安天周观察

主办：安天　2017 年 4 月 10 日（总第 82 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天收到国家计算机病毒应急处理中心感谢信

近日，国家计算机病毒应急处理中心向安天发来感谢信，感谢安天在 2017 年全国两会期间的网络安全保卫工作中做出的贡献。

两会是我国政治领域中最高级别的活动，因此做好网络安全保障工作至关重要。安天在 2017 年全国两会网络安全保卫工作中，主要采用了恶意代码分析和渗透测试服务技术，辅以监测分析，高质高效的完成了国家计算机病毒应急处理中心布置的技术检测、移动恶意代码检测、情报信息分析和应急处置支持等各项工作任务，有效的保障了重点单位的网络安全。

安天是中国应急响应体系中重要的企业节点，多次在重大网络事故和网络安全事件的响应中发挥关键作用，曾参加过十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。安天会一如既往，在维护国家网络安全工作中贡献自己的一份力量。

安天为海关总署信息中心提供反 APT 解决方案

海关总署作为国内信息化部署较早的国家机关，已经实现了高度的办公自动化、无纸化。因其业务既涉及国计民生又接触海量信息的特点，很容易成为高级可持续性威胁 (APT) 重点攻击的目标。特别是近几年，手机、平板电脑等移动计算设备的引入，对其安全防护和威胁检测提出了更大的挑战。

安天针对海关总署的具体防护需求，为其提供了专用反 APT 解决方案：①实时检测网络流量，发现网络中的恶意代码和安全事件，提供准确的威胁信息；②对安全事件进行统计分析，直观展示全网安全态势；③对可疑对象进行深度动态分析，有效发现未知威胁，及时识别 APT 攻击，并提供威胁的来源、组成和特性等信息，形成详细分析报告。

依托安天提供的专用反 APT 解决方案，海关总署信息中心已经建立了针对未知威胁和 APT 攻击的监控系统。该系统能通过清晰的视图与表格来发现隐藏的 APT 攻击，并捕获攻击载荷，发现攻击目的以及追踪攻击源；提高了对威胁的检测、分析、发现能力，缩短了威胁响应时间；同时，还可以随时了解网络状况，进而及时调整相应策略，抑制威胁传播，缩小危害范围，维护网络正常运行。

■ El Machete 窃取全球政府机构数据

近日，黑客组织 El Machete 使用定制恶意软件向全球知名国际政府机构发起攻击，并通过社工方式传播蔓延。据了解，该黑客组织已窃取数据逾 100GB。

研究人员称，尽管 El Machete 锁定拉丁美洲为主要攻击目标，但加拿大、英国、德国、韩国、俄罗斯、乌克兰和美国等政府机构也纷纷受其影响。El Machete 采用的恶意软件主要依赖于 Windows API，旨在逃避传统防病毒程序的检测。在过去的几年里，El Machete 开展网络间谍活动可谓畅通无阻，尽管公开可用的防御系统中包含诸多威胁识别指标，但多数杀毒解决方案的检出率仍非常低。

El Machete 在不断加强自身网络攻防能力，而此举无疑会使相关国家受到威胁。此外，许多国家的内部网络能力尚未获得提升，仍有可能被黑客组织列为攻击目标。（来源：http://www.hackbase.com/article-217232-1.html）

安天举行勒索软件『红蓝对抗』赛

近日，安天安全研究与应急处理中心（安天 CERT）与安天产品研发部门进行了一场勒索软件“红蓝对抗”赛，这也是安天定期在公司内部举办的关于产品的攻防竞赛小游戏。

“红蓝对抗”将两个部门的人员分成红蓝两支队伍进行勒索软件对抗比赛，“安天端点研发部门”担任“蓝军”，“安天 CERT”担任“红军”。比赛双方均被要求既不能影响用户正常使用 office，又需关闭安天智甲终端防御系统的威胁病毒库，保证勒索软件可以正常被执行。比赛中，“红军”挑选了两个勒索软件样本，自行编写出一个模拟勒索软件的样本；在勒索软件被执行后，“蓝军”使用安天智甲终端防御系统，在不依赖病毒库的情况下，依然可以感知勒索行为，提示用户发现勒索软件，并及时结束软件进程，保证受保护文档未被加密，最终“蓝军”3-0 完胜。

安天智甲终端防御系统借助安天分析团队对“敲诈者”的分析和预判，依托安天反病毒引擎和主动防御内核，完善了多点布防：包括文档访问的进程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定等，经过这些功能的强化，安天智甲终端防御系统不仅能够有效检测防御目前“敲诈者”的样本和破坏机理，还对其后续可能使用的技巧进行了布防。

除了 PC 端的防护产品，安天 AVL TEAM 对 Android 平台的反勒索技术也做了很多前瞻性的研究工作，并应用于安天移动反病毒引擎中。

每周安全事件

类 型	内 容
中文标题	90% 的智能电视能被恶意电视信号远程劫持
英文标题	About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals
作者及单位	CatalinCimpanu；BleepingComputer
内容概述	近日，瑞士的安全研究员 Rafael Scheel 在某安全会议上报告了针对智能电视的新型攻击方法，这种攻击方法允许相关人员通过发送恶意的数字视频地面广播 (DVB-T) 信号来远程控制设备，获得智能电视的 root 访问权限，发动 DDoS 攻击并监视电视用户。 这种攻击具有高度的危险性，因为攻击者可以远程发动攻击，不需要电视用户的交互，便可在后台运行。因此，电视被入侵后，用户可能会毫不知情。这类攻击主要针对宽带混合型标准的电视，而现在市面出售的智能电视约 90% 都支持这一标准。Rafael Scheel 称，任何人只需花费 $50-$150 就可以设立一个定制的 DVB-T 发射机，来发送恶意的广播 (DVB-T) 信号。
链接地址	https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	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.vmall.a[prv, rmt] 2017-03-27	该应用程序运行后隐藏图标，后台接收远程控制指令，窃取用户联系人、地理位置信息等信息，会删除用户数据，建议立即卸载。（威胁等级高）
		Trojan/Android.androspy.a[prv, rmt, spy]2017-03-28	该应用程序是间谍软件，会接收远程控制指令完成隐藏图标，上传用户的短信、联系人、通话记录等隐私信息。如非自主安装建议及时卸载，以免造成隐私泄露。（威胁等级中）
		Trojan/Android.hexunxiang.a[exp]2017-03-30	该应用程序伪装成安卓服务，安装后无图标显示，后台监听指定短信，并发送短信订购付费业务。造成用户资费消耗。建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.QQspy.at[prv, exp]	该应用程序伪装成 QQ 相关应用，诱导用户输入账户和密码，并连网上传，会造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Tool/Android.SMSBomber.ab[exp]	该应用程序为短信轰炸机，供用户实施对指定目标进行短信轰炸，建议谨慎使用。（威胁等级高）
		Trojan/Android.emial.ev[prv, exp]	该应用程序运行后隐藏图标，会诱导激活设备管理器，后台监听短信，拦截短信，窃取用户信箱、通讯录等隐私信息，通过邮件上传，遍历联系人发送恶意推广短信，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.HiddenApp.z[prv, sys]	该应用程序安装后无图标显示，会私自获取设备固件信息并上传至指定网址，造成用户隐私泄露。重新挂载系统目录，将文件写入系统目录下，影响系统正常运行。另外，会与其他手机病毒协同构成威胁，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsSend.lv[exp, sms]	该应用程序会伪装成热门应用，诱骗用户发送扣费短信，造成资费损耗，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	IIS 6.0 远程代码执行漏洞 CVE-2017-7269	在 Windows Server 2003 的 IIS6.0 的 WebDAV 服务的 ScStoragePathFromUrl 函数存在缓存区溢出漏洞，攻击者通过一个以“If: <http://”开始的较长 header 头的 PROPFIND 请求执行任意代码。（威胁等级高）
	较为活跃的样本	Trojan[DDoS]/Linux.Ddostf	此威胁是一类针对 Linux 平台，具有 DDoS 功能的木马家族。该家族样本运行后会连接远程服务器，向其发送系统敏感信息。它可以接收远程服务器的命令并执行 DDoS 攻击，包括 TCP、UDP 及 HTTP 的洪水攻击。（威胁等级中）
		Trojan[Backdoor].Win32.Zebrocy	此威胁是后门类的木马家族。该家族的样本使用了伪造的图标，在执行后与远端的控制服务器进行通信接受指令。（威胁等级中）
		Trojan.Win32.PlugX	此威胁是一类可以窃取用户信息并回传的木马家族。该家族的样本在运行后会连接多个服务器回传用户信息。同时，该家族样本会在注册表中创建启动项以实现驻留。（威胁等级中）
		Trojan.Win32.WhiteAtlas	此威胁是木马类家族程序。该家族利用的 Word97~03 版本的格式溢出漏洞，在执行后释放出 PE 文件，收集与系统有关的信息并上传。（威胁等级中）

NukeBot 银行木马的源代码被公布

Chris Brook / 文　安天公益翻译小组 / 译

近日，模块化银行木马 NukeBot 的作者发布了其源代码，以期重获网络犯罪社区的信任。

NuosBot 的作者 Gosya 在几个地下论坛上发布了指向该恶意软件的 GitHub 链接，称之为“zeus 式银行木马”。IBM X-Force 研究团队的人员表示，这一举动可能是反向报复。

IBM 研究员里默尔·凯瑟姆 (LimorKessem) 和伊利亚·科尔曼诺维奇 (Ilya Kolmanovich) 表示，Gosya 在销售该木马时出现了一些失误，这可能导致他除了公布其代码之外别无选择了。

黑客的恶意软件通常由论坛管理员验证，但是 Gosya 在加入一个论坛后立即开始兜售该木马。当回答有关 NukeBot 的问题时，他也显得紧张和警惕，这引起了其他论坛成员的怀疑。据相关人员分析，也许 Gosya 是在不同的论坛上以不同的名义出售同一个恶意软件。

默尔·凯瑟姆和伊利亚·科尔曼诺维奇写道：“当欺诈者意识到同一个人正试图以不同的名义出售恶意软件时，他们更加怀疑他是一个破解者，且试图歪曲或出售着并非他所有的产品。”Gosya 甚至将 NukeBot 的名称更改为 Micro Banking Trojan，但这似乎并没什么用，而且他被各个地下论坛禁止了。

NukeBot，也被称为 Nuclear Bot，于 2016 年 12 月首次出现在地下市场。Arbor Networks 是最先分析该木马的团队之一，其研究人员声称它包含大量的命令，

具有浏览器功能以及从 C&C 服务器下载 webinject 的功能。

X-Force 的研究人员也在 12 月份分析了该木马，他们表示，该恶意软件可能会动态窃取数据的“HTTP bot”。

Arbor 认为当时无法确定该木马的活跃性和传播程度，但是可以确定的是，它的售价已经接近 2500 美元，且是同一时间流行的木马 Flokibot 价格的两倍多，这也许会吓退原来存在的潜在买家。

尽管如此，相关研究人员仍然认为 NukeBot 是合法的。

虽然 IBM 的研究人员没有提供消除该恶意软件的方法，但在近期承认它有一个基于 web 的管理面板，用来控制受感染的终端和 web 注入。Gosya 在论坛上发布了几篇帖子，声称该恶意软件 (现名为 TinyNuke) 还具有其他功能，具体如下：

——能够对 Firefox，IE 和 Chrome 浏览器进行格式化和 web 注入；

——感染 x86 和 x64 浏览器；

——逆向工程 SOCKS 4；

——具有 HNVC 式的隐藏桌面；

——具有包含模糊字符串的 32kb 二进制文件。

Gosya 试图出售该恶意软件却屡屡碰壁，这很可能致使他公布了代码。默尔·凯瑟姆认为自己的猜测比较靠谱，并说道：“Gosya 对他在地下市场的不受信感到很失望，因此决定发布该恶意软件的主要模块，以供他人测试和证明。”

现在，该恶意软件的代码已经广为人知。默尔·凯瑟姆指出，它的修改和进一步传播只是时间问题，而最可能的情况是，代码可能被重新编译，或被僵尸网络运营者使用，并嵌入到其他恶意软件代码中。虽然目前还没有出现任何攻击事件，但这一情况很快就会被改变。

默尔·凯瑟姆对《安全周报》(Threatpost) 说：“我们认为每次所发生的的代码泄漏都会导致攻击者的利用和微调，而正好这个案例也是非常相似的。”也就是说，该木马的代码泄露会导致什么样的后果，我们仍需拭目以待。

2013 年夏，Carberp 木马的源代码在网上公布。据了解，早在 2011 年 5 月，Zeus 犯罪软件套件的代码就已经被泄露了。攻击者设法修改 Zeus 的代码，添加了新的 web 注入技术、定制模块和新的 C&C 服务器通信介质：Tor。

去年，Gozi 木马和 Nymaim 木马的代码在网上泄露。犯罪分子立马将这两个木马整合到了一起，创造了 GozNym。不久之后，GozNym 木马便进行了部署，为攻击者创收了 400 万美元，其主要受害者是商业银行机构、信用社和零售银行。

原文名称	“OilRig” Attacks Expanding Across Industries，Geographies
作者简介	Chris Brook，Threatpost 的副编辑。
原文信息	2017 年 3 月 30 日发布于 Threatpost 原文地址 https://threatpost.com/nukebot-banking-trojan-source-code-leaked-online-by-author/124653/
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。

安天发布《Necurs 样本分析报告》

近日，安天安全研究与应急处理中心（安天 CERT）分析人员发现 Necurs 僵尸网络于近期恢复活跃的状态。在僵尸网络程序利用代理模式来进行 DDoS 攻击的同时，它会重新发送垃圾邮件，影响股票市场。

Necurs 僵尸网络是世界上最大的僵尸网络之一，曾因利用垃圾邮件传播 Locky 等勒索软件而引人注目。Necurs 模块化的设计模式使得它很容易产生版本迭代和功能扩展。目前，Necurs 僵尸网络程序在原本主模块、Spam 等功能模块，以及在可动态加载其他模块的 rootkit 模块的结构基础上，扩展了 SOCKS 代理和 DDoS 等功能模块。

Necurs 僵尸网络程序在感染的主机上被成功执行后，会利用漏洞升级自身，并将自身复制为 C:\Installer｛根据主机信息生成的 BotGUID｝\ syshost.exe，而后启动自身，退出父进程。此外，子进程启动后会调用 netsh.exe，将自身添加至防火墙白名单中（Windows XP 系统则会禁用防火墙）。

Necurs 僵尸网络本身具有复杂的混合命令与控制模式。它既可以与命令控制服务器进行通信，也可以利用点对点功能共享命令控制服务器的 IP 地址列表。在通信过程中，它可以尝试利用程序资源中加密过的原始 IP 地址列表来连接服务器，也可以使用多种域名生成算法来识别和连接服务器。

Necurs 僵尸网络最新的两个模块是代理模块和 DDoS 模块。其中，在代理模块中，僵尸网络程序提供两种操作模式来保证中继连接，即直接代理和回连代理；在 DDoS 模块中，虽然并未利用放大技术来增加攻击强度，但仅以其僵尸网络的规模而言，最基本的攻击技术就能产生强大的破坏力。

Necurs 僵尸网络具有程序模块化的特性，它为“如何随着时间的推移来改变作业方法”提供了范例。尽管 Necurs 主要以其垃圾邮件模块而著称，但它其实也是一个可以用于达到不同目的的多模块恶意软件。因此，在威胁演进的同时，安全厂商也要持续跟踪不断变化的威胁动态，最大程度的保障用户的安全价值。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引（NSRL）鉴定器、可交换信息（EXIF）鉴定器、数字证书鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

文件名	42d15597c83ee42ec736b80cbb9c667d5538a4b14faa1bff2e4db981ab980097
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	115 KB
MD5	FE929245EE022E3410B22456BE10C4F1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Locky.gena
判定依据	BD 静态分析

静态启发式检测

检测类型	检测点	详细说明
PE 结构	非微软的版本信息	非受信厂商的版本信息，具有较低的受信级别。
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE 结构	PE 含数字签名	通常包含数字签名的程序具有较高的受信级别。

EXIF 信息

描述	值
File Size	114 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later，and compatibles
Time Stamp	2016:02:03 14:41:55+08:00
PE Type	PE32
Linker Version	9.0
Code Size	68096
……	……

报告地址：https://antiy.pta.center/_lk/details.html?hash=FE929245EE022E3410B22456BE10C4F1