（上接第三版）

3.4 拼接主机攻击作业积木魔方

2017 年 1 月 25 日，安天中英文双语发布了对方程式组织的第四篇分析报告《方程式组织 EQUATION DRUG 平台解析》，在该报告中，安天基于分析成果，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。这个积木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，揭示超高网空威胁行为体的模块化作业模式。至此，基于安天 4 年的持续跟踪与分析，发现超高能力网空威胁行为体（方程式组织）的完整作业能力。

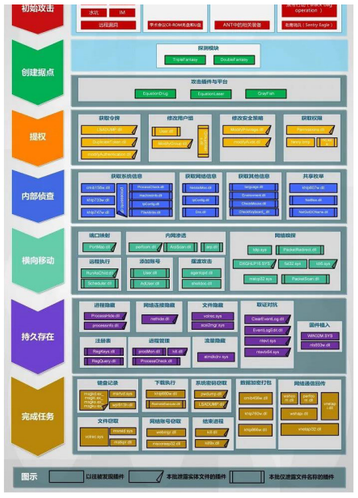

图 方程式组织主机作业模块积木图

4、2018~ 至今 引入威胁框架 构筑态势感知能力

4.1 “方程式组织”攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告

2019 年 1 月，在第六届网络安全冬训营上，安天首次介绍了方程式组织对中东金融服务机构 EastNets 进行攻击的过程。这是安天将针对方程式组织的历史分析成果与 “影子经纪人”泄露资料相结合形成的新的分析成果。2019 年 6 月 1 日，安天正式发布《“方程式组织”攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告》，报告精准还原了受到攻击影响的 IT 资产全景和拓扑关系，完整再现了杀伤链的全过程，详尽梳理了行动中使用的武器和作业流程，并以可视化方式予以复现。在报告中，安天在有关专家建议下，以“TCTF 威胁框架”V2 为参考，首次使用威胁框架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映射，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。2020 年 1 月，在第七届网络安全冬训营上，安天以态势感知和防御体系建设视角，对此事件做了重新梳理和解读。

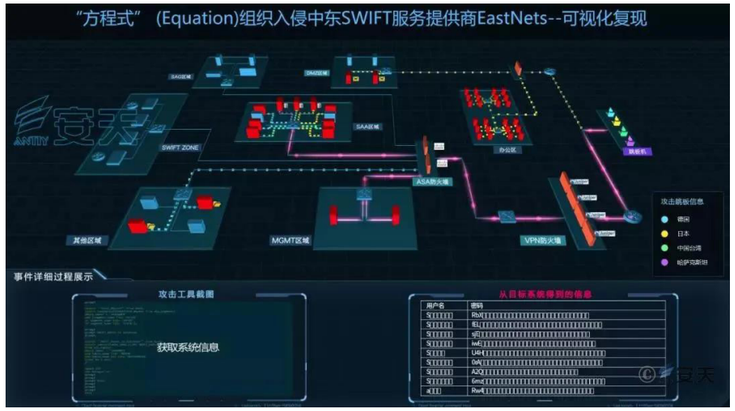

图 安天态势感知平台可视化组件对攻击行动的复现演示
（详细复现视频请查看：https://www.antiy.cn/video/20190531/lup.mp4）

4.2 震网事件的九年再复盘与思考

2019 年 9 月 30 日， 安天发布长篇报告《震网事件的九年再复盘与思考》，在报告中，安天详细比较了震网各版本特点和作用机理、分析了相关高级恶意代码工程框架和震网、毒曲、火焰和后期方程式组织所使用恶意代码间的关联。梳理了震网事件完整时间轴、震网整体结构和运行逻辑、以及震网存在大量样本的原因。反思了当前网络安全中检测引擎与威胁情报面临 APT 的挑战，并思考了如何建立起更可靠的基础标识能力与响应机制、更有效的支撑 TTP、更可靠的组织相关的情报、与业内专家携手，力求客观严谨进行分析验证，对改善防御提出建议。亦先后发布了《委内瑞拉大规模停电事件的初步分析与思考启示》《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》等报告。这些工作对推动用户改善防护，对我们自身提升核心产品能力均起到了积极的作用。同时，回看这些工作，还有很多不完备之处，还需要进一步的改进。

久织长缨在手，终能缚住苍龙。

微信扫描二维码可查看报告原文

安天周观察
安天官方微博　安天官方微信
主办：安天　2020 年 3 月 09 日 (总第 221 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天对“超高能力网空威胁行为体”系列分析回顾

1、背景概述

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。国家 / 地区行为体所发动的网络攻击，通常被称为 APT（高级可持续性威胁）攻击。而其中以美情报机构 NSA 等为代表的超高能力国家 / 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。安天将此类威胁行为体发动的网络攻击（如震网、方程式等）特别命名为 A^2PT（即高级的高级可持续性威胁），在过去近十年（自 2010 年 7 月起）的时间里，对此进行了持续的关注和深入的逆向分析工作。其中部分工作成果已在安天官网或微信公众号公开，或刊载于技术媒体、安天技术文章汇编。为便于研究者深入了解 A^2PT 攻击，本篇文献按照公开时间顺序将安天的分析成果形成如下索引摘要，便于网络安全工作者集中阅读参考。

2、2010~2012 以样本分析视角启动 APT 分析

2.1 跟进震网——APT 分析的起点

2010 年 7 月震网事件曝光，伊朗铀离心设施遭遇长时间网络攻击，导致严重后果，引起全球关注。7 月 15 日，安天启动分析工作，经过两个月的分析。2010 年 9 月 27 日，安天发布《对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告》。报告中对 Stuxnet 蠕虫的攻击过程、传播方式、攻击意图、文件衍生关系进行分析，分析其利用的多个零日漏洞，总结该蠕虫的攻击特点，并给出解决方案，最后做出评价和思考。该报告是国内较早的通过逆向工程系统分析震网的全面报告，成为国内公众了解 Stuxnet 蠕虫攻击真相和细节的重要参考资料，报告内容也被多本书籍文献引用。

2.2 补充分析——解密 USB 摆渡传播的判定逻辑

分析报告发布后，安天获得了多方反馈，其中集中反应的问题是，震网的 USB 摆渡行为无法再现。2010 年 10 月 11 日，安天发布了补充分析报告，指出震网通过 U 盘的传播是由包括时间戳和限制条件等七组配置数据来决定，比如它尝试连接因特网来判断自己是否在内部网络中，然后决定是否通过 U 盘传播。补充报告还分析了震网通过开启 RPC 服务、共享服务和远程

（下转第三版）

每周安全事件

类 型	内 容
中文标题	Molerats 组织针对政府和电信组织投送后门
英文标题	Molerats Delivers Spark Backdoor to Government and Telecommunications Organizations
作者及单位	Robert Falcone, Bryan Lee and Alex Hinchliffe
内容概述	从 2019 年 10 月到 2019 年 12 月初，Unit 42 团队观察到多起网络钓鱼攻击事件，针对政府、电信、保险和零售行业中六个不同国家（沙特阿拉伯、阿联酋、英国、西班牙、美国、吉布提）的八个组织，该活动可能与 Molerats 组织（又名 Galer Hackers Team 和 Gaza Cybergang）有关。所有的攻击中都使用鱼叉式网络钓鱼电子邮件，以传递恶意文档。恶意文档利用社会工程学引诱用户启用恶意宏或者点击恶意链接，以下载恶意载荷，大多数载荷为 Spark 后门。Molerats 使用多种技术逃避检测和分析，例如用密码保护传递文件、设置载荷执行限制、使用商业打包程序 Enigma 混淆有效载荷以及通信数据使用 3DES 或 AES 加密。
链接地址	https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/

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.Joker2.ac[prv,pay,exp] 2020-02-27	高	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息。造成用户隐私泄露和经济损失，建议卸载。
		Tool/Android.SMSForward.w[prv,exp] 2020-02-28	中	该应用程序是一款短信转发工具，通过短信转发至指定号码，警惕转发短信造成用户资费消耗和隐私泄露，建议谨慎使用。
		Trojan/Android.LockScreen.cy[rog,lck] 2020-02-29	中	该应用程序伪装为 QQ 工具箱，运行锁定屏幕，勒索用户添加指定 qq 解锁，影响用户手机的正常应用，建议卸载。
	较为活跃样本	Trojan/Android.BankerSpy.o[prv,spy]	中	该应用程序伪装正常应用，运行隐藏图标，监听短信，隐藏通知栏服务，联网上传用户短信、安装列表、设备固件信息等隐私，并私自发送短信，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.Cerberus.b[prv,rmt]	中	该应用程序伪装其他应用，运行后台监听用户的短信、通知栏信息，窃取短信及固件信息联网上传，并私自发送短信，访问未知页面，造成用户的资费消耗和隐私泄露，建议卸载。
		Trojan/Android.FakeInst.fm[prv,rmt]	中	该应用程序伪装其他应用，安装无图标或隐藏图标，根据指令获取用户短信、联系人、安装软件列表等信息，警惕造成用户隐私泄露，建议卸载。
		RiskWare/Android.Triada.bv[exp]	低	该应用程序包含风险代码，动态加载子包推送广告，可能会下载推送应用，造成用户资费损耗，建议谨慎使用。
		RiskWare/Android.Daikuan.u[rog,fra]	低	该应用程序运行访问第三方网贷网站，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Excel 资源管理错误漏洞（CVE-2020-0759）	高	Microsoft Excel 中存在资源管理错误漏洞，该漏洞源于该软件没有正确处理内存中的对象。攻击者可利用该漏洞在当前用户的上下文中运行任意代码。攻击者可利用漏洞安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan[Dropper]/Win32.Injector	中	此威胁是一种带有捆绑行为的木马类程序。该家族会在被感染的电脑中安装被压缩的恶意软件，并为黑客打开后门。该家族通过用户在成人网站或共享网站上下载的编解码器和 AcitveX 更新来感染电脑。该家族进入系统后隐身运行，并会弹出恶意弹窗。
		Trojan[Downloader]/Win32.Banload	中	此威胁是一种具有下载行为的木马类程序。该家族样本运行后，会在电脑中下载恶意程序并运行。该家族会修改注册表、添加启动项，以达到随系统启动的目的。该家族下载的文件可以盗取用户银行账号和密码。
		Trojan/Win32.Pirminay	中	此威胁是一种木马类程序。该家族入侵电脑后，会修改注册表信息，以便隐藏自己躲避杀毒软件的查杀。该家族的不同变种具有不同的恶意行为，如：自动下载恶意程序、允许黑客远程入侵、窃取用户信息（账号密码）等。
		RiskWare[RiskTool]/Win32.IMEStartup	低	此威胁是一种风险软件类程序。它能够隐藏系统中文件、隐藏 windows 中运行的应用程序、终止活动进程。
		GrayWare[AdWare]/Win32.Persi	低	此威胁是一种恶意广告的灰色软件类程序。该家族入侵用户电脑后，会劫持用户的浏览器，然后不断弹出广告。

（上接第一版）

访问 WinCC 系统数据库，来实现在局域网中的传播与更新，以及通过劫持 DLL 来攻击西门子系统的 PLC（可编程逻辑控制器）的行为，并确定震网注入的 PLC 代码只有在某种具体的硬件设备中才能正常发挥作用，这进一步表明它的针对性极强。

2.3 推演震网干扰离心机的作用机理

2012 年 1 月 17 日，安天微电子与嵌入式安全研发中心发布报告《WinCC 之后发生了什么》，推测震网可能的攻击场景机理：假设离心机转速采用 PID 算法实现自动控制，震网蠕虫攻击 WinCC，修改数据库中的 PID 算法相关参数，则离心机转速就会发生变化，甚至导致离心机转速自动控制失灵，轻则导致离心机分离功率和分离系数下降，分离核燃料级或者武器级铀 235 失败（铀 235 浓度不足）。

2.4 确定震网和毒曲病毒的同源性

另一个高度复杂的 Duqu 病毒浮出水面后，安天工程师提出了 Duqu 和 Stuxnet 可能存在同源性的猜测。2011 年 9 月，安天发布了《Duqu 和 Stuxnet 同源性分析报告》，其中对毒曲（Duqu）病毒的模块结构、编译器架构、关键功能进行分析，发现 Duqu 与 Stuxnet 相应结构和功能具有一定的相似性，同时在分析 Duqu 的解密密钥、反跟踪手段、程序 BUG 时，发现病毒作者编码心理特点与 Stuxnet 的逻辑相似。通过在 Duqu 与 Stuxnet 样本中发现的相同逻辑判断错误，由编码心理学的方法判断两者具有同源性，发布了关于 Duqu 与 Stuxnet 同源性的分析报告，并在《程序员》杂志发表了相关文章。

2.5 对火焰蠕虫的马拉松接力分析

火焰病毒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。2012 年 5 月 28 日，安天成立了针对火焰（Flame）病毒的分析小组，开始了为期数月的马拉松式分析，归纳了火焰的六次版本更新，发现了潜在的衍生文件。同时在漏洞攻击模块中发现了 Stuxnet 使用过的 USB 攻击模块，确立了两者的同源关系。经过 2 个月分析，安天发布了近 100 页的《Flame 蠕虫样本集分析报告》，但此事分析工作仅覆盖了不足 5% 的火焰病毒的模块，同时此事也触发了安天 CERT 对这种逐个模块堆砌式分析的反思。

2.6 安天对震网、毒曲、火焰系列分析工作的自我反思

2012 年 6 月 15 日，“网络空间新阶段安全威胁”高峰论坛在北京举行，业内部分专家和企业界工程师参加了本次论坛，并深入探讨了国内 APT 攻击的研究现状和发展。安天在此次会议上做了题为《管中窥豹—Stuxnet、Duqu 和 Flame 的分析碎片与反思》的报告。报告对安天在相关 APT 攻击样本的分析中的经验教训做了归纳总结，从人力投入结果、分析成果产出周期等和卡巴斯基等国际友商的进展做了对比。对这种完全以逆向样本模块分析视角展开的分析工作思路做了反思和自我批判，提出了要以工程体系对抗思维来看待 APT 分析工作。该报告录音整理稿刊登于当年的《信息安全与通信保密》杂志。

3、2013~2017 走向高级恶意代码体系分析

3.1 分析组件结构和持久化方法

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，并深度跟进 A^2PT 组织的新的恶意代码。2015 年初，卡巴斯基曝光了美国情报机构 NSA 下属方程式组织所使用的能够对硬盘固件进行持久化的木马。这也给安天公开发布分析成果创造了契机。2015 年 3 月，安天中英文双语发布第一篇关于方程式组织的分析报告《修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件》。报告对方程式组织相关组件：EquationLaser、EquationDrug、DoubleFantasy、TripleFantasy、Fanny 和 GrayFish 的关联做了独家分析，并基于卡巴报告的指引，对硬盘固件重新编程机理和攻击模块 nls_933w.dll 做了强化分析，验证了超高网空行为体可在一切可持久化场景中实现持久化的能力。

3.2 解密方程式组件的加密方式

2015 年 4 月 19 日，安天中英文双语发布第二篇关于方程式组织的分析报告《方程式（EQUATION）部分组件中的加密技巧分析》。在报告中安天对部分组件中的加密技术进行了分析，特别对该组织的本地注册表数据和远程通讯数据算法进行分析，指出该组织使用修改后的 RC 对称算法，并给出了完整的解密算法和密钥结构和二级密码表。该成果是对方程式组织加密机制的最早分析曝光。

3.3 分析方程式组织全平台作业能力，独家曝光 Linux 和 Solaris 样本

2016 年 4 月 27 日，首届中俄网络空间发展与安全论坛在莫斯科举行，安天技术负责人在论坛上做了题为《熊猫的伤痕——中国遭遇的 APT 攻击》的报告，报告以三组攻击的可视化分析介绍了三个威胁行为体对中国的网络攻击。这是中国安全厂商首次在国际会议上介绍中国遭受的 APT 攻击。在报告中，安天披露该组织样本具有全操作系统平台作业能力。

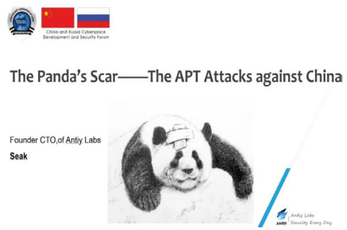

图 熊猫的伤痕——中国遭遇的 APT 攻击

2016 年 11 月 4 日，安天发布第三篇关于方程式组织的分析报告《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》中英文版，在报告中安天解密了该组织的几乎无死角的、全平台化攻击能力，全球独家解密了其 Linux 和 Solaris 平台的样本。在该报告中安天对此做了一个形象的比喻，我们需要破解的已经不只是一个“方程式”，而是更为复杂的“方程组”。

（下转第四版）