安天发布《tRat 远控木马样本分析报告》

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 tRat 的远控木马。该木马基于 Delphi 编写，攻击者使用垃圾邮件传播，通过宏病毒的方式下载 tRat 到受害者机器。

tRat 使用的宏病毒文档内容一般是知名公司的广告，以此来诱导用户点击启用宏的按钮；另外，还会以“invoice”这种模仿发票的常见垃圾邮件传播恶意代码的方式来进行攻击。一旦用户点击了启用宏的按钮，宏代码即连接网络下载 tRat 远控木马并执行。样本首先会复制自身到 %appdata% 下实现持久性，接下来，tRat 在启动目录中创建一个 LNK 文件，在系统启动时会直接执行恶意代码。样本中的大部分内容使用了加密，通信的数据也被加密并使用十六进制编码进行传输。恶意代码回传的“AUTH_INF”中，使用冒号分隔两个字符串，第一个字符串是其硬编码的标识符，第二个字符串是加密的系统信息，包含受害主机的计算机名称、系统用户名和 tRat 的 botID。恶意代码还拥有向 C2 发送请求下载模块的功能，目前可以发送命令“MODULE”，接收模块后可以将其作为 DLL 加载。

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。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：

文件由页面手工提交，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、数字证书鉴定器、文件元数据鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、智能学习鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）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	cd0f52f5d56aa933e4c2129416233b52a391b5c6f372c079ed2c6eaca1b96b85
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	176 KB
MD5	9FAEF92CBFCAE8C809636A908221E775
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.CMY3U
判定依据	反病毒引擎

◆ 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
延时	★★★
向其他进程内存写入数据	★★★
创建挂起进程	★★
终止进程	★★
在其他进程中申请内存	★
壳行为填充导入表	★★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
DNS 请求	★
连接网络	★
疑似桌面控制	★

◆ 进程监控

PID	创建	命令行
1408	target.exe	"c:\0af71267965a4de98da43cf234295ff5\share\target.exe"
6548	target.exe	"c:\0af71267965a4de98da43cf234295ff5\share\target.exe"

◆ 常见行为

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 17 日 (总第 164 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（总结篇）

安天研究院

习总书记在网络安全和信息化工作座谈会上曾指出“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”在这个过程中，对于网空威胁行为体，特别是以美国情报机构为代表的超级网空威胁行为体的认知就构成了我们建立自身防御能力和威慑能力的重要前提。与传统战争领域相同，网络空间的博弈对抗也要建立客观充分的敌情想定，深入分析敌我当前的体系、能力、态势、装备、编制、战法等相关因素。要在未来的博弈竞合中占据主动，既要发挥我们的传统优势和积累，又不能拘泥于原有的视野和惯性；既要把美方作为一个超级网空威胁行为体来对待，又要把其作为一个能力引领方来看待。为此，在之前的 11 篇解析文章中，我们对美方的大型信号情报获取项目、网空安全积极防御体系、网空进攻性支撑体系、网空攻击装备体系等分别进行了展开介绍，并对未来的能力演进进行了分析，从多个角度呈现了其在网络空间的强大能力。在本篇中，我们将总结美方在网络空间的能力优势和特点，并对应如何建设相应的防御能力提出相关思考和建议。

在网络空间的各个维度，美方都代表了

美方全球信号情报获取节点分布

最强能力。在复杂的组织、庞大的人员规模和充沛的安全预算保障下，美方建设了一系列大型工程系统，形成了支撑网空行动的工程体系，并依托这些工程体系，将情报获取、积极防御、进攻作业以及相关的支撑环节等网空能力逐步整合成为整体的国家能力。

美国具有国家安全至上的传统，随着国力发展，逐渐将全球无死角的监听与情报作业能力视为其全球利益和霸权的基石。从上世纪 40 年代开始，美国陆续通过“三叶草”、“尖塔”等计划，建立了对电报电话系统的监听存档机制，并从上世纪 60 年代开始建设以“梯队”为代表的各类信号情报获取系统，以形成情报网络基础。通过大型海底光缆监听、重点特殊区域监听、计算机网络利用（CNE）、运营商入侵、卫星监听、第三方情报共享等方式，美方能够在全球范围获取包括电子邮件、文件传输、语音通话、网络访问、短信、传真、电报等在内的各类网空信号情报，形成了网空作业的“先天优势”。特别是对于海底光缆和运营商的窃听，使美方在信号获取和投入侧都具备了无与伦比的隐蔽性掩护和反溯源性优势。

为实现对特定区域、目标，特定类型信号情报的获取，在大型信号情报获取系统的基础上，美方开展了大量针对性的信号情报监听项目，被斯诺登曝光的美国国家安全局（NSA）的“棱镜”项目就是其中的代表。据不完全统计，近年来被披露的美方信号情报监听项目已超过 30 个。通过这些监听项目，美方就可以实现对全球互联网人员目标、信道目标、设备目标等完整的画像，从而形成比较精准的目标定位能力。

在覆盖全球的信号情报获取能力基础上，美方建立了以“湍流”为代表的进攻性能力支撑体系，通过被动信号情报获取、主动信号情报获取、任务逻辑控制、情报扩散与聚合、定向等情报相关的能力模块，实现完整的网空情报循环，并结合“监护”、“量子”等相应的网空攻防能力模块，进一步实现情报驱动的网空积极防御和进攻行动。

在美方的情报作业到军事行动中，美方并不认为网络空间是一个独立的例外空间，而是将其整合为相对统一的情报作业思维和

情报流程

战术方法论，将网络作业作为传统情报作业在网络空间中的延伸，将网空能力视为对传统物理域能力的叠加和增益。美国网空司令部认为“物理领域的优势很大程度上取决于网络空间的优势”，因此美方并没有单纯的网空作业的概念，而是强调多域联合和跨域切换。美方基于一套成熟的网空威胁框架来统筹攻击作业，指引威胁猎杀。这一框架，由管理、准备、交互、存在、影响、持续进程在内相关环节构成，美方对其进一步细化，形成了对应的字典式指南。

美方究竟采用哪种作业方式或作业组合是由希望达成的不同目的和效果决定的。因此，在美方的网空进攻作业中，往往采用人力近场作业、物流链劫持、电磁中继、社会工程学等多种方式相结合，实现作业目的。在作业入口与突破点方面，美方借助其网络目标画像、定位能力和全球

（下转第三版）

每周安全事件

类 型	内 容
中文标题	Google+ 新 API 漏洞泄露 5250 万用户私人信息
英文标题	Google+ to Shut Down Early After New API Flaw Hits 52.5 Million Users
作者及单位	Mohit Kumar
内容概述	谷歌 12 月 10 日表示，在社交网络 Google+ People API（应用程序编程接口）中发现严重漏洞，具有相关权限的开发人员可窃取 5250 万用户的私人信息，包括姓名、电子邮件地址、职业和年龄。该 API 称为 "People: get"，允许开发人员请求与用户配置文件相关联的基本信息，漏洞是在 11 月的软件更新中引入。谷歌表示该漏洞目前没有被利用或被任何第三方应用开发者误用的证据，并保证不会泄露密码、财务数据、国家识别码或任何其它敏感数据。在 2018 年 10 月份，Google+ 曾泄露了超过 50 万用户数据，当时谷歌表示将在 2019 年 8 月底之前关闭 Google+，在最新的泄露事件发生后，将比原计划提前四个月关闭 Google+。
链接地址	https://thehackernews.com/2018/12/google-plus-hacking.html

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	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.b4aspy.k[prv,exp,spy] 2018-12-10	该应用程序为 b4a 语言编写，运行后隐藏图标，窃取用户短信、联系人、通话记录等隐私信息并通过网络上传，还会私自录像，发送短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.SmsSpy.aq[prv,exp] 2018-12-11	该应用程序伪装短信系统应用，运行拦截用户短信，窃取用户短信发送到指定手机，造成用户资费消耗和隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.FakeGooSpy.a[prv,spy] 2018-12-12	该应用程序为间谍软件，伪装其他正常应用，运行会获取被控手机基本信息、联系人信息、通话录音、GPS 位置、特定文件后缀文件、照片等数据并通过 FTP 方式上传至远程服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.SmsThief.bx[prv]	该应用程序伪装系统应用，诱导用户点击，后台私自窃取用户信箱信息发送到指定地址，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		G-Ware/Android.FakeQB.i[rog,exp]	该应用程序伪装刷 Q 币工具，无实际功能，运行要求用户分享该软件并诱骗用户付费，造成用户资费损耗，请立即卸载。（威胁等级低）
		Trojan/Android.fakewechat.m[prv]	该应用程序伪装微信，运行诱导用户输入微信账号密码登陆，后台私自上传至服务器，造成用户隐私泄露，请立即卸载。（威胁等级中）
		RiskWare/Android.FakeSexApp.g[exp]	该应用程序伪装色情软件，主界面任意点击即下载其他交友类软件，可能造成用户流量消耗，建议谨慎使用。（威胁等级低）
		Tool/Android.Boomerang.a[prv,rmt]	该应用程序为一款短信监控应用，通过短信发送监控指令，其监控的功能包括未接来电列表、未读短信、电池状态、WIFI 开关、设备音量，使用不当则造成用户隐私泄露，请谨慎使用。（威胁等级中）
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-2018-8597）	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	GrayWare[AdWare]/Win32.StartSurf	此威胁是一种具有修改主页行为的推广类灰色软件类程序。该病毒家族的样本会修改全部浏览器的快捷方式，并将首页地址指向 istartsurf.com。（威胁等级低）
		GrayWare[AdWare]/Win32.Vopak	此威胁是一种有广告行为的灰色软件类程序，该家族运行在 32 位平台下，具有安装捆绑软件、修改浏览器主页和修改默认搜索引擎等行为。（威胁等级低）
		RiskWare[Downloader]/NSIS.DomaIQ	此威胁是一种具有下载行为的风险软件类程序。该家族通常使用 NSIS（开源的 windows 系统下的程序制作工具）将木马与正常程序捆绑在一起。DomaIQ 是一个安装管理器，可以管理要安装或更新的软件，其中包括工具栏、浏览器加载项、游戏应用程序等。（威胁等级中）
		RiskWare[WebToolbar]/Win32.FirstFloor	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族样本运行后会修改注册表中关于浏览器的数据，弹出病毒作者指定的广告页面，干扰用户的正常工作。它的部分变种拥有远程控制和下载器的功能。（威胁等级低）
		Trojan/MSIL.Tpyn	此威胁是一种使用 MSIL 中间语言编写的木马程序。该家族通常会安装并运行广告件程序，窃取用户信息并回传。（威胁等级中）

（上接第一版）

部署的信号情报监听节点，实现互联网目标的快速识别和流量注入，进而将恶意代码通过浏览器打入上网用户的节点中。对于非上网用户，美方也能够通过其他作业方式，依靠各类针对性的网空攻击装备，对物理隔离网络进行突破，之后再进行横向移动。美方的网空攻击装备体系具有制式化、全平台、全能力特点，从美方的装备研发思路来看，其始终确保攻击装备的全 IT 场景覆盖能力，针对各种端点设备、网络设备、网络安全设备研发储备 0Day 漏洞攻击工具和对应的恶意代码。美方所使用的恶意代码，基于一个可扩展的模块化框架，对功能进行细分到原子化的设计。同时依托精致、严密的指令体系进行细粒度的作业控制。保证作业的隐蔽性、谨慎性，减少木马被完整捕获的可能性，并有效穿透端点主动防御软件。

美方网空作业技术流程与部分工程和装备作用的映射

在网空积极防御方面，美方建设了以 NSA 的“守护”为代表的积极防御体系，通过国家级的信号情报能力，提前获知对手的攻击意图、技术、工具等信息，将相应规则部署到边界的高速深包处理设备，在对手发动进攻时及时发现，快速响应。对于高“价值”的对手入侵行动，通过边界的高速深包处理设备将对手引入能够高度模拟其网络的“网空欺骗环境”中，与对手进行“隔空对抗”，诱导出更多情报，并在需要时进行反击。美方在网空防御方面十分重视利用民间技术和产品，高度尊重网络安全产品和服务价值规律，以 NSA 为例，商用网络安全产品是构成其防御体系的重要一环。但商用安全产品和企业，并非美方防御能力的最强点。在这些商用产品基础上，其形成了对威胁实现理解和环节整体防御框架体系，并进一步与国家战略情报相互协同。将战略情报通过能力框架脱敏转化为可公开的防御规则和信标。同时，NSA 提出了“鲨鱼先知”积极防御计划，通过与安全厂商共享威胁情报，提高整体态势感知能力，进而实现更加有效的高级威胁发现和快速响应。此外，在旨在保护政府网络系统安全的“爱因斯坦 3”计划中，其入侵防御能力就来自于 NSA。美方通过军用安全能力和商用安全能力的深度结合，不断完善防御体系，提升防御能力。

面对体系化作业的超级网空威胁行为体，我们应该如何应对？首先，我们需要意识到，网空对抗是常态化的进行时，其没有非常清晰的平时与战时的差异。因此网空威慑模型不是类似“核威慑”，以后果不可承受达成“互不使用”模式，而是体系化的攻击与体系化防御的持续对抗模式。必须以网空防御能力建设为基本盘，以强大的防御减少对手的可攻击面、削弱对手的行动能力和提升对手的攻击成本，并进一步通过反制能力提升对对手的威慑。面对复杂的安全形势，重要信息系统和关键信息基础设施防御水平的高低会在关键时刻决定国家战略的主动程度。

对于关键基础设施和重要信息系统，有效的敌情想定是做好网络安全防御工作的前提，要围绕“敌已在内”、“敌将在内”建立极限化的敌情想定：高级威胁行为体有突破目标的坚定意志、充足资源和充分的成本承担能力；防御者所使用的所有产品和环节，是攻击方可以获得并测试的，任何单点环节均可能失陷或失效，包括网络安全环节；信息系统规划、实施、运维的全生命周期都是攻击者的攻击时点；供应链和外部信息环境都是攻击者可能的入手点；攻击者所使用的攻击装备有较大可能是“未知”的，即对于防御方以及防御方的支撑维护力量（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。同时，敌情想定要深入结合目标场景，避免将防御的重点和成本始终投入到容易看见或容易理解的威胁中去，而脱离了高级网空行为体带来的更隐蔽、更致命的威胁。

对于网络信息系统这样一个复杂系统，不可能靠一个单点技术变革和单点创新，或产品堆砌来应对安全问题，必须以体系化的防御来应对体系化的进攻，网络防御没有“银弹”和“永动机”。在网空安全防御体系建设工作中，根据网络安全研究机构 SANS 所提出的“滑动标尺”模型，安天参与将其翻译引入国内后，国内多家能力型厂商以此为基础，在取得共识后进行了延伸拓展，安天在其基础上进一步提出了叠加演进的网络空间安全能力导向建设模型。滑动标尺的基本模型将网空安全能力分五大类别，其中基础结构安全、纵深防御、积极防御、威胁情报等四大类别的能力都是一个完善的网络安全防御体系所必须的，而反制能力则是应当由国家级网空安全防御体系提供。在这些网络安全防御能力的支撑下，通过实战化的网络安全运行，实现全面完善的网空安全防御。

具体来说，在基础结构安全和纵深防御方面，重点要保障安全能力的“深度结合、全面覆盖”，即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的深度结合，并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”，最大化覆盖构成网络的各个组成实体。在此基础上，建设以态势感知为核心的威胁情报驱动的动态防御能力体系，做到“掌握敌情、协同响应”，重点是在敌情想定的基础上提升网络系统的可弹性恢复水平，特别是依靠具有动态特性的积极防御能力，在威胁情报能力的驱动下，通过全面持续监控发现威胁踪迹，并针对潜伏威胁展开“猎杀”行动，从而发现并消除威胁。此外，还要加强网络安全防护运行工作，将安全管理与防护措施落实前移至规划与建设等系统生命周期的早期阶段，将态势感知驱动的实时防护机制融入系统运行维护过程，支撑起协同联动的实战化运行，实现常态化的威胁发现与响应处置工作，不断提升网络安全水平。

本文是本系列文章的最后一篇，因篇幅所限，还有大量内容没有完全展开，同时在文章写作过程中，虽然我们力求严谨，但水平有限，避免不了可能存在各方面疏漏，请广大读者谅解。感谢您一直以来的关注，希望我们的工作能够为我国关键基础设施和重要信息系统的网络安全防护工作提供有益借鉴和参考。

（本文重要观点参考自黄晟同志为《网络空间安全防御与态势感知》（Cyber Defense and Situational Awareness）一书撰写的译者序，特此鸣谢！）