安天发布《Sodinokibi 勒索病毒分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Sodinokibi 的勒索病毒。该勒索病毒主要通过钓鱼邮件进行传播，利用伪装邮件主题、文件名称、文件图标等带有迷惑性的内容诱导受害者进行点击。主要攻击对象包括商贸、科技、机关等公司或单位的人员。

在最近的一次攻击事件中，攻击者向受害者发送带有附件的钓鱼邮件，钓鱼邮件中携带恶意 word 附件，一旦受害者打开了恶意 word 附件，便会下载 Sodinokibi 勒索病毒。Sodinokibi 运行后首先将自身设置为自启动，如果被感染的机器启用了 UAC 功能，Sodinokibi 会获取运行许可，接着加密所有非系统运行环境路径的所有非 PE 文件，并将文件后缀改为随机变化的后缀名来加密受害者的文件，随后，执行命令删除并禁用全盘所有卷影副本。最后，修改桌面背景并创建一封勒索信，勒索信中提供了付款链接和解密方案网址，受害者在该网址中输入勒索信上的 key 和被加密的后缀，就会跳转到勒索界面，勒索金额为价值 2500 美元的比特币，如果延期两天后付款将提高到价值 5000 美元的比特币。

勒索病毒给企业和个人的数据安全带来了严重的威胁，一旦主机被入侵，主机中的文件都有可能被加密，而且被加密文件将难以恢复，因此防护显得极为重要。安天建议广大用户，不要将数据安全立足于加密后的数据恢复，应该安装杀毒、防毒软件（参考安天智甲工具）并及时升级系统和修补设备漏洞；对重要的数据文件进行备份，避免弱口令的使用，避免使用统一的密码。确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件来源于内部组件，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、文件来源信息鉴定器、文件元数据鉴定器、数字证书鉴定器、动态（Win7 x86）鉴定器、动态（Winxp）鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	290 KB
MD5	FB68A02333431394A9A0CDBFF3717B24
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=FB68A02333431394A9A0CDBFF3717B24

◆ 运行环境

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 进程监控

PID	创建	创建
1328	target.exe	"c:\72bf8036177e4b1c991520f7e19b36ee\share\target.exe"

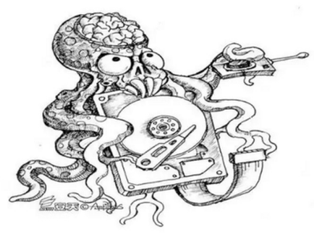
◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	137	192.168.122.255	137
0.0.0.0	68	255.255.255.255	67
192.168.122.111	138	192.168.122.255	138
192.168.122.111	123	13.70.22.122	123
192.168.122.1	67	192.168.122.111	68

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 06 月 10 日 (总第 186 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

重磅 | 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

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。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。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》，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》，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》，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》，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”、“火焰”、“毒曲”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”

（下转第二版）

（上接第一版）

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。

扫描二维码查看详细复盘分析

每周值得关注的恶意代码信息

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

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.ZooPark.b[prv,spy] 2019-06-01	该应用程序是一款间谍软件，运行后获取 root 权限，窃取用户短信、联系人、通话记录、地理位置、浏览器记录、日历记录、相册，手机各项基本信息，私自拍照、录音、录像、截屏，并将用户隐私上传至服务器。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.wandaPay.a[pay,exp] 2019-06-02	该应用程序包含恶意支付插件，监听短信并拦截删除支付短信，私自发送订阅短信，还可能包含色情内容，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.waaSpy.a[prv,rmt,spy] 2019-06-03	该应用程序为间谍应用，接收远程指令，上传用户短信、联系人、浏览器书签、照片、通话记录等信息，还会执行发短信、录像录音、照相等危险行为，造成用户隐私泄露，建议卸载。（威胁等级高）
	较为活跃样本	Trojan/Android.skcppostsol.a[rog]	该应用程序包含风险代码，可能会私自联网下载、安装未知应用，可能会对用户造成安全威胁，建议立即卸载。（威胁等级中）
		Trojan/Android.sesay.a[rmt,prv,spy]	该应用程序为间谍应用，接收远程指令，上传用户短信、联系人、浏览器书签、照片、安装包列表、位置等信息，还会执行发短信、隐藏图标、截屏等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.LockScreen.ck[rog,lck]	该应用程序运行置顶勒索界面，要求用户付费解锁，影响用户手机的正常使用，建议立即卸载。（威胁等级）
		Tool/Android.FrpPass.a[sys]	该应用程序为绕过 frp 验证工具，可能通过模拟按键绕过验证，如果手机被盗，可以进行非正常刷机，或者恢复出厂设置，请谨慎使用。（威胁等级中）
		RiskWare/Android.WBDPbocai.a[rog]	该应用程序是线上博彩游戏，其内容可能给用户的财产带来较大风险，且难以保障财产权益，请谨慎使用。（威胁等级低）
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-2019-0725）	当攻击者向 Windows DHCP 服务器发送经特殊设计的 DHCP 数据包时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在服务器上执行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Proxy]/Win32.Glupteba	此威胁是一种可以利用受害者计算机做为代理进行恶意操作的木马家族。该家族样本运行后连接远程服务器，攻击者可以通过被感染的计算机进行各种恶意操作，如发送垃圾邮件。（威胁等级中）
		Trojan[Monitor]/Win32.Ardamax	此威胁是一种具有监听功能的木马程序，通常捆绑在一些程序安装包中，运行后会开启监听功能，收集用户信息。（威胁等级中）
		RiskWare[Downloader]/Win32.Delf	此威胁是一种使用 delphi 语言编写的具有下载行为的风险软件家族。该家族通过邮件、P2P 网络等方式进行传播。该家族运行后，会在电脑中下载并执行恶意程序。（威胁等级中）
		Trojan[Dropper]/Win32.ChromPatcher	此威胁是一种具有捆绑行为的木马类程序。该家族会在后台记录收集用户信息并回传。（威胁等级中）
		Trojan[Backdoor]/Win32.Bedep	此威胁是一种带有后门的木马类程序。通过其他恶意代码传播，可以直接加载在内存中运行。（威胁等级中）

关注端点：对抗网络犯罪五个步骤

Matthew Lewinski / 文　安天技术公益翻译组 / 译

如今，各行各业遭遇的网络攻击越来越多，而网络犯罪分子也比以往任何时候都更加精明了。虽然 IT 漏洞的总数正在减少，但是“严重”漏洞的数量正在增加，漏洞实际被利用的数量也在增加。企业时刻面临被攻击的风险，这些攻击通常会造成破坏性的经济和声誉损害。随着智能手机、平板电脑等端点设备的日益普及，IT 团队不得不快马加鞭，以便赶上这种普及的速度。

“自带设备”（BYOD）计划和物联网（IoT）技术使该过程进一步复杂化，这是因为，连接到公司网络的每一台设备，都会增加公司受恶意软件和病毒感染的机会。许多访问公司数据的设备是移动设备，因此必须进行远程管理。通过部署端点安全策略，企业可以清晰地查看所有连接到公司网络的设备，因此这种策略必不可少。是否部署端点安全策略，会带来“顺畅的 IT 之旅”和“发生对业务产生重大影响的安全事件”之别。

企业可以采取以下五个措施来增强端点安全管理策略，对抗网络犯罪并保护敏感的公司数据。

实现资产管理的自动化并部署反病毒软件

对资产管理的可见性是关键所在。如果企业不知道其网络上有什么设备，那该如何进行管理呢？随着 BYOD 计划的日益普及，以及越来越多的 IoT 设备连接到企业网络，可见性变得越来越重要了。具备可见性，IT 部门就能了解物理资产的位置，实现流程的自动化，以便保护网络，减少（甚至消除）黑客能够利用的易受攻击的接入点。

通过建立对网络的可见性，IT 管理员还可以识别哪些系统需要部署反病毒软件。如今，越来越多的设备被添加到企业网络中，而且许多设备缺乏基本的安全和反病毒软件。因此，IT 团队应为每一台设备部署安全防护措施以防御攻击者，这一点至关重要。

实现补丁管理的自动化

补丁和软件更新会不断发布——不幸的是，许多用户却不能及时安装更新。通过自动化的补丁管理，IT 部门可以确保 Windows 和 Mac 平台以及可能存在漏洞的第三方应用（如 Adobe Reader 和 Oracle Java）及时接收并安装补丁。通过与 IT 安全审计相结合，自动化的补丁管理可帮助 IT 部门更快地发现潜在漏洞并识别不符合安全和配置策略的系统。

怀疑端点受感染时应快速响应

如果你怀疑端点感染了病毒，不要心存侥幸：请立刻将设备设置成初始状态。一旦设备遭到感染，再去修复会非常耗时且容易出错，并且无法确保问题不再发生。手动部署操作系统不利于 IT 部门采取适当措施来保护端点，但是实现这些流程的自动化则可以节省大量的时间，也能省去后面的麻烦。自动化的重建系统解决方案还可以提供简便的方式来促进更新，有助于保护网络安全，尤其是员工分布在不同的地域时。

确保可以远程跟踪和管理移动资产

简化移动端点管理的一种行之有效的方法是采用跟踪和管理软件。许多 IT 团队可能已经具备了基本的能力，但是，他们还需具备一些关键能力，如：识别企业网络上的所有设备并向移动设备发送特定命令以保护其安全。虽然具备可见性大有帮助，但 IT 团队也必须能够采取行动以保护关键数据。例如，如果移动设备丢失，IT 团队必须能够远程锁定该设备并擦除设备上的数据。其他关键的移动端点管理能力包括远程资产管理、设备解锁、口令重置和恢复出厂设置等。

确保适当的用户访问权限

为避免安全事件的发生，对于包含敏感公司数据的系统，必须向用户分配适当的访问权限。IT 团队必须能够轻松跟踪特定用户可以访问和正在访问的系统。默认情况下，用户只应分配最低限度的访问权限——虽然在有些情况下，他们可能需要拥有管理员权限。IT 团队应该了解每位用户具有哪种类型的访问权限，以防止过度授权的用户无意中传播恶意软件并导致敏感数据泄露。

通过实施上述端点管理最佳实践，IT 团队可以增强其数据的安全性，并最大限度地减少网络中易受攻击的接入点的数量。领先于攻击者意味着，企业需保持最新的端点策略并简化复杂的端点问题。为了最好地保护企业，IT 团队必须全副武装，随时准备好迅速采用可用的最佳工具，以便对抗攻击者。

原文名称	Focusing on Endpoints: 5 Steps to Fight Cybercrime
作者简介	Matthew Lewinski。Matthew Lewinski 是 Quest Software 公司的杰出工程师。
原文信息	2019 年 5 月 31 日发布于 Dark Reading 原文地址 https://www.darkreading.com/perimeter/-focusing-on-endpoints-5-steps-to-fight-cybercrime/a/d-id/1334754
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。