安天发布《DorkBot 僵尸网络样本分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一种名为 Dorkbot 的僵尸网络开始活跃。Dorkbot 僵尸网络最早在 2011 年 4 月被首次发现，其使用的攻击手段包括后门植入、密码窃取和其他恶意行为。Dorkbot 的传播途径也非常广泛，包括 USB 设备、IM 客户端、社交网络、电子邮件及隐蔽式下载。Dorkbot 的主要攻击目标是盗取用户凭证以及各种能够识别个人身份的信息。它同时还能够在受害者的 PC 上，通过控制服务器安装更多的恶意程序。

DorkBot 恶意软件被打包在一个 dropper 中，其中 payload 被嵌入到一个 RC4 加密的 blob 里。该 blob 可以在二进制编码的资源部分中找到，并且使用 Base64 编码。dropper 先对 Base64 编码的 payload 进行解码，然后对其进行后续解密，最后的结果由一段用于 PE 加载的 shellcode 和恶意软件原始二进制文件组成。在解密之后，控制权被移交给位于原始二进制文件中的 shellcode，然后将其进行装载并执行入口处代码。 Payload 拥有检验参数、拷贝自身、反虚拟机、终止自启动进程、APC 注入等功能，同时它会对文件修改进行监控，一个线程会不断计算 %appdata% 下复制的恶意二进制文件的 CRC32，并将其与原始文件的 CRC32 进行比较。一旦发生变化，复制文件会被删除，将其重写为原始文件的内容。

安天 CERT 提醒广大政企客户，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

目前，安天追影产品已经实现了对该类恶意代码的检出。

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、反病毒引擎鉴定器、动态（Win7 X86）鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据反病毒引擎鉴定器、BD 静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	1ec36fc1bb6bce36dd3a82304be237919ede3e6b790b7a248c340042353b5bc0
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	250 KB
MD5	5C55FC257423ACD1AE6382D88B1EE306
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
判定依据	反病毒引擎鉴定器、BD 静态分析鉴定器、动态行为鉴定器

报告链接：https://antiy.pta.center/_lk/details.html?hash=5C55FC257423ACD1AE6382D88B1EE306

◆ 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

◆ 危险行为

行为描述	危险等级
向其他进程内存写入数据	★★★
检测虚拟机	★★★★★
删除自身	★★★★
远程注入其他进程	★★★★
延时	★★★

◆ 常见行为

行为描述	文件 MD5
获取驱动加载权限	★
在其他进程中申请内存	★
查询 windows product key	★★
获取计算机名	★
枚举进程	★
创建挂起进程	★★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 12 月 10 日（总第 163 期）试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

美国网络空间攻击与主动防御能力解析（十一）

——美国网络空间的能力演进

安天研究院

在之前的文章中，我们分别展开介绍了美国大型信号情报获取项目，网空积极防御体系，网空进攻支撑体系以及包括用于突破物理隔离、持久化控制、漏洞利用、命令与控制和利用无线信号的网络空间攻击装备体系，全面解析了美国在网络空间的攻击与积极防御能力。在文本中，我们将对美国网络空间攻击与积极防御能力的演进进行分析，展现其未来发展的趋势。

随着网络技术的快速发展、网络场景的不断变化，美国在网络空间中的进攻与积极防御能力也会不断演进。为了应对未来可能出现的新威胁，必须对美国未来网络空间的能力演进进行研究，分析可能出现的新变化、新趋势，对未来的敌情进行合理的推测，以此建立有效的敌情想定，在此基础上发现我方防御能力的不足，指导我方网络空间防御体系的不断完善。未来美国网络空间的能力演进主要表现在战略思想、网络空间防御能力、网络空间进攻能力等几个方面。

一、 战略思想上的转变

2018 年 9 月，特朗普政府发布了《国家网络战略》，这是继小布什政府的《网络空间安全国家战略》（2003 年）后，15 年来美国公布的首项内容全面的网络战略。该战略强调对关键基础设施的保护、与私营企业合作、保护政府网络以及建立更强大的合作伙伴关系以共享威胁情报信息。与以往类似政策不同的是，《国家网络战略》展现了美国政府在应对网络空间对手方式上的转变，称为达成有效威慑，要让网络恶意行为体承受“反应快速、代价巨大、清晰可见的后果”。可以看出，特朗普政府计划加强进攻性网络行动，通过先发制人的网络攻击威慑对手。

同月，美国国防部发布了《2018 国防部网络战略》，该战略概述了一项军方如何处理网络安全的更为详细的计划，即以“防御前置”的方式从源头上破坏或制止恶意网络活动。所谓“防御前置”，实际上是强调网络进攻。几乎在同一时间，美国国家安全总统备忘录 13（NSPM 13）提出，美国总统可以将某些网络权限授予国防部长执行特定任务，以加速网络行动。NSPM 13 在很大程度上消除了奥巴马政府实施的长时间的机构间审批程序，使得军方更容易发起进攻性网络行动。

美国政府和军方的一系列动作，代表着美国网络安全从防御到攻击态势的危险转变，增加进攻性网络行动的做法可能会加剧网络冲突。一方面，快速的网络行动意味着没有足够的时间留给政府针对网络攻击事件进行追踪溯源，很有可能使美国攻击错误的目标；另一方面，“进攻是最好的防御”这一观点在网络空间中不能成立，先发制人的网络攻击并不能形成针对对手的有效威慑能力。

二、 网络空间防御能力持续提升

在网络空间防御方面，美国建设了国防部积极防御系统“监护”（Tutelage），并将相关技术应用到了旨在保障联邦政府机构网络安全的“爱因斯坦”计划中。在不断建设和演进过程中，正在形成一套具有完备有效的感知能力、积极防御及反制能力的国家网络空间安全防御体系。

应对外部威胁方面，在原有防御体系基础上，美国安全部门也投入了大量的人力、资金设立新的研究计划和项目，以应对网络空间中的各类威胁。NSA 的“零日网络防御计划”（Sharkseer），旨在利用商用成品（COTS）快速检测和缓解基于 Web 的恶意软件、零日漏洞和高级持续性威胁，并实现不同密级间的情报数据实时共享。此外，美国陆军正在测试欺骗性的网络防御技术——网络空间欺骗能力，该技术旨在诱骗攻击者让其误认为已经攻破计算机网络，可用于提供预警、虚假信息、混淆、延迟或其他方式阻止网络攻击者。在需要时，该技术还能通过欺骗攻击者，诱导出更多情报，进而驱动反击行动。

另一方面，长期以来以斯诺登为代表的各类泄密事件，给美国政府造成了巨大的损失。因此，美国情报机构高度重视内部威胁，并通过各种举措应对内部威胁。早期，在“7 号军火库”（Vault 7）中有一款名为“涂鸦”（Scribbles）的 CIA 网空装备，Scribbles 是一款用于将网络信标标签嵌入机密文档的软件，即在 Office 文档内部嵌入一个透明水印图片组件，用于追踪可能被内部人员、举报者、记者或其他人员复制的文档，以便监控机构追踪泄密者和外国间谍。Scribbles 的最新版本于 2016 年 3 月 1 日发布，在 Office97 至 2016 版本上通过测试，标记授权日期直至 2066 年。此外，在情报共享中，美国国家情报总监办公室（ODNI）选择可信数据格式（TDF），采用基于属性的访问控制，既可以指明接收者的身份及业务信息，也可以指明允许处理数据的终端或环境特性，以此保障安全受控的共享。

三、 网络空间进攻能力不断加强

通过之前对国家安全局（NSA）和中央情报局（CIA）的网络空间装备体系的梳理和分析，我们在一定程度上了解了美方网络空间装备库全平台、全功能的特点。《2018 国防部网络战略》中，将“加速网络能力开发”作为实现“建立更具杀伤力的联合部队”这一目标的重要举措。未来美方会不断丰富自己的网络攻击装备体系，并向覆盖更广泛、能力更全面的方向不断演进。

在漏洞挖掘、收集和利用方面，美方的优势能力无论是在“震网”（Stuxnet）还是“魔

（下转第二版）

（上接第一版）

窟”（WannaCry）事件中都得到了很好的证明。“震网”事件中，美方使用了5个Windows零日漏洞和1个西门子的零日漏洞，以一种看似近乎挥霍实则精妙组合利用零日漏洞的方式，实现了通过网络空间作业对伊朗核设施造成物理破坏的效果，几乎永久地迟滞了伊朗核计划，达成了美方的战略意图。2017年5月全球爆发大规模的“魔窟”感染事件，只是利用了NSA泄露的众多漏洞之一，就引发了席卷全球的勒索病毒感染事件，美方的漏洞储备能力可见一斑。未来美方将会持续加强其在漏洞挖掘和储备上的优势能力，并且不排除美方存在利用其在供应链上的优势，向设备中埋入漏洞的可能。类似地，在持久化控制、突破物理隔离、命令与控制等方面，美方将在目标覆盖范围、全面性、隐蔽性等方面持续提升，继续保持优势能力。

除了不断加强已有的攻击能力外，随着各种新设备的出现和新技术的逐渐成熟，新的攻击手段将会逐渐从研究进入实用。在Black Hat 2018上，研究人员展示了利用传真机对企业内部网络进行渗透的实例，只需掌握传真机的电话号码，就能对传真机进行攻击，并以其作为跳板，侵入内网。类似地，未来的演进趋势还包括：针对各类IoT设备，包括智能手表、音响、耳机、眼镜、摄像头，甚至汽车等的攻击将更加普遍；利用声、光、电、热、电磁波等建立信道，实现隐蔽通信的技术可能会逐渐成熟，被更多地应用在攻击行动中；通过无人机抵近目标，进行侦察、入侵、控制、窃取的作业方式可能逐渐增多等。

面对这些变化，应该如何完善我方的防御能力，以应对可能的挑战呢？首先应基于敌情的演进建立敌情想定，将高能力对手的敌情存在作为基本假设，包括内网已经被渗透、任何内网设备都可能被攻陷、我方人员已经被敌方策反、供应链已被敌方渗透、敌方有能力劫持我方设备采购的物流链等，以极限化的敌情想定驱动防御能力的演进。

在具体的网空防御体系建设中，需要强化已有静态的防御机制实现兼顾“结合面”与“覆盖面”的综合防御能力体系。将网络安全防御能力与物理、网络、系统、应用、数据与用户等各个层级深度结合，在信息化环境各层级结合网络安全防御能力，使防御能力与实际情况紧密结合；将网络安全防御能力部署到信息化基础设施和信息系统的“每一个角落”，力求最大化覆盖构成网络的各个组成实体，避免由于在局部的安全盲区或者安全短板而导致整个网络安全防御体系的失效。同时还必须加快建设动态防御能力体系，其中关键是针对网络空间时代的高水平复杂威胁行为体展开协同响应对抗的积极防御能力。最终实现构建具有与网络信息基础设施“深度结合、全面覆盖”的综合防御特点、强调“掌握敌情、协同响应”的动态防御特点的网络空间防御体系。

在之后的的文章中，我们将对美国网络空间攻击与积极防御能力进行总结，并对如何进行系统的应对提出建议，敬请期待。

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有6个移动平台恶意代码和5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.strongservice.a[prv,rmt,spy] 2018-12-03	该应用程序运行后隐藏图标，利用屏幕录制漏洞，针对安卓5.0-6.0系统的手机进行屏幕截图并上传，接收远程指令上传用户短信、联系人、通话记录、照片、浏览器书签等隐私信息，还会执行拍照、录音等危险行为，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.CellSpy.c[prv,spy] 2018-12-04	该应用程序伪装系统应用，实际为间谍件，通过配置后，可隐藏图标，后台通过邮件收集用户联系人、通话记录、位置、收件箱短信等隐私信息，造成用户隐私泄露，请卸载。（威胁等级中）
		Trojan/Android.Mobilespy.bb[prv,rmt,spy] 2018-12-05	该应用程序伪装正常软件，运行接收远程指令，窃取用户定位信息、短信、通讯录和通话记录上传至服务器，还会私发短信，造成用户资费损失和隐私泄露，请立即卸载。（威胁等级中）
	较为活跃样本	G-Ware/Android.Dropper.bx[sys,rog]	该应用程序运行诱骗用户获取Root权限，解密子包，私自安装程序到系统目录。严重影响用户使用，给手机带来未知风险。建议卸载。（威胁等级中）
		Trojan/Android.Locker.bj[rog,lck]	该应用程序伪装为公安相关应用，运行加载恶意子包进入勒索页面，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。（威胁等级中）
		Trojan/Android.FraudBot.a[exp,fra,bkd]	该应用程序伪装应用，运行后解密恶意子包，联网私自下载其他恶意应用，加载广告并模拟点击，弹出虚假调查表格诱导用户填写个人信息，并且存在后门。造成用户流量消耗和隐私泄露。（威胁等级高）
PC平台恶意代码	活跃的格式文档漏洞、0day漏洞	Microsoft Excel 安全漏洞（CVE-2018-8574）	当Microsoft Excel软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用Microsoft Excel打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。（威胁等级高）
	较为活跃样本	RiskWare[Downloader]/Win32.InstallVibe	此威胁是一种具有下载行为的风险软件类程序。该病毒家族的样本会在执行后启动一个下载器，在后台下载其他恶意代码文件并执行。与此同时，该病毒家族的样本会释放出一个恶意的DLL文件到%TEMP%文件夹中。（威胁等级中）
		GrayWare[AdWare]/MSIL.Solimba	此威胁是一种具有下载行为的风险软件类程序。该病毒家族的样本会在执行后下载大量第三方的应用程序并安装。并且该病毒家族的样本会注入其他的进程使自己难于清除。（威胁等级中）
		RiskWare[Downloader]/MSIL.Temonde	此威胁是一种可以下载推广应用的风险软件家族。该家族样本运行后连接远程服务器下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级低）
		RiskWare[WebToolbar]/Win32.Perinet	此威胁是一种具有安装浏览器扩展工具栏行为的风险软件类程序。该病毒家族的样本会在执行后安装一个浏览器扩展工具栏。并且该病毒家族的样本会注入其他的进程使自己难于清除。（威胁等级中）

简析“强壮的基础设施”

Brett Johnson/ 文　安天技术公益翻译组 / 译

采用“强壮的基础设施”可以防止类似配置不一致等常见问题导致的一系列问题，为基础设施带来更高的一致性和可靠性，以使得部署过程更简单、更可预测。

“强壮的基础设施”是将“基础设施即代码”（Infrastructure as Code，IaC）应用于实际运行环境的最终目标。基础设施配置完全通过代码和配置文件执行，并通过验证检查来确保最终实际运行的配置文件内容始终与早期预定义值保持一致。

实现真正“强壮的”环境需要高度成熟的流程，包括从基础设施管理到代码管理的各个流程。编写代码和配置的运营团队必须是受信任的，这样，企业才能够信任代码。

创建信任和成熟度没有捷径，只能通过实践（包括成功和不成功的实践）来实现。借鉴其他企业的经验教训，虽然能够防止犯相同的错误，但非捷径。

采用“基础设施即代码”实践，能够逐步实现“强壮的基础设施”，构建一个用于部署基于代码的配置框架。“强壮的基础设施”和“基础设施即代码”的主要区别在于“强壮”这一关键词。

实现“强壮”意味着，定义的设置与实际运行的设置之间没有差别。这需要自动端到端代码发送和验证；并在新配置达到主存储库后立即进行配置更新。

此外，还需要定期检查，以检测配置偏差，并在发现偏差后触发补救任务或告警。

基础设施的定义不仅限于物理硬件；还扩展到Kubernetes、Ceph、vSphere和OpenStack等软件平台。

通过REST和RedFish等协议编写API，能够提高编程交互和端点管理能力。标准API提高了交互能力，但并未简化任务。

将“强壮的基础设施”付诸实践

在下文中，我们将介绍强壮的基础设施的一些关键概念。

预期状态：首先，我们需要定义基础设施所需的设置；这可能是DNS或NTP设置，或者其他任何设置。如果目标基础设施已经存在，则已有的配置文档就是一个很好的初始信息源。此外，不要忘记验证环境中的配置，因为配置文档有可能是过期的。

大多数配置管理人员都不会要求应用所有的设置。在扩展设置之前，你可以在小范围内构建或验证设置。如果采用这种方法，维护所有设置的清单并跟踪每个设置的状态会很有帮助。

测试：在不同阶段进行测试，以降低犯错的风险，提高总体成功率。正确的测试覆盖范围较广，涵盖可能发生的多种成功和失败情况。

单元测试在函数层级测试代码，检查函数的输出是否与基于指定输入的预期值一致。测试驱动的设计规定：应该在编写代码之前编写单元测试。

集成测试用于测试代码函数之间或系统之间的集成，这类测试可能难以执行。

编排器：要想在更改基础设施时避免服务中断，通常需要先运行其他任务。例如，在启动任务之前将工作负载从一个主机切换到另一个主机。

编排器将多个工作流链接起来，并提供特定于该任务的外部逻辑。在配置交换机之前，编排器可能会进行检查，以确保冗余的配置正常运行。即使配置失败，该交换机也能正常运行。

CICD集成/交付流水线：流水线将不同开发环境中的代码投入到生产中，触发验证和合规测试。

使用流水线的目的是：自动从开发人员的计算机获取代码，将获取的代码集成到主代码库中，并交付这些代码。在这种情况下，其目的可能是配置文件更改。

工作流执行：触发器是启动工作流的事件。触发器可能是手动启动工作流的用户，也可能是计划任务或基于事件的触发器。

“计划任务”会定期运行，可能需要“splay”来更改启动时间。“splay”会为启动时间添加轻微的随机化（在给定范围内），通常为±配置值。

当收到git pull请求时，一个常见的、基于事件的触发器就会运行。它启动工作流，针对提交的代码执行各种测试——在代码合并之前，这些代码必须通过测试。代码合并可以触发相关的工作流，迅速将新配置应用于基础设施。

从概念上看，使用触发器自动执行配置更改是很容易的，但在实践中却很难。这需要了解所做的更改以及这些更改的任何潜在影响。此外，还需要实施完全基于代码的验证和回滚计划。

原文名称	Introducing Immutable Infrastructure
作者简介	Brett Johnson。Brett Johnson是VMware公司的高级顾问。
原文信息	2018年11月30日发布于Network Computing 原文地址 https://www.networkcomputing.com/networking/introducing-immutable-infrastructure/816408157
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。