安天周观察

主办：安天　2017 年 9 月 11 日（总第 103 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

态势感知项目交流会在安天举行 刘欣然一行莅临安天调研

9 月 7 日，态势感知项目交流会在安天举行。本次交流会旨在对由国家计算机网络与信息安全管理中心牵头的国家重点研发计划“网络空间安全重点专项”2017 年度项目“基于异构多元信息的安全分析、态势感知与决策关键技术与系统项目”的目标进行凝练，为项目启动会做准备。

安天作为本项目的参与单位之一承办了此次交流会，来自国家计算机网络与信息安全管理中心的副主任刘欣然等一行领导及其他项目参与单位如哈尔滨工业大学、中国科学院大学、中国移动通信有限公司等校企单位的研究人员参与了本次会议并进行了相关的学术交流与研讨。

在态势感知方面，安天已有成熟的技术积累，安天态势感知与监控预警平台可实现对网络流量、网络边界、业务系统、主机端点相关安全，感知防护环节的汇聚、分析、协调联动及综合研判。在 2016 年，安天协助黑龙江省委网信办建设黑龙江安全态势感知和应急处置平台，平台运行至今已实现网站监测、安全信息共享、态势感知和应急处置机制等客户价值。

会议期间，与会嘉宾对安天进行了参观调研，安天技术负责人进行了讲解，向来宾介绍了安天的发展历程及现状、核心技术及分布，并展示了安天取得的各项资质和荣誉。在安天持续与网络安全威胁对抗方面，特别介绍了对高级威胁的发现、捕获、分析等方面所做的工作，重点对“白象”、“APT-TOCS”等攻击事件的概况及安天的分析进行了讲解，并解答了刘主任对于“APT-TOCS”攻击事件的相关问题。在安天的产品方面，相关负责人也进行了详细的讲解，其中主要介绍了安天对于网络靶场及态势感知的理念、认知以及技术实现。

刘主任在听取了安天负责人的介绍后表示，安天虽然作为一个民营企业，但其发展过程却体现了一个国家乃至世界网络安全形势的变化。他对安天的技术能力及取得的成果表示肯定，对安天艰苦奋斗的精神及过程表示了赞赏，同时也对安天员工的生活表示了关心。

■ MongoDB 数据库遭遇大规模勒索攻击，26000 多台服务器被劫持

近日，据外媒报道，三个黑客团伙劫持了 MongoDB 数据库超过 26000 多台服务器，其中规模最大的一组超过 22000 台。安全专家 Dylan Katz 和 Victor Gevers 最先发现这次攻击，他们认为这是“MongoDB 启示录”的延续。所谓的“MongoDB 启示录”事件始于 2016 年 12 月底，并持续到 2017 年的头几个月。据悉，有多个黑客组织参与了此次攻击，他们劫持服务器后，用勒索程序替换了其中的正常内容。外媒称，大多数被攻破的数据库都在使用测试系统，其中一部分可能包含重要生产数据。部分公司最终只得支付赎金，结果发现攻击者其实根本没有掌握他们的数据。安全专家们使用 Google Docs 电子表格追踪了本次攻击，总计超过 45,000 多个数据库被攻破。目前，除 MongoDB 以外，另外几个著名的数据库也并未幸免，ElasticSearch、Hadoop、CouchDB、Cassandra 和 MySQL 的服务器也都遭到过劫持。（来源：https://www.bleepingcomputer.com/news/security/massive-wave-of-mongodb-ransom-attacks-makes-26-000-new-victims/）

■ 黑客瞄准英国高等学院窃取军事武器研究成果与专家敏感数据

近日，据外媒报道，境外高等院校的网络安全漏洞数量在过去一年内翻了一番，因为黑客正绕过他们薄弱的防范手段窃取国家机密信息。据悉，现今黑客似乎开始瞄准英国大学，旨在窃取导弹研究成果与专家个人敏感数据。

《纽约时报》援引信息自由法案 (FOI) 收集的数据显示，黑客于 2016-2017 年在医药、工程与导弹研究方面共计开展了 1,152 起恶意攻击活动，其受影响机构除牛津大学遭到 515 次未经授权的访问攻击外，还包括伦敦学院与伦敦玛丽皇后学院被成功攻击 57 次。此外某学院还声称，每月受到的攻击多达 10,000 次，多数源自中国、俄罗斯与远东等地区。网络安全公司 Darktrace 技术总监 DavePalmer 表示，虽然伪装军用车辆的导弹与机密设备是黑客首要攻击目标之一，但他们更想得到有关军事武器与专家研究成果的详细资料。（来源：http://www.ibtimes.co.uk/cyber-criminals-target-uk-universities-steal-missile-secrets-personal-data-1637958）

每周安全事件

类 型	内 容
中文标题	SynAck 勒索软件开始活跃
英文标题	SynAck Ransomware Sees Huge Spike in Activity
作者及单位	Catalin Cimpanu；Bleeping Computer
内容概述	近日，据外媒报道，SynAck 勒索软件开始活跃。这款勒索软件最先发现于 8 月 3 日，一个月之后开始活跃。SynAck 从未达到警戒水平，但本周其活动开始激增，据报道，将近 100 人使用了他们的 ID-Ransomware 服务检测电脑，结果发现是 SynAck 病毒。相关安全人员分析了上个月的样本后，检查出三个 SynAck 版本，判断的因素是软件使用的勒索信息。勒索软件不使用暗网上的支付门户，它会让用户通过 email 联系作者或者使用 BitMessage ID 支付。专家认为 SynAck 背后的黑客组织会使用 RDP 爆破来进入远程计算机，之后人工下载安装勒索软件。受害者报告的感染环境包括 Windows Server 主机和企业网络。
链接地址	https://www.bleepingcomputer.com/news/security/synack-ransomware-sees-huge-spike-in-activity/

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 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.fgdirSpy.a [prv，exp，rmt]	该应用程序伪装成系统应用，窃取用户短信、通讯录、通话记录、相册、APP 列表、位置、Facebook、浏览器历史记录等隐私信息，后续还会接收远程指令，执行截屏、重启应用、更新 GPS 位置、拦截电话等恶意行为，造成用户隐私泄露和资费消耗，请及时卸载程序。（威胁等级高）
		Trojan/Android.Ubsod.a [exp，rmt，prv，rog]	该应用程序是非官方应用，篡改加入恶意代码，程序运行会请求激活设备管理器，后台联网上传设备固件信息获取指令参数，具有推送广告、私自下载等恶意行为，监听拦截短信并上传短信息，造成用户隐私泄露和资费消耗。（威胁等级高）
		Trojan/Android.Proqnoz.a [prv]	该应用程序伪装成开发工具，私自上传个人媒体文件到远程服务器，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.WirexDdos.a [exp]	该应用程序伪装正常应用，运行会隐藏图标，私自频繁访问指定网址发起流量攻击，造成资费损耗，影响手机安全，建议立即卸载。（威胁等级高）
		Trojan/Android.Scaces.a [sys，prv]	该应用程序内嵌恶意代码，运行诱导修改手机设置，释放恶意程序，安装到本地，应警惕该程序造成的用户隐私泄露或资费损耗。（威胁等级中）
	较为活跃的样本	Trojan/Android.LockScreen.ao [rog，lck]	该应用程序运行时会自动将手机调节至最大音量，播放色情音频文件，造成用户的尴尬和恐慌，而后置顶勒索界面，勒索用户付费解锁，建议卸载。（威胁等级中）
		Trojan/Android.Fakegoogleplay.c[exp，sys]	该应用程序伪装正常应用，运行隐藏图标，关闭 WIFI，访问重定向网页，通过加载 JS 脚本，执行 WAP 计费，造成用户资费损耗。（威胁等级高）
		Trojan/Android.LockerMaker.e[spr，exp]	该应用程序为锁屏勒索、拦截马等恶意程序的推广应用，运行诱导用户加其 QQ 付费使用，恶意制造、传播恶意程序，建议不要使用。（威胁等级高）
		Trojan/Android.Mobilespy.aj[prv]	该应用程序运行后会获取用户的短信信息及联系人信息，并将短信信息及联系人信息上传到指定网址，可能会造成用户隐私泄露，建议立即卸载。（威胁等级中）
		RiskWare/Android.fakewechat.l [exp]	该应用程序伪装成微信，会通过指定网址获取支付信息。调用 Switfpass 支付 SDK，通过微信支付、支付宝等支付方式进行支付，建议谨慎使用以免造成资费损失。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Struts2 远程代码执行漏洞 CVE-2017-9805	Struts2 REST 插件使用带有 XStream 程序的 XStream Handler 进行未经任何代码过滤的反序列化操作，这可能在反序列化 XMLpayloads 时导致远程代码执行。任意攻击者都可以构造恶意的 XML 内容提升权限。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Injector	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。（威胁等级中）
		Trojan[PSW]/Win32.Tepfer	此威胁是一种窃取账号密码的木马类程序。该家族样本运行后会盗取被感染计算机上的用户账户信息（用户名、密码等）；能通过垃圾邮件、可疑链接、恶意网站等途径传播；可以修改计算机的系统设置，更改或删除重要文件，捆绑间谍软件、恶意软件及广告件等，使系统性能下降。（威胁等级中）
		Trojan[Dropper]/Win32.Sysn	此威胁是一种带有捆绑功能的木马类程序。Sysn 家族样本感染用户系统之后，会在电脑中释放并安装其它恶意程序。部分变种还可以对电脑进行远程控制，关闭电脑中的杀毒软件。（威胁等级中）
		Trojan/Win32.VBKrypt	此威胁是一种使用 VB 语言编写的木马类程序。该家族通过恶意网页进行传播。该家族的部分变种通过冒充一些常用软件来盗取信息。（威胁等级中）

DDoS 攻击的七个趋势

Jai Vijayan / 文　安天公益翻译小组 / 译

DDoS 攻击已经不再只是少数行业的大公司需要担心的事情了，每个企业都面临这种威胁。

不要纠结于数字

DDoS 攻击的实际数量和平均规模 (带宽) 每个季度都会有很大的变化，有时甚至以月为单位发生变化。从 Akamai Technologies《2017 年第二季度互联网 / 安全状态报告》来看，经过连续三个季度的下降后，2017 年第二季度的 DDoS 攻击比上个季度增长了 28%。同时，第二季度没有看到超过 100Gbps 的 DDoS 攻击。相比之下，就在上个季度，Verisign 报道称至少有一个攻击达到了 120Gbps，平均攻击规模比上一年高 26%。

数字本身不应该决定缓解策略：了解 DDoS 攻击已成为大多数组织面临的威胁才更加重要。

多向量攻击

结合了容量、应用级和协议级元素的多向量 DDoS 攻击已成为主要威胁。攻击者可以一次使用一个向量来启动这些攻击，或者同时使用所有向量以混淆目标。

Neustar 报道称，2016 年多向量 DDoS 攻击增加了 322 %；而在 2015 年，UDP、TCP 和 ICMP 是最受欢迎的攻击向量。早在 2016 年第一季度，诸如 Akamai 的公司报告称，多向量 DDoS 攻击占其减灾工作的 60 %以上。事实上，Verisign 在今年第一季度发现的最大 DDoS 攻击是多向量攻击，峰值带宽为 120Gbps，每秒大约传输 9000 万个数据包。该攻击主要由 TCP SYN 和 TCP RST 流量洪泛攻击组成，持续了两周，并在 15 小时的时间内持续发送了 60Gbps 的流量。Whalen 说，Arbor 最新的全球基础设施安全报告指出，67%的受访者报告了多向量 DDoS 攻击，比去年高 56%。

网络层 / 容量耗尽攻击仍然是最常见的

Imperva 研究团队负责人 Avishay Zawoznik 说，网络层攻击，仍然是最常见的攻击类型。这些攻击的特点是高带宽或每秒数据包数量，以受害者网络管道的带宽容量或受害者网络设备的路由容量为目标。Zawoznik 说，容量耗尽攻击的常见例子包括 SYN、ACK、UDP 和 ICMP 洪泛攻击。

Akamai 上个季度帮助客户处理了 4051 个 DDoS 攻击，其中 99%是容量耗尽攻击。80 %以上针对游戏行业的公司。埃及 IP 地址数量最多，占全球总数的 38%。

应用级 DDoS 攻击正在增加

虽然网络层 DDoS 攻击仍然很常见，但应用级攻击正在迅速增加。应用级 DDoS 攻击使用一系列看似合法的请求来轰炸业务应用程序，直到应用程序无法响应。与容量耗尽攻击相反，应用程序攻击的流量低得多，并以每秒请求量 (RPS) 进行测量。典型的攻击针对的是 HTTP 和 DNS 服务，现在越来越多地针对 HTTPS 服务。Imperva《2017年第一季度全球威胁全景报告》显示，网络层 DDoS 攻击连续四个季度下降，而应用层攻击每周达到近 1100 次。据 Arbor 称，DNS 攻击占去年所有报告的应用层攻击的 81%，超越HTTP成为最受欢迎的攻击类型。

大多数 DDoS 攻击小而简短

事实是，绝大多数 DDoS 攻击都涉及相对较低的流量。在 2017 年第一季度 Corero Network Security 为其客户处理的 DDoS 攻击中，80 %的规模不到 1Gbps。从 2016 年第四季度到 2017 年第一季度，98%的攻击都低于 10Gbps。在 2017 年第一季度 Corero 为客户处理的 DDoS 攻击中，71%不超过 10 分钟。

小型 DDoS 攻击经常用于窃取数据并掩盖数据泄露。Corero 表示，许多情况下，威胁源使用这些攻击来映射受害者的网络，安装恶意软件，作为勒索攻击的前身。虽说小型 DDoS 攻击可能不会导致网络瘫痪，但是会导致服务质量降级和拥塞问题。

DDoS 攻击更加持久

目前有很多执行 DDoS 攻击的工具，导致威胁源能够持续攻击受害者。例如，Akamai 报告说，在 2017 年第二季度，受害者平均遭受了 32 次 DDoS 攻击。一家游戏公司每天平均遭受 6 次攻击，共遭受了 558 次攻击。Corero 表示，其客户今年第一季度每月平均遭受 124 次 DDoS 攻击，比 2016 年第四季度增加了 9%。Imperva 在报告中说：“在宏观层面上，DDoS 攻击越来越短，但也更加复杂和持久。”

IoT 和移动僵尸网络驱动的 DDoS 攻击正在崛起

近年来，存在漏洞的移动和物联网设备大量扩散，为攻击者提供了创建大规模僵尸网络来执行 DDoS 攻击的机会。Marai 是这类僵尸网络的代表，不过其它僵尸网络也在崛起。最近的例子是 WireX，该僵尸网络由受感染的 Android 设备构建，针对多个行业的目标执行应用层 DDoS 攻击。本月，多个安全厂商的研究人员对该僵尸网络进行了分析，其中最大的攻击涉及 100 个国家超过 7 万个感染节点。Corero 在其报告中指出：“大规模僵尸网络驱动的 DDoS 攻击变得越来越普遍。它们已经足够强大，能够破坏本该安全的公司网络。”

原文名称	7 Things to Know About Today's DDoS Attacks
作者简介	Jai Vijayan，一位经验丰富的技术记者，拥有超过 20 年的 IT 行业新闻经验。
原文信息	2017 年 8 月 30 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/7-things-to-know-about-todays-ddos-attacks/d/d-id/1329758?image_number=1
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《FTP 僵尸掘金网络蠕虫分析报告》

近日，安天捕风小组在安全事件整理过程中，追踪到利用 FTP 服务器进行传播挖矿的蠕虫变种。近几年全球比特币市场一路走高催生出了一大批“矿工”。与此同时，黑客使用非法的网络手段进行挖矿。

该病毒利用 FTP 服务进行传播，尝试连接控制服务器，进行虚拟货币挖掘的蠕虫僵尸网络大量入侵网络 FTP 服务器，并呈迅速爆发趋势。主机感染该病毒后将尝试连接控制服务器，接收更新、接收控制指令、下载虚拟货币挖矿程序。病毒向磁盘中大量写入名称为“photo.scr”的母体，感染本地 html、php、aspx 等网页文件（感染文件的类型：php、htm、xml、dhtm、phtm、xht、htx、mht、bml、asp、shtm），并嵌入恶意代码。用户访问被感染网页时，蠕虫会自动进行传播，并利用字典主动向网络中的匿名弱口令 FTP 服务器写入病毒文件，以此激活病毒。

激活后，病毒开始对网络中的 FTP 服务器进行爆破。一旦成功登录，恶意软件的副本被上传到每个可写服务器。此时，能够呈现给用户（例如 HTML，PHP 和 aspx 文件）的每个文件都被 photo.scr 字符串感染。若用户打开该类文件会受到感染并安装挖矿软件，目标服务器的 ip、凭据和受感染文件列表将被发送到恶意软件的后端服务器。有了这些信息，攻击者可以登录到受感染的 FTP 服务器，感染更多文件并使受害范围进一步扩大。以下为安天建议用户的解决方案和防御措施。

1. 已感染病毒时的解决方案

1) 安装杀毒软件，全盘查杀病毒。

2) 对已感染病毒的网页服务器，可使用文本批量替换工具，删除网页文件中被植入的恶意代码（有 photo.scr 特征）。

3) 网络监测病毒域名解析行为，对病毒利用域名进行解析的主机，极大可能感染该家族蠕虫病毒。可对以下几个域名进行重点关注：stafftest.ru(176.126.84.24)hrtests.ru、profetest.ru、testpsy.ru、pstests.ru、qptest.ru、jobtests.ru、iqtesti.ru、managtest.ru、testworks.ru。

2. 防御措施

1) 关闭所有 FTP 服务匿名访问，修改弱口令账号，已知该家族蠕虫使用以下字典组合攻击 FTP 服务器，可以避免使用下列账号：anonymous、Admin、admin、www-data、anonymous、administrator、ftp、user、user23；密码：test、password、pass、pass1234、1234、12345、123456、1234567、12345678、123456789、1234567890、qwerty、devry、000000、111111、123123、abc123、admin123、derok010101、windows、123qwe、email@email.com。

2) 内部网络部署蜜罐系统进行感知黑客渗透内网活动。

3) 在网络中安装安天探海流量威胁检测系统，对网络中的可疑流量进行监控，且不会影响网络的正常使用，易于管理监控。

目前该病毒样本已由安天追影威胁鉴定器检出。

蠕虫程序

安天【追影威胁分析系统】无需更新病毒库，依据行为即可实现对上述蠕虫程序进行有效检测，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、动态行为 (Windows7) 鉴定器、静态分析鉴定器、动态行为（默认环境）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蠕虫程序。

文件名	./BEF104BEAC03466E3C73761223941C65
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.53 MB
MD5	BEF104BEAC03466E3C73761223941C65
病毒类型	蠕虫程序
恶意判定 / 病毒名称	Worm/Win32.Remoh.ah
判定依据	静态分析

运行环境

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office 2007、flash、wps、FoxitReader、adobe reader

其他行为

行为描述	危险等级	行为描述	危险等级
获取系统内存	★★	获取 socket 本地名称	★
连接网络	★		

根据动态行为 (Windows7) 得出该文件具有以下行为：获取系统内存、获取 socket 本地名称、连接网络。根据动态行为（默认环境）得出该文件具有以下行为：延时、获取主机用户名称、查找浏览器进程、查找指定内核模块、获取计算机名称、获取系统版本、连接特殊 URL、获取 socket 本地名称、连接网络、独占打开文件、获取系统内存、获取驱动器类型、创建特定窗体。

运行环境

操作系统	Windows XP 5.1.2600 Service Pack 3 Build 2600
内置软件	默认、ie6、office2003、flash、wps、FoxitReader、adobe reader

危险行为

行为描述	危险等级	行为描述	危险等级
延时	★★★		

其他行为

行为描述	危险等级	行为描述	危险等级
获取主机用户名称	★	查找浏览器进程	★
查找指定内核模块	★	获取计算机名称	★
获取计算机名称	★	获取系统版本	★★
连接特殊 URL	★	获取 socket 本地名称	★
连接网络	★	独占打开文件	★
获取系统内存	★★	获取驱动器类型	★
创建特定窗体	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=BEF104BEAC03466E3C73761223941C65