 EastNets机构简介

总部设在迪拜的EastNets是全球领先的金融服务领域合规和支付解决方案提供商，提供多种涉及SWIFT交易的服务，包括合规性、了解客户以及反洗钱等。在过去的35年中，EastNets利用特有的专业知识，为客户打击金融犯罪，制定和实施标准化及个性化解决方案，并提供风险管理、监控，分析及最先进的咨询服务和客户支持。EastNets还专注于端到端支付解决方案，使金融机构能够将传统的支付挑战转化为机遇，并使其更有效，更具成本效益地运营。包括一些大型国际金融机构在内的750多家客户依赖EastNets解决方案和专业服务，270多家企业和金融机构依靠EastNets提供外包SWIFT连接和合规软件解决方案。EastNets在全球主要城市设有地区办事处，并由广泛的全球战略合作伙伴网络提供支持[9]。

根据Treasury And Risk的统计[10]，加盟到SWIFT中的成员，70%会选择SWIFT服务提供商，来避免自建SWIFT产生的过高投入以及后续操作维护阶段的费用。SWIFT服务提供商就像是客户的“云”一样，在客户间发生SWIFT交易以及信息交换时，由其通过Oracle数据库以及SWIFT软件来管理。正是因为可以访问所有这些银行交易，很多SWIFT服务提供商也可以提供合规性、了解客户以及反洗钱服务。

被攻击资产简况

分析此次“方程式组织”攻击行动可以发现，EastNets网络环境按照不同功能特性从VPN接入、区域边界再到管理服务器、应用服务器、数据库服务器等进行了一定的层次和分区设计，各个逻辑分区之间也做了基于端口、IP的访问控制策略，部署了企业级防火墙，并且在服务器上部署了主流品牌的安全防护软件。但是即使这种具有一定的基础防护能力和防御纵深的网络信息系统，在面对超高能力网空威胁行为体的攻击时，依然被攻陷。

在此次攻击中，EastNets网络遭受攻击的资产包括VPN防火墙设备、企业级防火墙设备、管理服务器、应用服务器、SWIFT业务服务器、终端主机信息、登录凭证和安全防护软件与应用软件等资产，图2-2绘制了被攻击主要资产简况的拓扑图。

图2-2 被攻击资产简况拓扑图

被攻击的网络安全设备及网络设备信息

EastNets至少有10台以上的网络安全设备和网络设备被攻击或被探测，主要以Cisco和Juniper两种品牌为主，相关设备名称、软件版本、开放端口等信息，被方程式组织完全获取，并被影子经纪人泄露。详细信息如表2-1所示。

表2-1被攻击的企业级防火墙设备的详细信息

被攻击的管理服务器信息

被攻击的管理服务器一共有2台，内网IP分别为192.168.206.110（192.168.208.10 / 10.255.10.10）和192.168.206.111（192.168.208.11 / 10.255.10.11）。相关服务器主机名称、MAC地址、开放端口、安全防护软件和版本以及管理员用户名和口令信息等，被方程式组织完全获取，并被影子经纪人泄露。两台服务器均为Windows Server 2008系统，均开放了445和3389端口，其中一台安装了赛门铁克端点防护软件，另一台未安装防护软件。详细信息如表2-2所示。

表2-2 被攻击的管理服务器的详细信息

被攻击的应用服务器信息

被攻击的应用服务器共4台，其中包括邮件服务器、FTP服务器等。相关服务器主机名称、MAC地址、开放端口、安全防护软件和版本以及管理员用户名和口令信息等，被方程式组织完全获取，并被影子经纪人泄露。其中两台FTP服务器为Windows Server 2008系统，均开放21端口，其中一台还开放了22、135、446端口，两台服务器均安装了赛门铁克端点防护软件。另外两台邮件服务器均为Windows Server 2003系统，邮件系统使用Exchange Server搭建，均使用卡巴斯基端点防护软件进行防护。两台服务器均开放了DNS服务端口，其中一台提供SMTP和POP3服务，另一台通过OWA（Outlook Web Access）提供基于HTTPS协议的Webmail服务。

详情如表2-3所示。

表2-3 被攻击的应用服务器的详细信息

被攻击的SWIFT业务服务器信息

遭遇攻击的SAA（SWIFT Alliance Access）服务器有10台，其中有6台分属5家中东地区银行，有3台为多家银行共享的SAA服务器，有一台为共享SAA的备份服务器。这些服务器操作系统均为Windows Server 2008，安装了赛门铁克的端点防护软件，这些服务器配置了相同的管理员口令。10台服务器中有9台为“方程式组织”确定攻陷，其中7台有相关攻击日志记录。这十台服务器的主机名称、MAC地址、开放端口、安全防护软件和版本以及主机管理员用户名和口令信息，其中3台SAA服务器上运行的Oracle数据库的管理用户名和口令信息，被影子经纪人泄露。详情如表2-4所示。

表2-4被攻击的SAA服务器的详细信息

被窃取的信息资产信息

被窃取的信息资产主要有网络设备和网络安全设备的登录凭证、SAA业务服务器中的多家银行机构业务数据（如账号名、账号状态、密码）等。根据分析网络设备和网络安全设备的配置文件信息，有不少于300个登录凭证被窃取。表2-5展示了经过屏蔽处理后的部分被窃取信息。从这些信息可以判断，方程式组织的攻击目的是获取部分其感兴趣的账号、密码，并进一步获取其资金情况和交易信息、资金流动轨迹等。

表2-5 被窃取的部分信息资产信息

3

事件中所使用的攻击装备情况

“方程式组织”攻击EastNets行动所使用的攻击装备可覆盖EastNets信息化场景中的多种设备和端点系统，包括网络边界的VPN防火墙设备、企业级防火墙设备、管理服务器以及支撑SWIFT业务的SAA服务器等。这些攻击装备大致可分为三类：漏洞利用工具和攻击平台、持久化工具、控制/后门类恶意代码，全套攻击装备拥有覆盖全平台全系统的攻击能力[4]。

漏洞利用工具和攻击平台

相关漏洞攻击装备主要针对网络设备、防火墙等网络安全设备和各类端点系统，其主要作用为突破边界，横向移动，获取目标系统的权限，为后续植入持久化、控制载荷开辟通道。其中典型的漏洞攻击装备EPICBANANA、EXTRABACON和1个未知装备是针对防火墙的，本次攻击中，方程式组织使用了先进的FuzzBunch漏洞利用平台[11]，针对Windows系统进行作业（其中包含至少17个漏洞利用插件，本次行动可能使用了其中的5个），详情见下表：

表3-1 攻击EastNets所使用的漏洞利用工具列表

在本次攻击事件发生时，上述使用的漏洞皆为未公开漏洞。本次攻击中使用漏洞的总数超过了“震网”攻击事件（震网攻击中使用了5个Windows 0day和一个西门子0day漏洞），体现出了超高能力网空威胁行为体充足的攻击资源储备。其中的“永恒”系列漏洞利用工具均被装载于FuzzBunch攻击平台。FuzzBunch是一个类似MetaSploit强大的涵盖大量漏洞攻击和载荷植入的攻击平台，采用行命令方式进行操作，其主要包含扫描探测工具集（Touch）、漏洞利用（Exploit）工具集、植入和配置更新工具、载荷（Payload）模块。扫描探测模块用于获取主机系统和相关服务指纹信息、可攻击的开放端口，以及确定目标是否存在指定漏洞；漏洞利用工具中至少包括17个漏洞的利用模块，其中两个被称为特别（Specials）漏洞，即永恒之蓝和永恒冠军两个重量级漏洞——这种标识可能是为保证在使用相关漏洞中是高度慎重的。植入工具中有两个模块，分别用于向被攻击主机输送攻击载荷并加载，以及投递和更新相关配置文件。功能载荷插件集主要用于漏洞模块攻击成功后向目标安装后门、加载DLL、枚举进程、增删改查注册表项、RPC服务等，其建立起了在主机侧的远控操作机制，这些操作符合安天在此前报告中，对其木马“设计框架化”、“组件积木化”、“操作原子化”的判断。FuzzBunch平台的模块结构如图 3-1所示。

图3-1 FuzzBunch漏洞攻击平台的结构拆解

本次事件中所使用的漏洞攻击装备，安天曾在分析报告《安天关于系统化应对NSA网络军火装备的操作手册》[11]中对这些漏洞攻击装备进行过梳理和分析，绘制了漏洞利用关系图，如图3-2。

图3-2 泄露的NSA网络军火装备的漏洞利用关系图

持久化/植入攻击装备

超级网空威胁行为体高度重视在目标场景中形成持久化的能力，研发了大量实现持久化能力的装备。持久化攻击装备通常在突破目标后使用，主要针对BIOS/UEFI、固件、引导扇区、外设等环节，难以发现和处置的深层次加载点，或形成可反复植入的作业机会窗口。在高级持续性威胁（APT）活动中，确保持续性能力。通过持久化提供的加载机会，攻击者可以保持与目标系统建立初始连接和初步控制权，并进一步输送复杂攻击载荷，从而实现对目标的完全控制和管理。此次攻击中使用了如下持久化装备：

表3-2攻击EastNets所使用的持久化/植入攻击装备

其中，FEEDTROUGH[12]是针对Juniper、NetScreen等防火墙进行固件层持久化的攻击装备，可以在防火墙启动时向系统植入载荷，这一技术与该攻击组织对硬盘固件的持久化思路如出一辙[2]，是更底层的难以检测和发现的持久化技术。

图3-3 ANT-FEEDTROUGH攻击装备

根据斯诺登曝光的相关信息分析，NSA的下属部门ANT（全称为“先进网络技术”或“入侵网络技术”部门）拥有FEEDTHROUGH的持久化装备，ANT具有整套持久化装备，立足于全面覆盖各种端点系统、外设和接口、无线网络和GSM蜂窝网络、主流网络设备和网络安全设备等，达成在各种信息场景中实现运载、植入和持久化。安天在早期曾对ANT的攻击装备进行过梳理，并形成了ANT的装备体系图，如图3-4。

图3-4 ANT装备体系

控制/后门类恶意代码

此类攻击装备是攻击行动中最终植入到目标系统的载荷，用于持久化或非持久化对目标系统的控制。本次行动攻击者所使用的攻击装备如表3-3所示，其中前7项针对网络安全设备及网络设备，最后1项针对Windows主机系统。与持久化工具所追求的建立隐蔽的永久性入口不同，方程式组织在的控制/后门类恶意代码，更强调内存原子化模块加载作业，文件不落地，最大程度上减小被发现与提取的可能性。与持久化工具的组合，呈现出“藏于九地之下（固件等深层次未知），动于九天之上（内存）”的特点。

表3-3攻击EastNets所使用的控制/后门攻击装备

DanderSpritz是其中最典型的控制平台，拥有严密作业过程和丰富规避手段的模块化攻击平台，安天曾在《方程式组织EQUATION DRUG平台解析》[5]一文中对其进行了全面分析。DanderSpritz拥有界面化的远程控制平台，具有复杂的指令体系和控制功能，与传统RAT程序有着明显的区别，一旦植入目标系统后会采集系统各类安全配置信息并提示攻击者哪些配置或信息可能会导致自身被发现或检测。其payload有多种连接模式，其中“Trigger”模式是一种激活连接模式，既不监听端口也不向外发出连接，而是通过监听流量等待攻击者的激活数据包，这使得控制端的部署变得灵活而难以被封禁。

图3-5 DanderSpritz远程控制装备界面

DanderSpritz具有模块化的架构设计，拥有非常丰富的标准化攻击工具和插件，是“方程式组织”网络武器代表。安天在此前分析报告中对“方程式组织”其他的木马模块插件进行梳理，整理了这些功能插件在攻击过程中可能形成的组合，并绘制了“方程式组织”主机作业模块积木图。该图初步展示了一个将主机情报作业按照“原子化”拆分的模块组合的拼装，如图3-6所示：

图3-6 “方程式组织”主机作业模块积木图

在“方程式组织”主机作业模块积木图中可以看到，“方程式组织”通过模块化的方式涵盖了各个攻击阶段使用的武器。而每一个武器又有更细粒度的功能指令，比如创建据点阶段的“DoubleFantasy”武器就有分工明确的分支指令（如下图），不同指令之间相互配合可以完成一系列的操作行为。

图3-7 DoubleFantasy指令分支

4

攻击过程复盘

2012年7月至2013年9月，“方程式组织”使用来自多个不同国家和地区的跳板IP，对EastNets发起了6次网络攻击。攻击者通过先后6条不同的入侵路径相互配合，针对不同的系统和设备使用了包括“永恒”系列在内的多套攻击装备，最终攻陷了位于EastNets网络中的4台VPN防火墙设备、2台企业级防火墙、2台管理服务器，以及9台运行多国金融机构业务系统的SAA服务器和FTP服务器以及对位于DMZ区域的邮件服务器。

图4-1 “方程式组织”对EastNets网络的总体攻击过程复盘

总体攻击过程

从总体攻击上看，攻击者通过来自全球多个区域的跳板机器，使用多个0Day漏洞突破多台Juniper SSG和CISCO防火墙，然后植入持久化后门，使用“永恒”系列的0Day漏洞控制后续的内网应用服务器、Mgmt Devices(管理服务器)和SAA服务器。除了突破防火墙，攻击者还突破了处于外网的邮件服务器，对外网的邮件服务器和同网段内的终端进行了扫描和信息搜集（如安全防护软件和应用软件安装情况）。在部分攻击过程中，虽然还存在一些诸如未能向终端植入持久化模块的失败操作，但通过多次入侵路径的先后配合，“方程式组织”最终还是完成了对EastNets网络全球多个区域的银行机构数据的窃取。

攻击跳板：

本次攻击所使用的互联网攻击跳板，均为被植入PITCHIMPAIR后门的商用Unix、FreeBSD或linux服务器主机，多数来自全球高校和科研机构。这些节点运行更多依靠系统自身的健壮性，和高校、科研机构人员的自我运维，而不像Windows环境一样，处于始终的高频对抗之中，反而推动了商用安全产品的保护能力的不断完善。对于超高能力网空威胁行为体来说，这种在商用安全能力感知之外的节点，反而成为一种理想的建立持久化跳板的目标。同时，由于这些服务器自身位于高校和科研机构，因此其并不简单的具备跳板价值，其本身也在不同时点会与直接情报获取活动产生直接关联，在不同形式和任务角色中，这些节点会被以不同的方式利用。2016年11月影子经纪人曾公开一份遭受入侵的服务器清单，清单的日期显示2000~2010年间，以亚太地区为主的49个国家的相关教育、科研、运营商等服务器节点遭遇攻击，受影响的国家包括中国、日本、韩国、西班牙、德国、印度等。如图4-2。在相关爆料中，亦提及相关服务器可能是Linux、FreeBSD和Solaris。这与方程式组织攻击EastNets所使用的跳板情况信息，形成了非常好的相互印证。

表4-1 “方程式组织”攻击EastNets网络使用的跳板机器

图4-2 “方程式组织”在2000~2010年间对全球互联网节点的入侵可视化复现

总体攻击过程如下：

步骤1：选择来自日本、德国、哈萨克斯坦和中国台湾的6台被入侵服务器作为跳板，利用Juniper ScreenOS软件的身份认证漏洞（CVE-2015-7755）攻击EastNets网络的4个Juniper VPN防火墙，攻击成功后向目标系统植入FEEDTROUGH持久化攻击装备到防火墙中，最后通过FEEDTROUGH向防火墙中植入ZESTYLEAK和BARGLEE两款后门攻击装备，实现对防火墙的完全控制。在其6次攻击中有2次是直接使用“永恒”系列漏洞攻击装备，向位于DMZ区域的邮件服务器进行攻击，并向内网进行扫描。

步骤2：利用EPICBANANA或EXTRABACON漏洞攻击装备攻击2台Cisco企业级防火墙，攻击成功后向目标系统植入JETPLOW或SCREAMINGPLOW，最后通过JETPLOW或SCREAMINGPLOW向防火墙系统植入BANANAGLEE，实现对防火墙的完全控制。

步骤3：利用“永恒”系列的0Day漏洞攻击两台管理服务器，攻击成功后向服务器系统植入DoublePulsar或Darkpulsar，最后再通过DoublePulsar或Darkpulsar向服务器系统植入DanderSpritz平台生成的后门载荷（DLL），对其进行远程控制。

步骤4：以2台管理服务器为跳板，利用“永恒”系列漏洞攻击装备获取后端的9台SAA业务服务器的控制权，使用的“永恒”系列漏洞包括ETERNALROMANCE（永恒浪漫）、 ENTERNALCHAMPION（永恒冠军）、ETERNALSYNERGY（永恒协作）、ETERNALBLUE（永恒之蓝）。最后在SAA服务器上执行SQL脚本initial_oracle_exploit.sql和swift_msg_queries_all.sql，对本地Oracle数据库中存储的多家银行机构业务数据（账号名、账号状态、密码等）进行转储。还通过管理服务器对其它区域中的FTP服务器进行攻击。

可视化复现

根据上述总结分析，安天态势感知平台可视化组件对攻击行动的复现演示如图4-3所示。

图4-3 安天态势感知平台可视化组件对攻击行动的复现演示

（详细复现视频请查看：https://www.antiy.cn/video/20190531/lup.mp4）

5

网空威胁框架与本次事件的映射分析

以“方程式组织”为代表的超高能力网空威胁行为体，具有庞大的攻击支撑工程体系、装备体系和规模化作业团队等特点，并在这些资源的支撑下，成功执行高度复杂的攻击活动。如果对类似攻击组织的分析停留在0day漏洞、恶意代码等单点环节上，既无助于对其整个过程进行全面的分析，也难以有效地指导防御工作。为应对高能力网空威胁行为体的攻击活动，安全人员需要有体系化、框架化的威胁分析模型，对其行为展开更深入、系统的分析，理解威胁，进而实现更有效的防御。当前类似的分析模型包括洛克希德·马丁公司（Lockheed Martin）的Kill Chain（杀伤链）和MITRE公司的ATT&CK等。

Kill Chain由洛克希德·马丁公司于2011年提出，定义了攻击者为达到目标必须要完成的7个阶段，并认为防御者在任意一个阶段打破链条，就可以阻止入侵者的攻击尝试。Kill Chain将网络攻击模型化，有助于指导对网络攻击行动的识别和防御，但整体上粒度较粗，全面性不足，相应的应对措施也缺乏细节支撑。为解决上述问题，MITRE公司在Kill Chain的基础上，提出了ATT&CK模型，即对抗战术、技术和通用知识库，将入侵全生命周期期间可能发生的情况划分为12个阶段，分别为初始访问、执行、权限提升、防御逃避、凭证访问、发现、横向移动、收集、命令与控制、渗出和影响，每个阶段又细分了具体的攻击技术。ATT&CK提供了对每一项技术的细节描述、用于监测的方法及缓解措施，有助于安全人员更好地了解网络面临的风险并开展防御工作。但ATT&CK侧重于具体的攻击技术，在层次性和对入侵行为的分类方面偏弱。

NSA和CSS参考各类现有框架，于2018年3月发布了《NSA/CSS技术网空威胁框架》（NSA/CSS Technical Cyber Threat Framework）（以下简称“威胁框架”）V1版本，该框架是一个基于国家情报总监（DNI）网空威胁框架开发的、与网空行为活动紧密结合的通用技术词典，NSA在整个情报体系内共享这一词典，实现对情报共享、产品研发和作战规划的支撑，促进情报体系各机构间更紧密地合作。

随着网络威胁不断升级，NSA和CSS在“威胁框架”V1的基础上进行调整和延伸，对其中划分不细致、归类不准确的内容进行重新梳理，于2018年11月发布了V2版本。“威胁框架”V2共包含6个阶段（Stage）、21个目标（Objective）、188种行为（Action）和若干个关键词（Key Phrases），提供了标准定义，能够指导讨论攻击者全生命周期内的活动，呈现攻击事件全貌，可视化攻击者所使用的策略及手段，协助安全人员制定针对性的防御措施。

由于“威胁框架”尝试将各种可能的目标和行为涵盖在内，其恰恰将其自身和关联的专属攻击能力也涵盖在内。例如，“方程式组织”覆盖各种型号硬盘固件持久化能力，“量子”（QUANTUM）攻击系统修改通信路径的能力，“湍流”框架下的被动信号收集系统“混乱”（TURMOIL）向中点发送信标、仿冒合法流量的能力等等，都能够在“威胁框架”中得到映射，体现出其体系化、复杂化的网空攻击能力。因此，“威胁框架”对于梳理来自超高能力网空威胁行为体的网空攻击活动来说，就成为了非常有效的方法框架体系。

图5-1 NSA/CSS技术网空威胁框架

安天以“威胁框架”V2为参考，对超高能力网空威胁行为体攻击行动的各阶段行为进行标准化描述和分类，协助分析这些行为体的意图和行为，为相关防御工作的开展提供借鉴。

通过本次事件的复盘分析，可将该事件中涉及的威胁行为映射到“威胁框架”V2中。攻击者基于长期环境准备，在多个国家或地区建立大量跳板机资源，可以随时选择发起攻击，利用ZESTYLEAK、BARGLEE、BANANAGLEE攻击装备打击防火墙，获得防火墙权限，实现对设备的控制并管理服务器。利用“永恒”系列漏洞获取服务器控制权后在其上执行sql脚本，查询与服务器相连的Oracle数据库中的信息，获取凭证以及内部架构信息。利用已获取的凭证对相关Windows的主机和服务器实现远程登陆，横向移动到不同的办公地点主机继续收集相关用户凭证。最后，采用数据加密等规避手段防止受害者发现威胁。这些行动都能够与“威胁框架”的类别与动作建立映射。

图5-2 本次事件映射到威胁框架

这一攻击事件共涉及15个目标中的47种行为，其中包括推测的和确定执行的行为。

经过分析，确定使用的行为如下

■**侦察：**收集凭证、测绘可访问网络、扫描设备；

■**环境预制：**应用数据文件中添加可利用点、建立跳板、预置载荷；

■**投递：**利用受感染主机；

■**利用：**利用固件漏洞、利用本地应用程序漏洞、利用操作系统漏洞、利用远程应用程序漏洞、利用零日漏洞；

■**执行：**通过服务控制器执行、利用解释脚本、利用系统接口、写入磁盘；

■**内部侦察：**枚举账号和权限、枚举文件系统、枚举操作系统和软件、枚举进程、测绘可访问网络、嗅探网络；

■**提权：**利用操作系统漏洞；

■**凭证访问：**定位凭证；

■**横向移动：**远程登录、利用远程服务、写入远程文件共享；

■**渗出：**从本地系统收集、从网络资源收集、压缩数据；

■**命令与控制：**中继通信；

■**规避：**规避数据大小限制、加密数据、操纵受信进程、仿冒合法流量、使用rootkit、将文件存储在非常规的位置、根据环境调整行为。

同时，对于进行这种复杂、严密、动用大量网空攻击装备资源的攻击，必然有系统的前期准备工作，包括规划统筹、确定目标、选择攻击装备（也可能包括为现有攻击装备不覆盖的IT场景临时研发装备）等。

6

事件总结

基于对被攻击资产情况、所使用攻击装备和攻击过程的复盘梳理，这份报告基本呈现出了整体的攻击全貌。从事件发生的2012~2013年的背景来看，被攻击目标的布防情况，总体体现出在那个时代信息资产的布防特点，部署了包括VPN、防火墙、主机杀毒等基础安全环节，对内部资产做了基本的分区，进行了一定的配置加固等等。这些防护手段是建立起网络防御体系的基本工作，对于防范一般性的网络攻击是有效的，但对于防护超高能力网空威胁行为体则是完全不足的。

同时，通过相关泄露的资料，也可以看到系统管理者存在一些非常明显的配置和安全策略失误。例如，同组的多台服务器采用相同的超级用户口令，导致一旦其中一台的口令被提取还原或嗅探，就可以被连锁突破；不同组的服务器口令存在明显的“公共部分+序号”的可猜测规律；防火墙没有对可以访问管理接口的IP地址作出明确的限定策略等。

建立起能够有效防御高级网空威胁行为体的防御体系，并不是简单的查缺补漏，而是一个复杂艰巨的过程：

（1）必须直面开放式场景和信息系统规模增长带来的安全挑战，全面提升网络安全规划能力，落实全生命周期的安全规划建设运维。传统银行系统依靠物理安全隔离保障自身资产的时代早已过去，随着跨行转账、通存通兑，类似SWIFT等服务就必然成为在公网上可以到达的基础设施。必须立足于开放式场景的现实条件、信息系统规模日趋扩大和复杂度日趋增加的前提，信息系统的开放度越高，规模越庞大，就越需要在规划、建设和运维的全生命周期同步提升网络安全整体能力，就越需要系统全面的安全规划。

（2）重要信息资产和规模性信息资产，需要以“敌已在内，敌将在内”作为客观敌情设定。鉴于当前信息系统的规模、供应链的复杂程度以及各类信息交换的必然性，将威胁阻挡在边界（安全网关或网闸）之外已经是一种高度不现实的想象。对于掌握大量突破隔离网络装备、可以渗透配送物流环节、可以进行上游供应链预置作业的超级网空威胁行为体来说，其既可能从网络边界逐层突破，也可能借助其他作业手段直接建立内部桥头堡。因此，对于关键基础设施和重要信息系统，必须将“敌已在内”和“敌将在内”作为最基础的敌情设定。安天在2017年提出了“有效的敌情想定是做好网络安全防御工作的前提”的观点，这是源于军事演习的防御思考，但在过去两年的理念的不断推动实践中，我们日趋感到网络空间所面临的风险，比演习想定更为严峻。敌将在内，可以作为一种想定，指导“防患于未然”的规划。而敌已在内，则已经构成了“现实战情”，需要具备将威胁行为体“找出来，赶出去”的威胁猎杀能力。

（3）参考的“威胁框架”，更新对威胁行为体和攻击活动的系统性认知，以深化和完善敌情设定，进而改善防御。网络防御者必须直面高级网空威胁行为体，掌握着大量高级装备和攻击资源，其行动是复杂过程组合的既定事实，同时复杂的过程并不必然均由“高级”攻击手段和“高级”装备支撑。一方面，一些低级的配置错误和未及时修补的漏洞会成为威胁行为体进入的入口；另一方面，高级网空威胁行为体也会劫持和利用低级网空威胁行为体所掌控的僵尸网络等资源。将安全防护工作视为对各种威胁类型如恶意代码、DDoS、网站篡改和僵尸网络等的一一应对，进行产品堆砌，显然不能组合起有效防御体系。而从威胁框架出发，针对威胁每个阶段、逐个行为推演，无论对评估当前防御体系及相关安全产品能力的有效性和合理性，还是对形成体系化的防御规划与建设目标，都是一种有益的工作。

（4）任何单点环节均可能失陷或失效，包括网络安全环节本身。在复盘过程中可以看到，虽然整个SWIFT系统是使用了两层防火墙来构建防护，但由于攻击者基本上为所有的主流IT设备场景，包括各种主流防火墙，都针对性开发了适配性的攻击装备，所以说任何单点环节均可能失陷或失效，包括网络安全环节本身。防火墙是一种必备的网络安全设备，如为重要边界安全设备配套类似安天探海等全流量监测和记录设备，再通过单向网闸将数据结果摆渡到内部，供态势感知平台进行深度分析，就是一种行之有效的方式。其不仅可以弥补防火墙设备要求效率而带来的检测深度不足，进一步提升边界防御能力，而且也能够将对防火墙的攻击流量记录留存，为后续可能的威胁发现、取证、溯源、猎杀等工作提供必要基础。

（5）全面精准的已知威胁检测防护能力和未知威胁发现能力都非常重要。在敌情设定下，可以看到，高级网空威胁攻击者所使用的攻击装备有极大可能是“未知”的，这种未知是指在局部或全局条件下，攻击装备对于防御方及其维护支撑力量（如网络安全厂商）来说，是一个尚未获取或至少不能辨识的威胁。但如果对已知威胁都不能进行有效防御，那么对于超高能力威胁行为体的防御就更加难以实现。我们看到，类似攻击EastNets所使用的漏洞利用工具在被分析报告揭示后，这些工具都成为了“已知威胁”，而被更低级别的攻击者所广泛利用，形成了更大面积的影响和损害。有效的防御这些威胁就是必须的基础能力。对于未知威胁无法杜绝其首次突破防御的可能，因而应该通过合理的防御体系来控制其活动的影响范围，限制其横向移动的能力。由于未知威胁可能导致原有检测能力不能对攻击者实现留痕，所以需要更全面的数据采集能力和基于失效设计的防御纵深。同时在与威胁对抗的过程中，能够对海量已知威胁事件进行精准的检测也是必不可少的能力需要。

（6）建立“体系化的防御”才能应对“体系化的攻击”。在高级网空威胁行为体开展体系化攻击的情况下，仅仅进行单点或简单的多点防护，并不足以形成有效的防御体系。必须将单点对抗转化为体系对抗，将产品机械堆砌转化为能力有机融合。安天在国际网络安全研究机构SANS所提出的“滑动标尺”模型[16]的基础上，与国内多家能力型厂商共同约定为基础模型后进行了延伸拓展，提出了叠加演进的网络空间安全能力模型，将网空安全能力分为五大方面，其中基础结构安全、纵深防御、态势感知与积极防御、威胁情报四大方面的能力都是完善的网络安全防御体系所必需的。将防护目标所处的物理环境、通信网络、计算环境、应用和数据等技术层次与叠加演进的模型有效关联融合，能够迅速的找到所需的安全举措。在可管理性有保障的基础上、结合合理的防御纵深，态势感知与积极防御才能够发挥相应的作用，协同指挥部署的安全产品。威胁情报的价值才得以最大化。对抗高级网空威胁行为体，必须在态势感知与积极防御以及威胁情报方面进行系统的建设与投入，但同时这种投入的有效性又依赖于基础结构安全和纵深防御的支撑。需要看到态势感知与积极防御和威胁情报都是需要高成本投入的，这符合安全对抗既是体系对抗也是成本对抗的特点。

（7）态势感知必须面对战术响应，才能够应对高速多变的网空威胁。不能停留在对“宏观态势”的“把握掌控”和策略调整，基于PDCA循环的信息安全生命周期也无法抵御快速发生的攻击行动。此次行动的攻击装备和相关技术动作都具备极高的隐蔽性，其既不会触发防火墙、入侵检测和主机杀毒软件的相关告警，也不会带来明显的流量异常和突变，其相关的横向移动、控制与窃取操作混杂在系统正常流量当中。及时发现这种微观细节的差异，并快速针对该事件进行检测、理解、决策制定和行动执行，从而实现抵御攻击、进行恢复乃至实施反制是积极防御的目标（参见安天与业内专家共同翻译的《网络空间安全防御与态势感知》[17]一书及译者序内容。）。这种态势感知体系，不是简单宏观层面的监测+大屏，而是复杂的战术型态势感知平台体系，是安天人正在全面发力的重要战略方向。

（8）保障重要信息资产和规模性信息资产安全，必须建立起实战化运行机制。“体系化的防御”不仅仅是体系化的安全产品部署，“态势感知”也不仅仅是机器的态势感知。要发挥体系的作用，需要建立完备的安全运行流程，落实安全运行相关角色与职责，制定和完善配套的安全运行规范流程。尽管在基础结构安全和纵深防御方面部署的安全举措多数都是无需人参与即可生效的，但也需要人进行更新、维护和审计等相关工作，这些工作的及时和持续是保障安全措施有效的基础。要建立起“资产、配置、补丁、漏洞四打通，运维安全一体化”的基础安全运维能力。态势感知与积极防御工作是围绕网空防御人员设计展开的，也就更依赖于实战化的运行机制，才能让“人在闭环之上”发挥出关键能动性价值。未来安全厂商提供的安全产品、系统、平台都必须满足整体实战化运行的要求。

（9）最后，也是最重要的一点，超高能力网空威胁行为体并非是无法应对的。既要对超高能力网空威胁行为体的能力有充分的认识，又要避免将其神化从而导致防御的虚无主义。以同批次攻击事件为例，方程式组织在本报告复盘分析的“JEEPFLEA_MARKET”行动中展示了超级攻击能力，但在被曝光的另一起针对EastNets在拉美和加勒比地区的合作伙伴BCG的攻击行动“JEEPFLEA_POWDER”则未获成功。对高级网空威胁，从防御到猎杀，当然不能基于撞大运式的偶然，不能寄希望于超高能力网空威胁行为体的高抬贵手。我们需要坚定与之斗争的信念，要清晰的认识到与应对敌情所需的防御能力之间的差距，坚定投入的信心和决心，做好长期、持续和扎实的基础工作。

路漫漫其修远兮，吾将上下而求索。

但可以确定的一点是，我们从今天开始努力，就比从明天开始，早一天到达目标。

分析团队补记

这是一份经历了多次修订和完善的报告，在相关复盘分析过程中，我们感受到了一种巨大的压力、焦灼与责任感。面对超高能力网空威胁行为体在2012~2013年已经具备的攻击能力，深知建立起对这样的攻击者的防御能力是非常艰巨的工作，也是必须达成的目标。同时，我们也非常担心超高能力网空威胁行为体无节制的提升攻击能力，将使网络空间武器化成为一种汹涌的逆流。

报告发布日，正是6月1日国际儿童节，《世界儿童和平条约》中有这样童心的呐喊：

我们，全世界的儿童，向世界宣告，未来的世界应该和平。

我们要一个没有战争和武器的星球……

参考链接

[1][Kaspersky：Equation: The Death Star of Malware Galaxy]

http://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/

[2][安天：修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件]

https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[3][安天：方程式（EQUATION）部分组件中的加密技巧分析]

https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[4][安天：从“方程式”到“方程组”EQUATION攻击组织高级恶意代码的全平台能力解析]

https://www.antiy.com/response/EQUATIONS/EQUATIONS.html

[5][安天：方程式组织EQUATION DRUG平台解析——方程式组织系列分析报告之四]

https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html

[6][安天：对Stuxnet蠕虫攻击工业控制系统事件的综合分析报告]

https://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html

[7][安天：Flame蠕虫样本集分析报告]

https://www.antiy.com/response/flame/Analysis_on_the_Flame.html

[8][安天：探索Duqu木马的身世之谜——Duqu和Stuxnet同源性分析]

http://www.antiy.com/cn/security/2012/r120521_001.htm

[9][EastNets]

https://www.eastnets.com/about

[10][How to Pick a SWIFT Service Bureau]

https://www.treasuryandrisk.com/2010/10/01/how-to-pick-a-swift-service-bureau/

[11][安天：安天关于系统化应对NSA网络军火装备的操作手册]

https://www.antiy.com/response/Antiy_Wannacry_NSA.html

[12][Schneier on Security：FEEDTROUGH: NSA Exploit of the Day]

https://www.schneier.com/blog/archives/2014/01/feedtrough_nsa.html

[13][美国网络空间攻击与主动防御能力解析（概述篇）]

https://mp.weixin.qq.com/s?__biz=MzI0NjU2NDMwNQ==&mid=2247485034&idx=1&sn=97ab78fc4ea250fad8f4a96ff6547633&scene=21#wechat_redirect

[14][美国用于漏洞利用的网空攻击装备解析]

https://mp.weixin.qq.com/s?__biz=MzI0NjU2NDMwNQ==&mid=2247486352&idx=1&sn=d48c5e182103d574e6b3127b8d1889f9&scene=21#wechat_redire

[15][美国用于命令与控制的网空攻击装备解析]

https://mp.weixin.qq.com/s?__biz=MzI0NjU2NDMwNQ==&mid=2247486420&idx=1&sn=29ddac3b1dd9873c5d793746f1055ed0&scene=21#wechat_redire

[16]国际网络安全研究机构SANS所提出的“滑动标尺”模型

https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

[17][美]亚历山大·科特、克利夫·王、罗伯特·F.厄巴彻编著 黄晟 安天研究院译. 网络空间安全防御与态势感知[M]北京：机械工业出版社，2019.

附表：安天对网空威胁行为体的能力分级

●响尾蛇APT组织针对巴基斯坦的定向攻击事件分析

●安天发布APT攻击组织“绿斑”分析报告

●安天发布：潜伏的象群——越过世界屋脊的攻击

●安天图解方程式组织积木式主机作业

●安天发布方程式组织Drug攻击平台初步解析

↙点击下方“阅读原文”，报告将持续更新修订
