网络安全

2016年总结
2017年预测

AhnLab

CONTENTS

2016年总结

- 2016年席卷全球的安全威胁TOP5

2017年预测

- 2017年网络安全所面临的威胁TOP5
- 应对2017年安全威胁专家提出的建议

AhnLab

2016年总结

2016年席卷全球的安全威胁TOP5

AhnLab

2016年席卷全球的安全威胁TOP5

01. 席卷全球的勒索软件

勒索软件(Ransomware)，已不需要在此多说明，它已成为了当今世界安全方面的主要话题，不仅是安全行业，就连普通用户也通过新闻媒体经常听到。这一年中，勒索软件的种类和数量爆发性增加，给全世界带来了巨大的损失。根据ASEC接收的举报，年初勒索软件举报数仅占总举报的15%，而到11月末竟然超过了60%，足足增加了4倍以上。

仔细观察2016年勒索软件趋势，可以看出勒索软件反复着大大小小的变化过程和消灭，结果呈现了一种进化的形式。去年，臭名昭著的TeslaCrypt在今年5月突然宣布终止。另外，通过韩国社交网站传播并给韩国用户带来较大损失的CryptXXX勒索软件在今年7月以后开始消停。相反，通过垃圾邮件传播的Locky勒索软件和通过语音提示用户的Cerber勒索软件则反复升级。今年还出现了一种打破对勒索软件的传统概念的勒索软件，不仅加密文件，还会篡改磁盘主引导区。尤其，今年还出现了一种代办勒索软件制作和传播服务的勒索软件即服务(Ransomware-as-a-Service, RssS)，有助于勒索软件的全球范围的扩散。甚至，勒索软件已开始支持各种语言。过去，大部分的勒索软件仅支持英语。但是现在，有些勒索软件如“TeslaCrypt”、“CryptXXX”、“Locky”、“Cerber”等除了英语还支持各种语言。

勒索软件的传播和感染方式也变得越来越多样化。从通过电子邮件附件、偷渡式下载(Drive-by-download)、恶意广告(Malvertising)等的传播方式到最近的结合社会工程学手法和利用RDP(Remote Desktop Protocol)的方式。

此外，教育和研究目的的开放源码EDA2和Hidden Tear等恶意利用到了勒索软件制作，甚至还出现了模仿CryptXXX、Locky、Petya等有名勒索软件的事例。从攻击者的角度来看，利用勒索软件可以在短时间获得较大的直接收入。由此可见，勒索软件的增加趋势不会消停。

2016年席卷全球的安全威胁TOP5

02. 针对性攻击 性价比高且无境界

筛选特定的目标进行攻击的针对性攻击(target attack)的投资成功率很高，所以在过去几年呈现急剧增加趋势。针对性攻击可以分为政治目的的攻击和针对一般企业的攻击。

今年2月，美国国土安全部(DHS)的人员信息被窃，此事件怀疑是俄罗斯所为。而在8月，原以为是失误导致泄漏的美国国家安全局(NSA)的黑客工具(Shadow Brokers)，后来才知道也是与国家之间的间谍战有相关。

针对个人的目标攻击大多也带有政治目的。香港、缅甸、叙利亚、阿联酋和哈萨克斯坦等国家发生了以反对执政党的政治家或社会运动家等为目标的针对性攻击。

针对一般企业的攻击主要目的是窃取客户信息，即个人信息。今年，雅虎、Dropbox等均发生了个人信息被窃事件。另外，还盛行一种被称为商务电子邮件诈骗(Business email scam)的传统电子邮件篡改事件，给欧洲和北美地区的企业带来了巨大的损失。据美国联邦调查局(FBI)的统计，电子邮件篡改受害事例仅在美国就发生了共7,000件，损失额达到740万美元。今年在韩国发生的某企业的电子邮件被黑导致损失240亿韩元(约2,057万美元)贸易货款，该事件是由沙特阿拉伯国有石油公司沙特阿美石油公司(Saudi Aramco)的电子邮件帐户被黑所致。

针对性攻击长时间地、精准地对确定的目标发起全方位的隐蔽性攻击，因此受害者需要较长的时间来认知被攻击事实。即使受到攻击大多时候只是猜想，很难确认被攻击事实，因此检测和应对都很不容易。当攻击对象为企业或者机关等组织的一员，可能会导致严重的损失，需要仔细地监控和持续关注。

2016年席卷全球的安全威胁TOP5

03. IoT恶意软件的先发制人

随着物联网，即IoT(Internet of Things)技术的发展，与物联网相关的安全威胁也持续演变。物联网设备考虑到易用性和低功耗，通常使用嵌入式Linux操作系统。对于用户终端使用的操作系统来讲，管理并非容易，尤其小规模的制造商根本就不大考虑安全而设计。物联网存在的这种缺陷，给攻击者提供了一个良好机会，他们并没有放掉这个良好的机会。

今年9月，网络犯罪研究记者布莱恩•克雷布斯的博客网站——KrebsOnSecurity.com和主机托管公司OVH遭到了分布式拒绝服务(DDoS)攻击。10月，美国最主要DNS服务商Dyn遭遇了大规模DDoS攻击，导致了Twitter、Spotify、Netflix、AirBnb、CNN、华尔街日报等数百家网站无法访问。这两起攻击都使用了物联网恶意软件 - “Mirai” 。

各种物联网设备被利用在网络攻击，一些恶意软件的源代码被公开，今年一年被发现的物联网相关的恶意软件超过1万。

最近，物联网设备制造商开始关注安全问题。但是，物联网设备一旦购买或者安装后很难持续管理。假设安装后大概使用5年左右，那么利用物联网设备的攻击事件未来几年很有可能持续发生。

2016年席卷全球的安全威胁TOP5

04. Exploit Kit: 适者生存 激烈的漏洞攻击

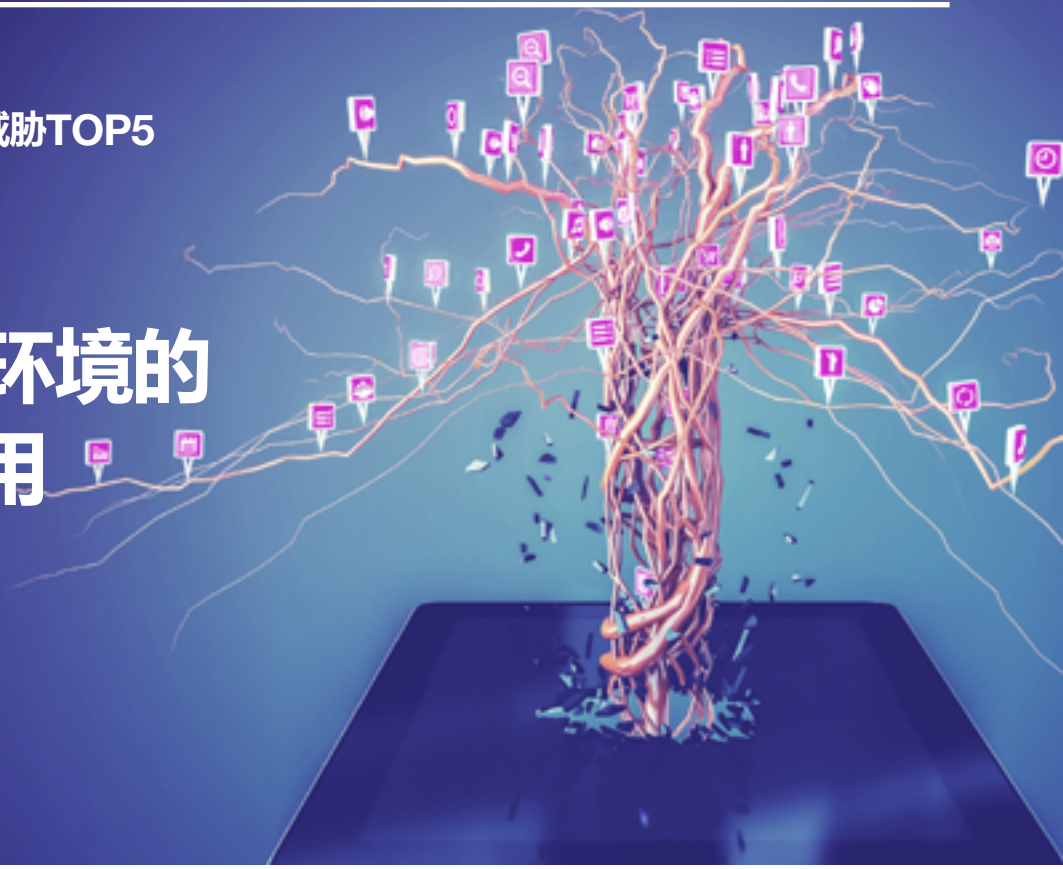
Exploit Kit(漏洞利用工具包，以下EK)是一种集合了各种漏洞利用工具，可对多种文件格式进行自动化分析、漏洞利用测试，比较有名的EK有Blackhole EK，Phoenix EK，Nuclear EK等。随着勒索软件黑市的活跃，EK更加为所欲为。今年上半年最活跃的臭名昭著的顶级EK- Angler EK和Nuclear EK突然消失后，Neutrino EK继承Angler EK继续活动，但在下半年也减少了活动。而Sundown EK和Magnitude等还持续活动。

EK的多层次的重定向(Redirection)技术主要用在通过在线广告网络和网站传播勒索软件等恶意软件的恶意广告(Malvertising)攻击。利用各种脚本形式的下载器或者EK的勒索软件传播目前仍然持续发生，还发现了多数利用Windows Powershell的恶意软件。

另外，随着EK的活跃，包括EK经常利用的互联网浏览器(Internet Explorer, IE)、Flash和Java等漏洞，各种漏洞攻击变得更加猛烈。尤其，利用文档文件相关的EPS(Encapsulated PostScript)漏洞和Opentype字体漏洞的恶意软件传播也呈现增长。利用Windows操作系统的正常功能的设计缺陷的代码注入手法的AtomBombing被证实影响所有版本的Windows操作系统。

2016年席卷全球的安全威胁TOP5

05. 已适应移动环境的Rooting应用



2016年发现了多数基于安卓(Android)系统的Rooting智能手机的恶意应用。今年7月开始到10月，AhnLab收集的Rooting恶意应用的数量比上半年增加了30%左右。

可以看出，恶意应用日益增加。恶意应用获取root权限后在用户手机执行恶意行为，如在用户未知的情况下安装应用到手机，或者避开手机安装的防病毒软件的检测，窃取个人信息或植入广告等。

上半年主要流行通过Rooting植入广告或偷偷安装应用的恶意应用，而在下半年出现了攫取金融信息为目的的Rooting应用。

恶意应用利用安卓操作系统的漏洞试图获取智能手机的root权限。上半年出现的恶意应用Godless利用多个漏洞获取安卓操作系统5.1以下版本(Lollipop)的root权限。

如上述，利用安卓操作系统的恶意应用越来越增加，Google致力于加强安卓系统的安全而多角度的努力。自2015年发现Stage fright漏洞以来，Google每月提供安卓操作系统的安全更新，同时公开各智能手机制造商的更新响应排名。今年发布的安卓操作系统7.0(Nougat)来说，当攻击者试图通过Rooting篡改系统的时候，可以使手机无法启动。问题是，根据智能手机制造商或者手机生产年度，有可能不提供安全更新。因此，使用旧版本操作系统的智能手机用户面对安全时需要格外的注意。

2017年预测

2017年网络安全所面临的威胁TOP5

应对2017年安全威胁专家提出的建议

AhnLab

2017年网络安全所面临的威胁TOP5

01.
勒索软件
将越来越肆虐

2016年，勒索软件(Ransomware)呈现快速增长趋势，带来了严重的影响。对于攻击者来说，勒索软件是一个相对容易赚钱的有效的犯罪手段。而对企业来说，他们面临着业务中断或者失去重要信息等恐惧，而不得不支付赎金。加上，出现了一种代办勒索软件制作和传播服务的勒索软件即服务(Ransomware-as-a-Service, RssS)，促使勒索软件的全球范围的扩散并形成了一个市场。

2017年，勒索软件预计更加复杂和高级，攻击范围也将继续扩大。勒索软件的目的是获取金钱利益，那么它的目标当然会指向“钱”聚集的地方。到目前为止，网络金融犯罪主要由网络钓鱼或域欺骗方式来主导，即通过假冒网站来窃取用户信息。但以后，勒索软件将上升到网络金融犯罪活动的中心。

此外，结合鱼叉式网络钓鱼的勒索软件和瞄准企业之间交易货款的犯罪组织多年来一直在活动，因此频繁发生贸易往来的企业需要格外注意。

2017年网络安全所面临的威胁TOP5

02.
攻击工具的普及和网络犯罪的高度且加速发展

仅仅几年前，网络攻击被认为是具有专门IT技术的黑客的专属物。而最近，不仅是在网络黑市，而且在一般的互联网上，即使没有具备专门的IT知识也可以利用勒索软件即服务(Ransomware-as-a-Service, RssS)制作恶意软件，并发起网络攻击。这种工具的普及导致网络犯罪的增加。同时，不能将网络罪犯限定为特定人物或组织，因此对网络犯罪的响应和调查也将变得更加困难。

攻击者将致力于当前的攻击技术的升级换代，不仅持续利用垃圾邮件附件和偷渡式下载方式的攻击，而且通过利用应用软件存在的安全漏洞的Expolit工具更积极地传播恶意软件。为了预防持续增加的Exploit漏洞攻击，需要定期检查网站的伪造和篡改与否，尤其特别要注意利用WebShell的攻击。

2017年网络安全所面临的威胁TOP5

03.
内部入侵
并试图控制系统

2010年前后发生的大多数黑客攻击企业的主要目的是窃取企业机密或企业持有的个人信息。然而，最近黑客攻击企业的目的已不仅仅是单纯的窃取信息，已发展成控制企业内部的基础设施。尤其是今年，将会出现各种攻击手段，试图入侵组织内部的基础设施。

通过这种攻击，基于受感染的系统入侵企业内部的基础设施，首先通过收集内部信息和检索获取系统帐户信息。通过反复收集和利用主要帐户来攫取内部系统的操作权限，最终掌握整个基础设施。

一旦掌握企业内部系统后，就可以伪装成该企业服务所需的正常程序，并可在各种PC上安装恶意软件。此外，还通过受感染PC连接的网络上的其他系统，试图控制另一个企业的内部系统。

2017年网络安全所面临的威胁TOP5

04.
永不停止的针对社会基础设施的攻击和网络恐怖主义

在2017年，预计全球的政治和经济利益的冲突将进一步深化。由于国家之间的理念冲突加深，针对国家机关和企业的网络恐怖主义经常发生。

在以前，黑客的攻击目标主要是许多用户使用的在线服务，而最近的攻击对象已扩大到几乎所有的公司和机关，且不管服务的类型和规模。据推测，在大规模的网络恐怖袭击，例如针对社会基础设施的攻击的背后主要是恐怖组织或敌对国家。攻击的动机大多是宗教、信念和政治冲突，而不是经济利益。尤其，当针对社会基础设施的攻击成功时，会造成社会混乱和恐怖，并可以最大限度地发挥广告效果。又由于宗教和政治纠纷不容易解决，因此预计将来针对社会基础设施的攻击持续发生。

大多数的社会基础设施的内部系统安全运营在未直接连接到外部网络的隔离环境中。然而，如果有一个系统连接到外部网络，或有一个连接外网和内网的点，就无法从安全威胁中获得自由。不管在哪里，安全最脆弱的环节是人。越是强大的安全策略，越是给用户带来不方便，可能会有不遵守安全策略的员工。攻击者将捕获这种漏洞并利用各种方法试图发起攻击。

2017年网络安全所面临的威胁TOP5

05.
物联网与物联网威胁

物联网(Internet of Things, IoT)技术的发展将进一步加快。然而，人们对物联网仍然缺乏安全意识，存在安全漏洞的产品还会持续销售。而黑客则不会放过这一点，预计物联网恶意软件也将迅速增长。

去年在美国发生了Mirai恶意软件发起的大规模的DDoS攻击。该攻击就利用了网络路由器、DVR(Digital Video Recorder)和IP摄像机等IoT设备。物联网设备特性上，一旦购买或安装，就很难进行售后管理，并且在初始状态下使用几年。就用户而言，除了应用物联网设备制造商提供的安全补丁之外，没有明确的应对方法。

近年来，物联网设备制造商开始关注安全问题。然而，由于技术缺乏或其他原因，没有具体考虑物联网设备加强安全的问题。此外，物联网设备具有低功耗和低费用的特点，实际上难以增加安全强化功能或提高价格。

为了防止迅速扩散的物联网设备的安全威胁，不仅是制造商，而且还需要网络安全提供商和政府机关的有机合作。此外，各个国家争先恐后地加快物联网技术和产品开发，仅通过个别国家的监管很难解决范围广泛的物联网安全威胁。通过各国政府和附属机构和制造商的全方位的合作，构建对物联网设备的最低限度的检查系统，并需要抓紧建立一个实用的安全强化指南。

应对2017年安全威胁专家提出的建议

2017年
不容忽视的安全威胁

在网络黑市中，恶意软件制作和分发服务-RaaS已经落地，并基于这种服务形成了新的犯罪生态系统。根据经济原理，该生态系统将产出更多样的恶意软件，并通过积极的活动扩大他们的范围。此外，基于资本主义相互竞争的市场逻辑，继续投资和努力来制作和分发具有差别的恶意软件和服务。这使得今年的安全威胁变得更加高级。

由此可以看出，企业和机关在处理安全问题的方式上也将发生变化。首先，企业需要统一安全管理平台，将当前的安全解决方案融合到一个平台，有利于统一收集信息和管理。然后，安全提供商为了有效处理收集的信息，并有效应对最新的威胁，将试图融合自动化、机器学习等技术。

应对2017年安全威胁专家提出的建议

趋势 1.
机器学习在安全领域的应用

今年将是诸如数据挖掘(Data Mining) 和机器学习(Machine learning) 等分析大数据的技术在安全领域全新落脚的一年。虽然企业引进多种安全解决方案来应对日趋复杂多端的安全威胁，但总是缺乏管理这些解决方案的人力资源。很多企业可能试图将机器学习应用在安全领域，代替人类专家解决安全问题。在传统安全系统中被忽视的一些数据，在机器学习中可能发现新的信息。通过融合诸如机器学习等新的技术，可以产出不亚于专家分析的成果，并且减少的资源将用在新的领域或事业，形成良性循环结构。

应对2017年安全威胁专家提出的建议

趋势 2.
安全领域的细分和统一管理的需要

在物联网(IoT)和云计算为代表的IT环境变化的时代，随着各种平台和服务，细分安全领域的需求将增加。通过各种研究结果和经验建立他们对最新技术的了解的公司正在应用适合各行业的技术和服务。在此过程中，理应同时考虑安全因素，并选择适合各环境的安全技术和解决方案。尤其，统一管理和监控分散在各领域的安全解决方案，并在此基础上具体实现有效应对的统一安全的需要。另外，威胁信息的可视化是必不可少的。为解决发现的问题的实际应对将成为安全的主要项目。

应对2017年安全威胁专家提出的建议

趋势 3.
攻击工具的普及

随着勒索软件即服务(RaaS)的兴起，即使没有具备专门IT技术的人也可以发起网络攻击。加上漏洞利用工具包的攻击手法也在升级，网络攻击很可能进一步发展。

随着恶意软件制作及发布服务导致网络攻击的普及，不能再将攻击者局限在特定人或特定组织。就是说，不仅在应对网络攻击，而且在调查攻击的主体时候都会面临诸多困难。因此，为了最小化安全漏洞暴露于网络攻击的范围，需要改进用户对安全补丁的重要性的认识。对于企业和机关，要强制应用员工的安全补丁，还有必要考虑建立管理方案或投资引入安全解决方案。

应对2017年安全威胁专家提出的建议

结论：
这一切都归结于“人”

最近发生的大多数黑客攻击事件通常针对组织内特定个人或团体。主要采用向特定个人或团体发送邮件并诱导执行附件的鱼叉式网络钓鱼(Spear Phishing)，或攻击特定个人利用的网站后传播恶意软件的水坑式攻击(Watering Hole)等。

值得注意的是，在一系列最近发生的黑客攻击事件中，针对性攻击也终究是从“恶意软件”的流入起源，以及没有妥善管理的PC或服务器在中间起着桥接作用。为了提前防止安全威胁的入侵，不仅需要建立不同的解决方案，还需要利用专门的服务，但更重要的是如何利用它们。急于判断引进解决方案就万无一失的安全管理员，还有很缺乏安全意识的用户，这些因素增加了安全事故的发生。归根结底，这一切的开始和结尾都会有“人”。2017年，必需做好对依然如故的安全漏洞“人”的教育和管理，还要做好对各解决方案和服务系统的检查和有效运营。从组织内部的一般用户到安全管理员、企业管理者，应持续做出努力以减少人为因素导致的安全问题。

网络安全

2016年总结
2017年预测

发行　AhnLab, Inc.
起稿　AhnLab 安全应急响应中心(ASEC) ASEC响应组
编辑　AhnLab 内容企划部门

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京）/ +86 21 6095 6780（上海） | cn.sales@ahnlab.com

AhnLab.com

AhnLab

网络安全

2016年总结
2017年预测

AhnLab