【译】Cisco年中安全报告（2017）

angel010 / 2017-11-06 17:16:00 / 浏览数 6552 技术文章 技术文章 顶(0) 踩(0)

[redacted]

投稿

直接右上角[redacted]-[redacted]-[redacted]选择[redacted]。投稿时麻烦提供下可联系到作者的IM，方便审核沟通。（如未收到回复，联系wx：50421961）

Ps: MD[redacted]Word[redacted] ([redacted]•[redacted]•[redacted])[redacted]✧

主要发现

Business email compromise (BEC)。对攻击者来说，BEC企业邮件攻击是高获利的攻击面。根据Internet Crime Complaint Center (IC3)的数据，2013年10月到2016年12月，攻击者通过BEC诈骗获利53亿美元。而勒索软件2016年只获利10亿美元。
Spyware.
作为恶意软件的一种形式，许多组织都低估或者彻底忽略了Spyware的作用。Spyware可以窃取用户个公司的信息，弱化设备的安全态势，增加恶意软件感染的概率。
Internet of things(IoT，物联网)，物联网是企业合作和改革的方向。随着物联网的发展，安全风险也随之增加：不可见性是一个问题，防卫方并不知道什么样的物联网设备连接到网络中
Cisco记录了检测所需时间（TTD, time to detect)的中位数，这个时间从研究刚开始的39小时（2015年11月）降到3.5小时（2016.11-2017.5）。
Cisco观察到2016年中起垃圾邮件的数量激增，而同时工具利用活动有明显下降。攻击者从利用工具来传播勒索软件变为通过垃圾邮件传播，垃圾邮件中有含有宏的恶意文件
Supply chain attacks供应链攻击给攻击者一种通过被黑站点传播恶意软件到组织的新方法。如软件供应商的网站被黑，攻击者利用从该站点下来软件来感染主机。
Cyber攻击的频率、复杂性和体量都急剧增长，说明黑客经济遇到了拐点。目前的攻击主题主要通过对一些列有用的和低成本的资源的快速访问来获利。
对企业安全来说，云是一个被忽略的方面。Open authentication(OAuth)风险和单个特权用户账户的管理漏洞为攻击者创造了非常容易就可以利用的安全缝隙。攻击者也可以迁移到云上来进行企业云环境的攻击。
利用工具活动急剧减少。由于企业商业模型的改变等原因，利用工具活动减少，但这种情形可能是暂时的。
未合理应用和为了合法用户访问访问而故意开放的DevOps服务给企业组织带来巨大的安全风险。
通过对Fancy Bear cyberespionage组织使用的域名进行ThreatConnect分析，发现了研究攻击者IP基础设施的意义。比如，可以将这些恶意的域名、IP地址、email地址加入黑名单。
2016年底，cisco威胁研究人员发现并报告了3个Memcached服务器远程代码执行漏洞。3个月后发现互联网上扫描的之前发现有这3个漏洞的服务器中有79%漏洞仍未修复

简介

威胁场景一直在变化，但是cisco的威胁研究和技术伙伴发现威胁的迅速发展和攻击的体量变化带来了很多问题。

新的攻击策略：Destruction of service(DeOS)

攻击者现在在寻找一种可以消除安全网（safety net）的方法，组织依靠安全网来恢复系统和数据。DeOS攻击的表现依赖于攻击者的核心动机和创造性、能力的限制。唯一确定的是新出现的物联网和存在安全漏洞的物联

重点：减少碎片化的安全工具箱

为了减缓攻击者的攻击、限制攻击时间和空间，保护者拥有他们需要的大多数解决方案。问题的关键是如何运用这些安全。碎片化的多产品安全方法阻碍了组织管理威胁的能
Data Protection Regulation）的数据保护要求带来的安全挑战。

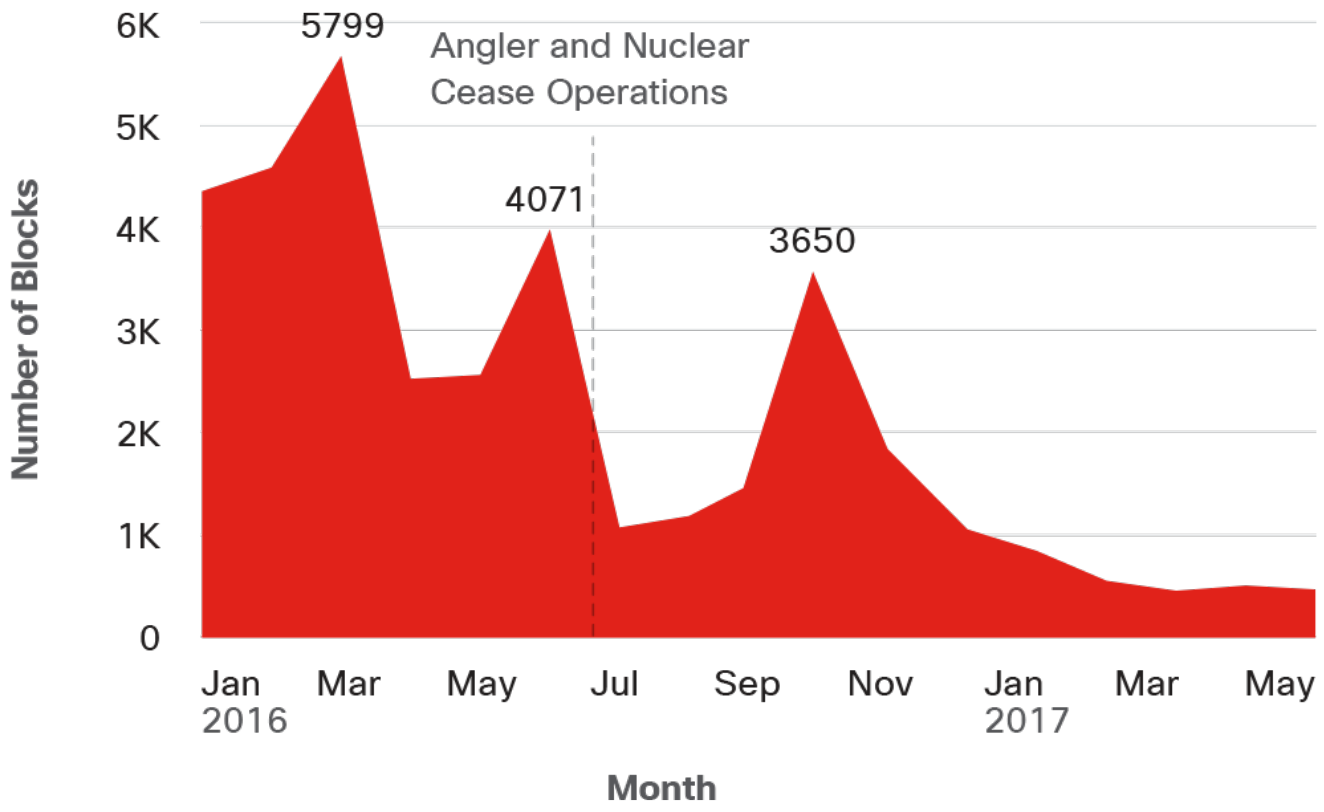
攻击行为ATTACKER BEHAVIOR

利用工具减少，但并未消失

以Neutrino为例，利用工具仍然活跃，但活跃期很短。工具的作者把它租给特定的操作者来获利。这种租借的方法导致Neutrino工具并没有那么流行，同时难以检测。
如图1所示，利用工具活动自2016年1月起急剧减少。该趋势回应了Blackhole利用工具的作者和发布者在俄罗斯被抓。当Blackhole停止操作时，对利用工具市场产生了巨大

Figure 1 Exploit kit activity

Source: Cisco Security Research



For more info visit: **cisco.com/go/mcr2017**

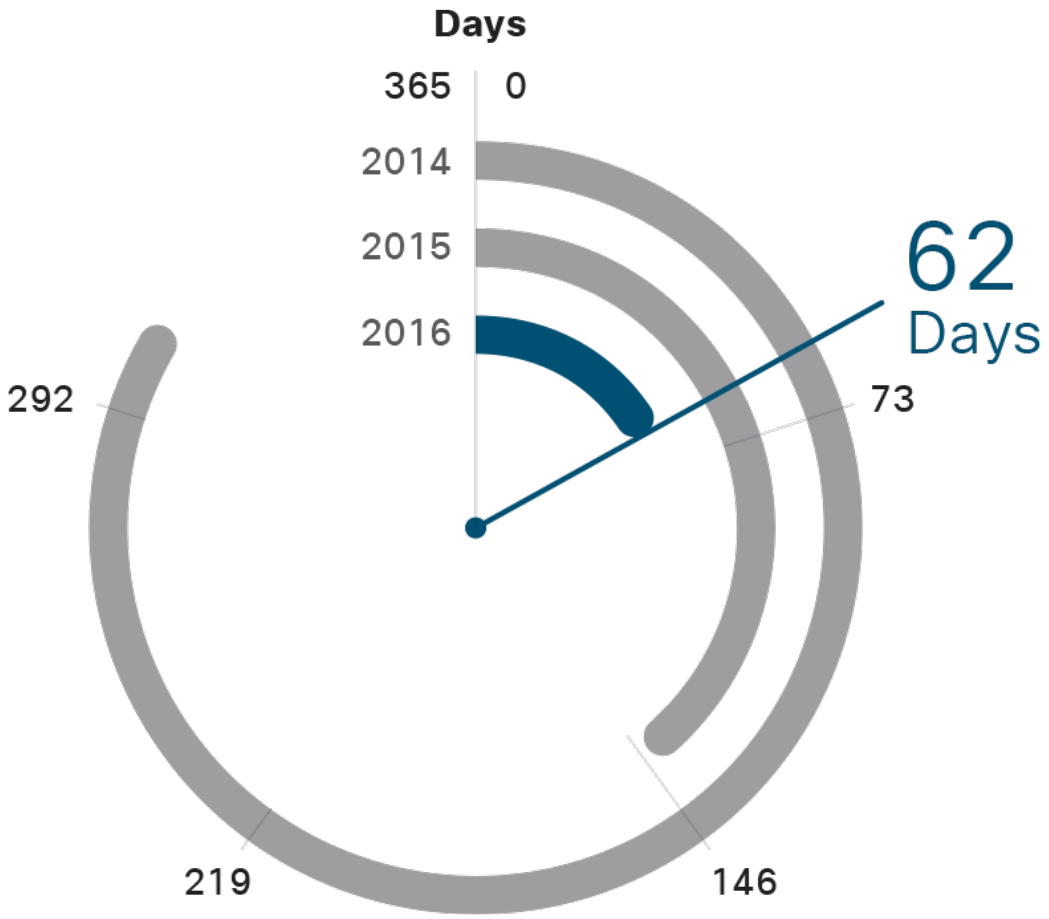
另一个趋势是网络犯罪通过邮件来传播勒索软件和其他恶意软件，这种方式和传播迅速，且性价比很高。攻击者创新地使用一些方法来避免被检测到。比如，Cisco威胁研究

防护者的行为如何改变攻击者的关注点？

对Flash的漏洞及时打补丁，可以减缓利用工具市场的速度。Flash软件一直是吸引web攻击的一部分。然而，flash攻击变得越来越难利用，一部分原因是补丁及时更新。

Figure 2 Number of days required to patch 80% of flash vulnerabilities

Source: Qualys



For more info visit: **cisco.com/go/mcr2017**

如图所示，2014年修复80%的Flash漏洞需要308天，2015年需要144天，到了2016年这个时间变为62天。
当防护者对flash软件打补丁的速度变得越来越快时，一些利用工具的作者可能会把注意力转移到利用过去已经发现但是被忽略的漏洞上去。安全团队需要花时间去评定是否

Web攻击方法说明Internet变得成熟了

代理很早就出现了，而且随着互联网的发展功能越来越成熟。防护者使用内容扫描的代理来检测网络基础设施中的潜在威胁。这些威胁包括：

- PUA，比如恶意浏览器扩展；
- 木马；
- 指向垃圾邮件和广告欺诈的链接；
- 特定的浏览器漏洞，如JS和图形渲染引擎；
- 浏览器重定向、劫持和其他将用户定向到恶意web内容的方法；

全球web拦截活动

Cisco追踪了不同国家和地区的基于恶意软件的区块活动。攻击者频繁地改变攻击的基地，寻找有弱点的基础设施。通过检查整体的流量和区域活动，Cisco的威胁研究人员
ratio值等于1表明block的数量和网络体量是成正比的。Block活动高于正常值的国家和地区的网络中含有的有漏洞的服务器和主机。图4是全球2016年11月到2017年5月的

Figure 4 Web block ratios (global)

Source: Cisco Security Research

Spyware的影响很大

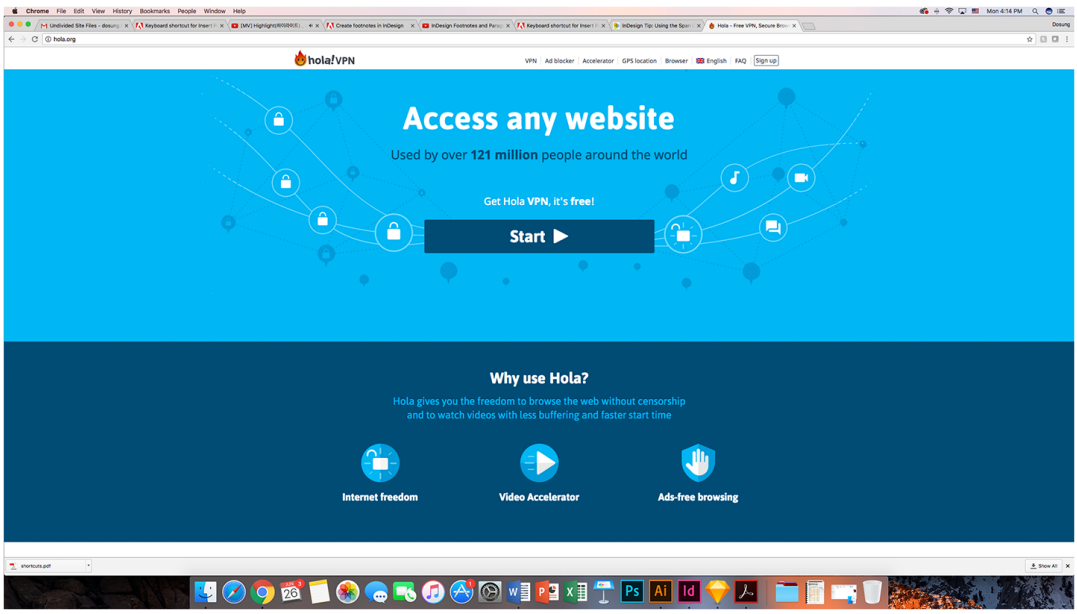
许多网上的PUA广告软件都是spyware，spyware的厂商尽可能地把软件做得看起来像合法的工具，提供给用户很多有用的服务。然而，无论怎么伪装，spyware都是恶意软
monitor系统资源监视器和木马trojans。
在企业环境下，spyware会带来一系列潜在的安全风险，比如：
窃取用户和公司的信息，包括PII个人识别信息和其他隐私、机密信息；
通过修改设备的配置、安装额外的软件、允许第三方访问来弱化设备的安全等级。一些spyware甚至允许远程代码执行，可以让攻击者完全控制设备；
增加恶意软件感染的概率。一旦用户感染了类似spyware或adware之类的PUA，他们就容易感染更多恶意软件。
为了研究spyware感染的情况，Cisco的研究人员研究了大约300家企业的网络流量（2016.11-2017.5）来找出目前企业网络中存在的spyware家族和被感染的程度。研究人
unlocker。

Hola

Hola是一款免费的web和手机端VPN应用，既是spyware又是adware。它使用点对点的缓存技术，让用户存储其他用户下载的内容。这是一款分布式的基于浏览器的客户端

Figure 6 Screenshot of Hola VPN's homepage

Source: Cisco Security Research



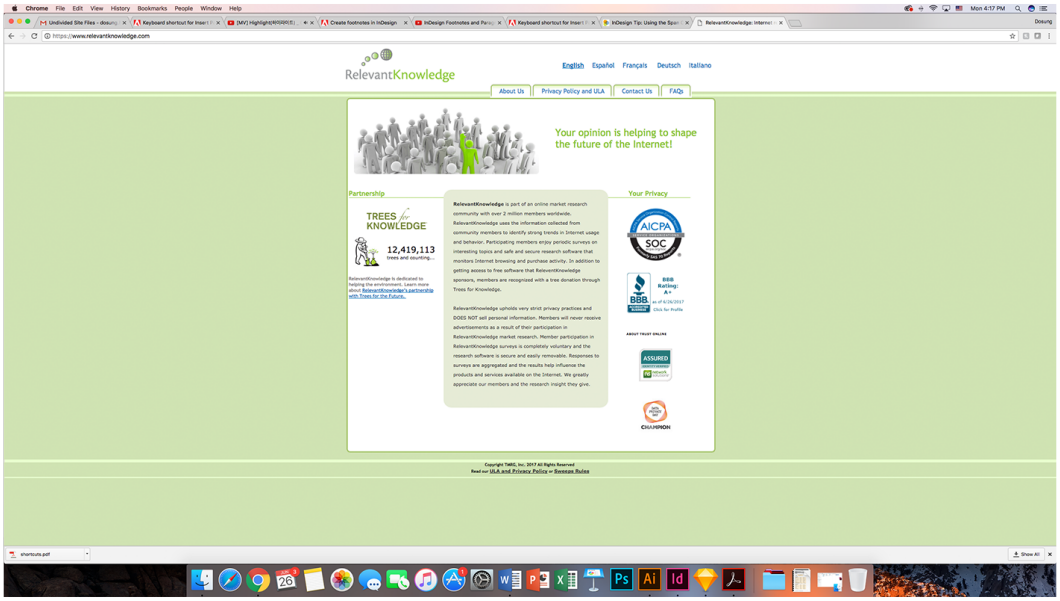
为什么说hola是spyware？Hola的一个功能就是通过Luminati服务出卖用户带宽，可以在用户系统中安装自签名的证书，下载文件时可以绕过病毒检查，远程执行代码。

RelewantKnowledge

RelewantKnowledge收集大量的用户浏览习惯、系统和配置的信息，属于spyware和系统监视器。RelewantKnowledge可以直接或间接方式安装，甚至不需要用户同意。

Figure 7 Screenshot of RelevantKnowledge's homepage

Source: Cisco Security Research



For more info visit: **cisco.com/go/mcr2017**

为什么认为是spyware？RelewantKnowledge可以未经用户同意直接安装，而且收集的信息会卖给第三方。

DNSChanger/DNS unlocker

DNSChanger/DNS unlocker是同一恶意软件的两个版本。DNSChanger是一个木马程序，能够改变甚至截至感染主机的DNS设置。DNS unlocker是一款可以不安装的广告恶意软件服务。恶意软件用自己的域名服务器替换DNS设置中的域名服务器将用户HTTP和其他请求从主机指向攻击者控制的服务器，攻击unlocker可以在受感染的主机上执行命令。

为什么认为是spyware？除了上面提到的功能，DNS Unlocker能窃取PII，重定向用户的流量，通过在特定服务注入来改变用户的内容，比如在线广告。

数据表明，在样本中这三款spyware家族中，DNS Unlocker是最流行的。DNS Unlocker的感染率占了月感染量的40%。

利用工具活动的减少好像会影响全球垃圾邮件的趋势

研究人员发现垃圾邮件的体量在不断增加，同时利用攻击的情形保持不变flux。Email是可以直接到达终端的，所以攻击者通过社会工程学钓鱼，可以轻而易举地dupe users最终搞定整个企业的网络。

恶意邮件Malicious email: A closer look at malware authors' file type strategies

更多的网络犯罪选择email作为传播勒索软件和其他恶意软件的首选，cisco的研究人员记录了恶意软件家族使用比较多的文件类型。这可以减少我们TTD所用的时间。

我们分析了2017年1月到4月的恶意软件检测来找出恶意邮件中的前20个恶意软件家族。

文件类型和恶意软件家族的关系

研究样本中前5个恶意软件家族中，每个家族都有不同的文件类型策略，比如：
- Adwind，远程访问木马RAT，最长使用的是jar文件；
- Nemucod，用来传播勒索软件的木马下载器，使用的是.zip文件；
- MyWebSearch，一款恶意广告软件，在文件选择上非常有个性，只使用.exe扩展，有时每个月只使用一个文件扩展类型；
- Fareit，另一款RAT，使用很多文件类型，但是偏爱.zip和.gz文件；

可以看出，许多恶意软件家族使用更加模糊和古老的文件类型，如.jar和.arj。

相比勒索软件，企业邮件的威胁可能更大

最近，勒索软件受到安全界越来越多的关注，相比之下，企业邮件受骇（business email compromise，BEC）带来的安全威胁可能更大。Flashpoint研究了BEC问题，发现BEC是目前最有吸引力最容易获利的黑客攻击手段。而这看似简单的攻击是依赖社会工程

一般，BEC的基础是发给财务人员的（伪造的）邮件。首先，攻击者会研究公司的架构和员工，如利用社交网络的简历来建立可能的命令传递链。这种邮件可能会来自CEO或

BEC的目标一般是大型公司，虽然大公司可能有针对金融诈骗的成熟的防御体系。但是Facebook、Google等公司都是BEC的受害者。因为BEC消息不含有恶意软件和链接，

Internet Crime Complaint Center（IC3）的数据显示，2013年10月到2016年12月BEC诈骗的金额为53亿美元，平均每年17亿。相比之下，2016年勒索软件只收到10亿美元的赎金。2013年10月到2

应对BEC诈骗需要改进企业运作流程，Flashpoint建议对用户进行培训，比如培训用户识别与普通金融转账不同的转账要求，在电汇前与其他同时确认一下细节。

恶意软件6个月的发展

趋势1：攻击者使用恶意软件分发系统，而该系统需要用户的一些正的行为才能激活威胁

越来越多的恶意邮件附件能够绕过自动恶意软件检测系统。在沙箱环境中，这些恶意附件并不会有什么恶意行为，而在用户环境下：
- 密码保护的恶意文件，密码会在邮件正文中提供给用户；
- 恶意文件弹出对话框请求用户权限（如，点击ok按钮）来执行一些操作；
- Word文档中的恶意OLE对象；
- Pdf文件中嵌入的恶意word文档；

Sender policy framework defense（SPF发送策略框架）这样的威胁检测工具能够拦截来自伪造邮箱地址发来的邮件。但是，企业并没有决定开启这项功能，因为SPF可能会拦截合法邮件除非IT管理员

像Facebook、Google这样的巨头和员工数较少的企业都是BEC诈骗的潜在目标。因为这是一种低成本、高汇报的攻击方法，这样攻击方式未来可能会持续发展。

趋势2：攻击者用勒索软件的codebase来最大化利益
使用开源的代码库，像Hidden Tear和EDA2来创建恶意软件是既快又容易，性价比也很高。Hidden Tear这样的开源代码库会公开勒索软件代码供大家学习。攻击者会修改代码然后应用到新的恶意软件中。研究人员发现最近几个月的许多新的勒索软件家族都是基于开源代码

趋势3：Ransomware-as-a-service (RaaS) 平台发展迅速
像Satan这样的RaaS平台对于想进入勒索软件市场又不想写代码或设计新的勒索技巧的人来说是非常理想的。这类平台的运营者，增长非常快，并且截取了攻击者的一部分获

趋势4：内存中的恶意软件变得越来越流行
有这样一种流行的恶意软件，他们依赖powershell或WMI在内存中运行恶意软件，而不会有任何的文件系统和注册表的修改。这让检测恶意软件变得更难，调查取证和应急

趋势5：攻击者依赖匿名和分散的基础设施来混淆C2C
研究人员发现访问恶意软件和Tor网络中的C2C服务中使用桥接服务增多。例如Tor2web，是一个允许网络上的系统访问Tor网络中的所有事物的代理服务，在这个过程中，

威胁情报：追踪攻击和漏洞

Cisco的安全团队Talos坚持进行漏洞研究和威胁趋势分析。漏洞研究尤其重要，因为他强调了攻击者和防守者之间的战斗。一般认为攻击者有优势，因为有更多的时间进行准

另一个趋势是攻击者从利用攻击发起攻击转变为利用垃圾邮件。在研究中，包含Flash和Java软件的威胁变少了，因为浏览器开发者拦截了相关的插件，因此，攻击者很难利

Time to detection检测所需时间

Cisco定义TTD为攻击产生到检测到的窗口时间。图中，TTD的中位数变大表明攻击者引入了新的微信；TTD变小，表明防守者很快找出了已知的威胁。

图20反映了2016年11月到2017年4月之间发效率最高的前20个恶意软件家族。平均TTD为3.5小时，比较老的和流行的威胁的TTD时间小于3.5小时。一些漏洞虽然是已知的

Time-to-evolve趋势：Nemucod, Ramnit, Kryptik, and Fareit

一些恶意软件家族产生大量的DGA（domain generation algorithms），用来保持恶意软件的新鲜度和攻击用户系统的有效性。一些恶意软件家族产生大量的DGA域名，这些域名与给定的域名的不同的，是一种隐藏流量和避免被

从2016年11月到2017年5月，研究人员对4大著名的恶意软件家族进行了深入分析，分别是Nemucod, Ramnit, Kryptik和Fareit。分析了传递这些恶意软件的文件类型和文件内容类型的变化，对每种恶意软件家族，检查了web和邮件传递的方法。

图21是该时间段内四大恶意软件家族进行web攻击所使用的特别的攻击向量

图22是该时间段内四大恶意软件家族进行email攻击所使用的特别的攻击向量

TTE分析：Kryptik

Kryptik恶意软件是高级银行木马的合并，该木马的源码是开放的。TTE研究中，大约1/3的Kryptik恶意软件的web事件包括JavaScript，约25%的使用.php扩展。包含MIME
图23的数据表明，恶意软件很难被检测到。到2017年4月底，Kryptik RAT TTD的中位数大约是平均TTD的2倍。

TTE 分析：Nemucod

Nemucod仍是2017年最常见的恶意软件家族，下载器被用来分发恶意软件和其他威胁，比如后门木马等。Nemucod使用了超过15种文件扩展和文件内容类型的组合，见图
hash比较多，这表明安全社区在成功检测到了Nemucod的新实例，所以恶意软件作者开始使用之前成功使用过的older hash。

DGA域名的活动期expanding 和overlap

The expanding life spans—and overlap—of DGA domains
许多恶意软件家族依赖DGA来快速产生伪随机的域名来对抗检测。DGA域名活动期比较短，但有时候也可以持续几个月。Anomali公司记录了一些与恶意软件家族相关的DG

出现这种情况的原因可能是攻击者为了尽快进化恶意软件来避免被拦截。恶意软件作者需要赶在进入拦截黑名单之前开发出新变种。恶意软件背后生存DGA域名的算法在创建

通过分析基础设施来了解统计工具

在分析的过程中，找出了潜在的恶意域名，IP地址，帮助防守方在攻击方侵入网络钱采取行动。域名和IP地址是与鱼叉式钓鱼攻击相关的。通过研究相关的域名，安全专家可

根据ThreatConnect的分析，该过程的步骤如下：
□Bellingcat提供了来自于俄罗斯政府资助的黑客的鱼叉攻击的邮件头消息，ThreatConnect使用之前的Fancy Bear行为来判断Fancy
Bear主导了对Bellingcat的攻击。
□ThreatConnect用WHOIS注册信息找出鱼叉攻击消息的域名的注册时间和注册域名的email地址。
□用被动DNS可以找出注册域名所用的IP地址。这就找出了与攻击者相关的IP地址。
□再次使用被动DNS，研究人员找出了哪些IP地址与域名之间的关系，来排除多域名的IP地址。
□用WHOIS和被动DNS，ThreatConnect找出了可能的攻击者的IP地址的子集，缩小了可能被用于APT攻击的IP地址的范围。
□从IP地址的子集中，ThreatConnect用被动DNS找出同一时间同一IP地址的不同域名。
□ThreatConnect还找出了注册原始域名的同一email地址注册的其他域名。当一个email地址注册了APT活动相关的域名时，其他用该email注册的域名也可能被用于APT攻
□ThreatConnect用新发现的域名来进行随后的迭代分析。
□ThreatConnect使用被动DNS来找出已知域名的子域名。这些信息可以帮助找出系统IP地址上的邮件服务器和其他子域名。

图28中使用的分析方法可以帮助找出与攻击活动和潜在的攻击活动相关的指数级的邮件地址，IP地址和域名。

图29 ATP组织使用的基础设施之间的关联

供应链攻击：一个被攻击的单元会影响整个企业网络

攻击者也想让攻击的操作变得更高效。RSA发现，供应链攻击对网络犯罪的攻击者来说，可以付出较小的努力得到最大的攻击效果。RSA检测到有攻击者向企业系统管理员常

被攻击的软件可以在厂商的网站上下载，导致的结果就是，利用一个被攻击的单元——厂商的网站，通过软件和自动更新，能够把威胁传播到更多的企业网络中。RSA通过对

RSA发现软件的下载页和升级页都被黑了。这就意味着之前下载了被黑版本软件的公司如果选择了自动更新，那么仍然处于威胁中。虽然网站被黑的时间只持续了2周，但是

如果企业想要拦截供应链威胁，检测过程很难。终端安全可能是最好的防护，实时监控可以帮助检测可疑的活动。

攻击者需要提供一个被黑的单元，然后就可以感染许多目标。这些攻击是静默的，给攻击者足够的时间来隐藏。

指向学术网络的基础设施Infrastructure harvesting targets academic networks

在Kingslayer的例子中，攻击者的方法包括隐藏在合法的硬件中，给软件使用者一种他们提供的产品很干净的印象。在Schoolbell僵尸网络的例子中，攻击者使用基础设施作
harvesting”。在这种攻击中，攻击者会尝试控制企业的基础设施，然后利用这些设施去进行大规模的利用活动。

因为该僵尸网络的目标是学术网络，因此Schoolbell僵尸网络是这种对抗策略的一个例子。在schoolbell僵尸网络的活动高峰，RSA发现被感染的僵尸网络个数大约有2000个
harvesting方法给了这些组织一个警告，那就是他们不是网络攻击的目标，因为他们没有有价值的数据。在网络安全方面，学术组织可能采用的方法比同样大小的其他行业组

IoT僵尸网络：僵尸网络在增长，而且僵尸网络已经有了

2016年的一种攻击趋势是将互联的设备变成僵尸网络，9月开始各种TB级的攻击纷纷出现。10月的DynDNS攻击导致上百个主流网站中断服务，是最严重的IoT
DDoS攻击。这些攻击正式把我们带入1TBps DDoS攻击时代。Radware分析了三大僵尸网络的活动，分别是Mirai，BrickerBot，和Hajime。

Mirai僵尸网络是DynDNS攻击的元凶，感染了成千上万的IoT设备，然后用这些设备发起大体量的DDoS攻击。研究人员估计有上百万被感染的IoT设备参与了这些攻击。

工作原理：
1、Mirai使用BusyBox软件和60多个设备厂商的默认用户名密码暴力攻击Telnet服务器来连接到受害设备。
2、每个受感染的设备都不会再加入其他的僵尸网络。
3、Mirai发送受害设备的IP和证书到集中的ScanListen服务。
4、新加入的受害设备会帮助感染新的僵尸，是一种自复制的模式。

BrickerBot

Permanent denial of service
(PDoS)攻击是一种快速转移的僵尸攻击，用来破坏硬件设备使其不能正常工作。这种形式的网络攻击现在越来越流行了。PDoS攻击带来的危害特别大，会严重破坏系统以至

BrickerBot可以：
黑掉设备。使用跟Mirai一样的暴力Telnet方法来黑掉设备。
破坏设备。一旦成功访问设备，BrickBot执行一系列的linux命令来破坏存储。然后执行命令来破坏网络连接、设备性能、擦除设备上的所有文件。

图33 BrickerBot 执行的命令顺序

Hajime

安全情报研究人员通过严密监控发现Hajime非常有意思。因为虽然感染了成千上万的设备，但是并没有采取进一步的行动。Hajime的运营者声明说自己是白帽黑客。

工作原理：Hajime是一个灵活的、精心设计的IoT僵尸网络，可以成员僵尸进行自我更新和功能扩展。Hajime通过扫描互联网TCP23和TCP5358开放端口发现和感染新的受

安全研究人员发现Hajime会清除感染了Mirai的设备，而BrickerBot会破坏感染了Mirai或Hajime的设备。

Ransom denial of service (RDoS)

2016年，约49%的公司收到至少一次网络勒索事件，其中39%是勒索软件，17%是勒索DoS。图35是2016年不同国家网络勒索攻击的分布。

Radware声称，Armada
Collective对大多数RDoS攻击负责。勒索数额一般为10到200比特币（大约3600到70000美元）。当支付时间到了以后，攻击者会以超过100Gbps的速度带走目标的数据中
Collective的名字。使用的技巧有假的勒索信，希望以低成本来获取高收益。下面是一些检测虚假勒索信的技巧：

- 勒索要求。一般Armada Collective要求的赎金是20比特币，其他的组织勒索的数额也在20比特币上下。所以，比较低的勒索数额可能就是假的。
- 检查网络。真正的攻击者会在发送勒索信息前进行一波小的攻击。如果网络没有任何异常，勒索信和威胁可能就是假的。
- 寻找组织结构的漏洞。真正的攻击者是非常有组织的，假的黑客一般不会链接到一个网站，也不会有官方帐号。
- 考虑其他的攻击。真正的攻击者可能同时的目标是很多公司，确认其他行业组织是否收到类似的勒索。
  ### 恶意攻击经济学的变化
  网络攻击的频率、复杂性、体量在过去的几年里都急剧上升，这表明黑客经济已经到了拐点。Radware说目前的黑客社区从以下几方面得利。
- 对一系列的有用且低成本的资源的快速访问；
- 有价值的目标把越来越多的有价值的信息放到网络上；
- 随着互联网的发展，影子经济的成熟提供给恶意攻击者效率、安全和匿名性。

  ## 勒索医疗设备的情况出现了
  为了在互联的世界中变得更加高效，许多医疗设备也必须与IT和操作技术结合在一起。然而，设备和系统中已知的安全漏洞随着互操作的增多，将原本互相隔离的系统（
  device hijack。

医疗设备攻击的影响是很大的，因为一般中小型的医院有大概12000到15000台设备，其中10-12%是连接网络的。跟许多的物联网设备一样，医疗设备设计之处并没有考虑

许多的网络犯罪都想黑掉医疗设备，因为攻击者知道对一些救命的医疗设备发起的勒索行动收益一定是巨大的。许多攻击者可能不止于此，他们可以控制植入式医疗设备，可

另一个MEDJACK事件是关于MRI系统被黑。同样利用的是xp系统的漏洞，攻击者在系统中找到了患者的数据，然后意识到可以进一步控制医院的PACS系统。取证分析发现

TrapX研究人员建议企业和其他组织采取下面的步骤来减少对医疗设备和其他重要的OT技术的勒索攻击的可能性和影响：

- 了解连接网络的医疗资产的种类和数量；
- 与供应商保持联系、确保他们履行了合同中的软件、设备和系统的更新和替换工作；
- 与高层讨论这些问题，让他们意识到安全的重要性和所面临的安全威胁；
- 用工具进行网络和自动化威胁检测和补救。

漏洞

地缘更新：WannaCry攻击

在5月中旬大规模的WannaCry勒索软件攻击之前，全球关于网络空间安全的讨论急剧上升，而且收到的威胁会越来越严重。Cisco从最近的全球攻击中发现了3个重要的问题

- 1、政府应该向厂商及时报告软件漏洞，包括POC；
- 2、技术开发人员应该公开获取、处理和公布漏洞、补丁、解决方案和相关工作信息的机制；
- 3、企业领导应该把网络安全放在最重要的位置上。

漏洞升级：密钥泄露之后的攻击事件增多

之前的Cisco安全报告讨论的漏洞的泄露近几个月还存在，比如OpenSSL。研究发现了与密钥泄露相关的漏洞活动：Shadow
Brockers组织公布的漏洞利用影响Windows系统，Operation Cloud Hopper运动包含针对管理服务提供商的钓鱼攻击，WikiLeaks Vault
7发布的美国情报文档描述了流行软件方案和操作系统如何被黑。漏洞可以在大众没有意识到的情况下存在和被利用。发布的漏洞允许更多的人去利用它，也给了防守者机会

图39中的Office漏洞发布后被就Dridex僵尸网络利用了，Apache Struct2漏洞也很快被利用了。

客户端漏洞增长趋势

2016年的Cisco半年安全报告提到服务端的漏洞正逐渐增长，攻击者利用服务端的软件漏洞来获取整个企业网络的访问权。2017年的前几个月，服务端的漏洞比2016年同期

利用工具活动明显减少

利用漏洞的工具利用活动明显减少，整体的利用工具活动也减少了。软件厂商尤其是web浏览器拦截了常用的威胁来源，如Adobe
Flash和Java；攻击者开始使用简单的攻击策略，如勒索软件，DDoS，BEC等。

漏洞种类：缓冲区错误居首

在Common Weakness Enumeration (CWE)
威胁种类中，缓冲区错误仍然是网络犯罪分子最常用的漏洞利用。这是软件开发者经常犯的编码错误。为了预防该错误，开发者应该确保缓冲区的限制确保不被利用。

不要让DevOps技术暴露企业

2017年1月，攻击者开始加密公开的MongoDB实例并勒索赎金来换取解密密钥和软件。攻击者随后把目标扩大到其他的数据库，如CouchDB和Elasticsearch。由于没有进行

CouchDB

调查中，75%的CouchDB服务器是open的，即连接到互联网且不需要验证。只有不到25%的服务器需要验证。2-3%的服务器好像被勒索了。约2%左右的CouchDB服务器

Elasticsearch

同样的，75%的Elasticsearch服务器是open的，而20%左右的服务器好像被勒索了。好消息是含有PII信息的服务器比例比较低。

MongoDB

虽然1月的勒索攻击是针对MongoDB服务器的，使用MongoDB服务器的个人和企业组织需要增强他们的安全实践。几乎100%的MongoDB是open的，好消息是这些服务

图46是Rapid7在研究中发现的MongoDB服务器的数量库大小分布图。大多数数据库表的数量小于10，应该是实验用的服务器。大于20个表的服务器应该是真正的生产系统

Docker

Docker是一种业务流程框架，其运营者对安全相当重视。然而，仍然有超过1000个Docker实例是open的。大多数发现的Docker实例分布在美国和中国。大多数的Docker

Rapid7发现，199个open
Docker实例中，至少3个活动容器在运行（图49）。企业组织使用这些不安全的生产系统是冒着极大风险的。攻击者可以创建互联网到任一个系统的shell连接，并控制他们

使用这些DevOps技术的公共互联网实例的组织需要按照下面的步骤来确保不处于威胁中。安全团队应该：

- 开发安全应用DevOps技术的严格标准；
- 维护公司拥有的公共基础设施的活性；
- 保持DevOps技术的更新和补丁分发；
- 执行漏洞扫描操作。

企业组织对已知Memcached服务器漏洞更新的速度不够快

攻击者在寻找暴露在互联网上的不安全的数据库，他们可以进行攻击、数据窃取、勒索等操作。自1月的MongoDB数据库勒索攻击之后，勒索攻击变得越来越流行了。企业

影子经济中攻击互联网上的数据库和其他设施的趋势让补丁分发变得更加急迫。及时加入了认证，DevOps服务仍然存在风险。

只有约22%的服务器开启了认证，事实上所有需要认证的服务器也有被攻击的风险。我们研究中取样的服务器分部在全球，主要是在美国和中国。

黑客利用云技术Malicious hackers head to the cloud to shorten the path to top targets

云是黑客攻击的边界，黑客也在尝试对云进行攻击。因为云系统对许多企业组织来说是具有重要意义的。黑客意识到可以破坏云系统来渗透连接的系统。2016年底，Cisco发

OAuth带来的风险

在Cisco2017 Annual Cybersecurity
Report中，研究人员揭示了第三方云应用引入企业带来的风险。一旦通过OAuth认证，这些应用接触公司的基础设施，与企业云和SaaS平台自由通信。如图52所示，
每个企业组织的云应用的数量自2014年依赖急剧增长。每个企业平均有超过1000个独立的应用和超过20000次的安装。

最近针对Gmail用户和尝试滥用OAuth基础设施的钓鱼攻击强调了OAuth的安全风险。攻击者尝试控制用户的email账户，并在通讯录中传播钓鱼蠕虫。Google报告称约0.1

云是一个被忽视的角落：单个特权云用户风险巨大

迄今为止，一些大的破坏最初都是某个单独的特权用户账户被黑或误用。黑客一旦获取了特权账户权限，就有了进入网络内部的钥匙，可以进一步窃取数据并造成更大的伤害

研究发现，82%的特权用户每个月只从1-2个IP地址登录。对其他非正常模型的活动应该进行调查。60%的特权用户从来没有登出操作，这让未授权的用户更容易访问。用户

云安全的共享责任

公司在扩展云应用时，需要了解确保云安全中的角色。云服务提供商负责所出售技术的物理、法律、操作和基础设施的安全。企业负责底层云服务的使用安全。在共享的环境

未管理的基础设施和终端使企业处于威胁中

现在的动态网络通过引入新的安全威胁、减少可见性来增大攻击面。云和影子IT设备、应用是造成该问题的罪魁祸首。网络和网络时代的终端、资产管理方案能够创建未知的

为了获得可见性，组织需要访问实时的、内容推动的安全情报。没有可以实时监控和泄露检测的安全方案，攻击者能够成功地访问网络且不被检测到。组织还应该检查他们的

防守者的安全挑战和机会

安全能力基准研究Security Capabilities Benchmark Study: Focus on verticals

虽然每个行业所面临的安全挑战不同，每个行业的安全成熟度也不同，但是也有一些共同的考虑。每个行业的安全专家都意识到不断成熟的威胁，而且需要比攻击者提前一步

以前，这些技术和相应的团队是分开工作的，OT职员管理机器和工厂，IT管理企业商业应用。如今，许多OT传感器和系统已经归属商业端。随着互联的系统来到OT的世界，

公司规模与安全方法Company size affects approach to security

攻击者破坏网络、窃取信息，与大企业相比，中小型企业（small and medium-sized
businesses，SMBs）抵御这些风险的能力有限。如果公共破坏伤害了一个品牌，引起客户转向他的竞争者，此时，大公司可以更好地预测这种影响。SMB应该确保有减少威

因为预算和支出比较少，SMB一定程度上不太会有重要的安全防御措施，比如34%的SMB使用邮件安全工具，而45%的大公司使用邮件安全工具。

与小公司相比，大公司更可能有正规的书面的安全策略（66% vs 59%），而且会要求厂商有ISO 27018认证（36% vs 30%）。

寻求安全改善的SMB可以关注安全策略和步骤，采纳常用的威胁防御来减少攻击带来的负面影响。与外部安全服务协同可以企业带来有效的正规的安全策略来开发最佳实践。

用服务来弥补知识和人才缺口Using services to bridge knowledge and talent gaps

在安全部门内部，关于哪种防御方法更优的讨论一直有，最佳的解决方案还是集成的架构。安全团队面临的另一个影响安全抉择的挑战就是：缺少安全专家。随着威胁持续升
Capability Benchmark
Study研究发现在许多行业中，人才缺乏是采纳高级安全流程和技术的主要障碍。事实上，人才缺乏是一个全球问题。外部的服务可以弥补这种人才上的缺口。除了人才，安

Alert
fatigue是内部安全团队一直遇到的问题，许多安全人员看到的警告远超过自己所能进行调查的数量，这就会导致一些潜在的严重安全威胁未被修复。当有一些低级的警告时
fatigue的原因有很多，比如孤立的系统可能会产生重复的警告，团队可能不能区分不同优先级的警告或假阳性的警告。可能是因为缺乏审计这样的安全工具，这就是外部的

外购服务和威胁警告数据

在检查不同国家对外购服务的使用时，一些特定国家的SMB表明有很大可能性使用了外购服务而不是企业自己的服务。比如，在澳大利亚，65%的SMB使用外购的应急响应

在对告警和修复的研究中发现，印度、巴西、和美国的SMB占的比例比较高，而在告警修复方面，中国、俄罗斯、英国的比例比较高。

IoT安全威胁

Cisco认为IoT有三部分组成，分别是IT（Information technology）、OT（operational technology）和CT（consumer
technology）。工业物联网（IIoT）是指连接的设备在工业控制网络中，这是相对企业IT网络和数据中心的一个概念。IoT在企业合作和革新上有很大发展空间，同样企业和

不可见性是一个问题，大多数的防护者并没有意识到IoT设备是联网的。IoT设备包括从摄像头到温度感应器等等，而这些设备并没有考虑太多的安全性。许多设备的安全性还

- 很少或者没有CVE报告和更新；
- 在特定的架构上运行；
- 有一些没有打补丁或者过期的应用是有漏洞的，比如Windows XP；
- 很少打补丁。

虽然IOT设备不能很容易地访问，甚至拥有者也不能，当系统被黑后，几乎不可能修复。这些设备可以作为攻击者的基础。IOT设备的一个安全问题是防护者可能不能理解来

黑掉大规模的物联网设备可能会严重影响商业、政府甚至网络的运行。利用IOT设备发起的DDOS攻击已经产生了，IOT僵尸网络也逐渐增多，说明攻击者已经盯上IOT了。

为了应对IOT的安全挑战，攻击面正在快速增长，而且变得更加难以监控和管理。防护者需要：

- 保持以前签名的活性；
- 对IOT设备进行IPS防护；
- 严密监控网络流量；
- 追踪IOT设备如何接触网络并与其他设备互联；

- □及时打补丁；
- □与有产品安全基线和发布安全建议的厂商一起协作；

安全能力基准研究：特定行业Security Capabilities Benchmark Study: Focus on select verticals

Service providers服务提供商

Key industry concerns主要的行业考虑

服务提供市场是一个不同的行业，包括通信、云和web基础设施、媒体、提供SaaS模型应用的商业等。除了这些以外，服务提供商出售管理安全服务：调查中71%的服务提

服务提供商的规模创造新的挑战

在每个行业，安全厂商和攻击的增值是个问题，因为解决方案是不集成的，也不提供供应商面对的威胁的执行层面的视觉。在服务提供商来看，这个问题因为市场规模的问

Breaches can increase customer churn破坏可以增加销量

因为破坏，57%的服务提供商说他们解决过公共监督的问题。在遭受破坏的企业中，约一半说破坏帮助他们改善安全状况。服务提供商的安全专家看起来能很快从破坏中学习

High adoption of standards标准采用量高

服务提供商在使用标准方面高于其他行业，这可能是他们管理商业范围能力的体现。约2/3的服务提供商说他们有正规的安全战略和标准的信息安全策略实践。除了这些，基

Public sector公共部门

Key industry concerns主要的行业考虑

因为不同的限制，公共组织对安全威胁的反应不是很积极。有限的预算，很难吸引人才，缺乏对威胁的可见性都影响着公共组织应对网络攻击的能力。但是，公共部门由于规
Information Security Management
Act）来保护重要信息系统的机密性和完整性。在州和本地也有同样的安全要求。公共部门组织也在努力管理云迁徙的过程，这也是规定所要求的。在联邦级，Federal
Risk and Authorization Management Program (FedRAMP)提供了使用云产品和服务的标准，州政府和本地争睹也需要存储政府数据的云提供商有相关认证。

管理云上数据

对公共部门组织来说，迁徙到云的过程有很多的好处也有很多的挑战，都需要持续的防护。1/3的公共部门组织说目标攻击、APT攻击、内部渗露是高级的安全威胁。除了这

预算、人才缺乏影响威胁分析

预算、人才和监管的限制影响公共部门达到安全目标的方式。比如，组织在采用某些特定工具时会比较慢，因为需要有相关知识的员工来实施和分析结果。只有30%的公共部

为了检查大量的告警信息，Cisco的安全研究专家说道公共部门组织可能需要大量的安全员工，但是却没有相应的人员编制。55%的公共部门组织的安全员工数量小于30人，

破坏推动安全改善

公共部门中缺乏人力和安全工具对攻击破坏有一定的影响。53%的公共部门组织说过去他们处理过由于数据泄露引起的公共监督。我们应当假设攻击和破坏会发生在每个企业

公共部门组织表示当破坏发生时，安全团队会从这些经验中学习：46%的受访者说破坏推动安全在一定范围内有了改善。然而，组织需要在技术上进行投资来走在安全破坏的

外购可以增加价值，但是不会增加企业实力

外购是公共部门获得更多的资源的一个重要策略。超过40%的受访者说他们在全部或部分外购像监控、审计这样的服务。在这些外购服务的组织中，大约一半引用洞察力、

渗透和其他审计服务应该有外部组织来完成，但是有全部依赖外包服务的趋势，也就是说随着时间的推移，公共服务组织将不依赖自己的专家。公司内部的知识对于复杂攻击

Retail零售业

主要的行业考虑

当零售业遇上安全破坏，这个消息会变得备受瞩目。因为对零售业的攻击会暴露客户经济数据和其他个人信息，攻击收到了媒体的注意并且需要扩大对客户的服务范围。不像

对安全的看法可能是过度自信的标志

零售商一定程度上会认为他们的安全保护比较充分，认为与媒体每天报道的数据泄露数量不符。比如，61%的零售商安全专家完全同意他们保持了全部的PCI规范，63%的零

有目标的攻击和内部泄露是最大的忧虑

持续关注收入减少和品牌声誉破坏的问题，零售商的安全专家说有目标的攻击（38%）和内部泄露（32%）对组织来说是最主要的安全威胁（图64）。来源于内部的攻击逐

解决员工缺少的问题

零售商在建立自己的安全资源时，在人力和工具方面会觉得手头拮据。24%的零售商安全专家说缺乏有经验的安全人员是应用高级安全过程和技术的主要障碍。由于缺乏安全

当人员成为问题时，自动化的安全解决方案就变得更重要了。自动化可以帮助弥补人员缺乏所带来的问题，比如安全解决方案考虑了根据隔离的位置对受感染的设备自动分类

物理位置和数据在地理分布上是分散的，所以安全团队必须假设这些位置都遵守了安全最佳实践。没有与远程位置进行持续通信，商店运行的安全方案可能没有打补丁并且过

公共破坏后零售业的收入和品牌声誉受到影响

零售业意识到安全破坏对商业有实际的影响。去年，零售安全专家说运营、财务和品牌剩余是安全破坏带来负面影响最大的几个领域。54%说他们处理过数据泄露带来的公共

制造业Manufacturing

主要的行业考虑
80%的美国工厂办厂时间超过20年了，他们会逐渐增加对是否有升级的防护措施的考虑。随着制造商向过期的机器添加了联网的设备，安全专家认为攻击者可能会找到利用这

对简化的系统的需求

在升级和结合制造系统时，制造商需要把安全方案分解复杂的小问题。46%的制造商安全专家说他们有6个以上的安全服务厂商，20%说有超过10个的安全服务厂商。当问到

大量的产品和厂商的制造设置给安全专家一个很困惑的画面。其中的复杂性说明需要IT和OT团队一起来缩小对安全威胁的集中范围，比如使用那些可以解决最急迫安全威胁的

整合IT和IT团队的专家意见

安全团队的组合可能在保护制造业的资产上存在阻碍。随着有专门制造系统知识的专家的退休，这些专门的制造系统并不会被取代，这会造成具有专业知识的人才流失。将近

避免破坏可以改善竞争的状态
对于企业中使用的老旧系统，制造商意识到出于安全原因和提高自己的竞争优势，需要改善和升级系统。根据Global Center for Digital Business
Transformation的报告，40%的制造商在未来5年内受到市场破坏的影响，一部分原因是他们没有赶上高级竞争者的步伐。安全在竞争优势上占主要地位，因为安全可以帮助

根据Cisco的调查报告，公共安全破坏会对制造业品牌带来负面影响，40%的制造业企业说过去发生过数据泄露引起的公共监督，28%说去年他们由于攻击遭受过损失。然而

公用事业Utilities

主要的行业忧虑
2016年俄罗斯黑客攻击乌克兰电厂事件强调了公用事业在保护重要基础设施所面临的挑战。公用事业不在闭环监控和数据采集网络中运行，同样的远程监控和控制发电厂、

关于信息物理融合的安全考虑已经扩展到了供应链。Federal Energy Regulatory Commission (FERC)最近指导North American Energy Reliability Corporation
(NERC)开发了重要基础设施保护的新标准，尤其是公共事业供应链方面。这些标准是为了解决工业控制系统中与主要电子系统操作相关的工业控制系统软件、硬件、计算和网

目标攻击和APT是主要忧虑
目标攻击是公用事业和能源安全专家的主要忧虑。安全专家说目标攻击（42%）和APT攻击（40%）是他们企业组织所面临的最主要的安全威胁。手机服务、用户行为习惯、

他们网络的复杂性等于说公用事业和能源企业组织必须评定这些威胁告警消息的影响，并决定哪些值得修复。将近一般的公用事业和能源安全专家说，每天会有上千个告警消

严格的预算控制会影响对外购的影响
因为监管严格，公用事业和能源企业组织不能增加在安全方面的预算。增加资金需要各方的同意，这个过程耗时巨大。根据报告，这可能可以解释对外购安全的依赖。超过6
27001和NIST 800-53的标准化信息安全策略实践。

公共破坏会推动安全改善
当公共事业遭遇公共破坏，公众会认识到公用事业是重要基础设施的一部分，这种破坏和泄露会让重要服务处于威胁中。61%的公用事业组织报告说因为数据泄露，他们解决

攻击模拟和演习是常见的事

公用事业安全专家表明他们进行常规的模拟和演习来检测安全基础设施中的弱点。92%的安全专家说他们进行半年或年度的模拟来检测应急响应方案。在执行演习时，84%的

医疗行业Healthcare

主要的行业考虑

在医疗行业，关于安全的大多数决策是病人的安全推动的，而不是监管的需求和公司资产的保护。医疗组织的领导害怕针对记录关键任务的设备和危害病人生命安全的攻击。

目标攻击是医疗安全团队的担忧

勒索攻击已经对医疗组织带来了伤害。因为网络犯罪分子指导医疗服务提供者需要保护尽一切可能保护病人的安全，医疗行业成为越多网络犯罪的目标。在Cisco的研究中，

然而威胁总是比员工能够解决的要多，在很多行业都是如此。超过40%的医疗组织说他们每天会遇到上千个安全告警消息，然而只能调查其中的50%（图71）。在医疗安全团

根据Cisco安全专家的说法，被调查的告警消息远小于医疗安全团队负责人设想的，比如事实上只将威胁拦截在网络之外，leader会认为威胁已经解决了。这些组织只能够解

管理的挑战：缺乏有经验的员工和安全解决方案的复杂性
许多医疗组织用一系列复杂的安全方案来应对安全挑战。60%的医疗组织说他们从6个以上的厂商的解决方案，29%的说使用10个以上厂商的解决方案。2/3的安全专家说他

首席信息安全官（CISOs）和安全运维经理在安全工具上会有不同的看法。没有在安全管理的一线工作可能对网络中使用的工具没有很深入的理解。在管理安全方案的复杂网

流量分片的意义The value of segmenting traffic
允许特定的系统和设备使用不同的安全协议是医疗行业中额外的需求，这些需求也是关于病人安全的考虑。医疗设备是很贵的，而且会保存很多年，所以他们的软件和操作系

运输业Transportation

重要的行业考虑

传统的运输业技术基础设施是基于封闭的专有系统。而运输业正在转向连接的网络，但是安全专家担心这个过渡的过程中会遭受攻击。但是因为增长的维护费用和现有系统的

APT和互联设备是主要威胁
随着运输组织建立了复杂和互联的基础设施，并且看到增长的网络面带来的影响，不同的威胁就出来了。超过1/3的运输安全专家说APT威胁和BYOD、智能设备的使用是组

为了满足信息访问的需求，运输业安全团队认为数据必须放在网络的边界，而且应该可以实时访问。控制对数据的访问和确保只对需要的人开放是安全实践者的关键考虑。他

缺乏安全人才可能会导致外购
有经验的安全人员可以帮助运输业应对安全挑战，但是这些组织是否能够吸引合适的人才是一个问题。超过一般的运输业安全从业人员说他们的专职安全人员小于30人。他们

随着安全运营能力变得更加复杂和有针对性，运输业组织吸引人才的可能性降低了。运输业当局需要能够招募、弥补和保留保护重要国家和本地基础设施所需要的高质量人才

标准化的信息安全实践，比如ISO 27001和NIST
800-53，可以帮助运输业组织遵循已经建立的安全基准。54%的运输业安全专家采用标准化的信息安全策略实践，2/3有正规的书面的安全策略（图73）。运输业组织已经

模拟攻击可以带来安全改善
与其他严格监管的行业类似，运输业是重要的基础设施，所以安全性至关重要。有80%的组织至少每季度进行一次模拟攻击。几乎一半的组织说模拟攻击的结果可以推动安全

金融业Finance

主要的行业考虑
金融业服务组织是网络犯罪的目标之一。客户金融数据和对账户用户名、密码的访问的价值，吸引网络犯罪分子对金融服务商业发起一系列的攻击。事实上，一些恶意软件

安全团队也面临把现有应用和新技术融合的艰巨任务，同时要确保没有安全问题出现。金融科技公司是金融服务企业组织的合作商，他们发现供给面在扩大，而且变得更加复

金融业服务组织必须确保他们是符合监管要求和安全的。在许多严格监管的行业中，有一个趋势是任务满足监管要求就解决了所有安全问题。像网络分片这样的合规需求确实

多厂商的环境增加了迷惑、不确定
金融业服务组织在多厂商环境下是正常的。57%的金融业服务组织说他们使用6个以上厂商的产品，29%的金融业服务组织说他们使用超过10个厂商的产品（图74）。2/3的

Cisco的安全专家说在金融业，一个组织使用30个厂商的产品也是很常见的。为了快速和有效地响应新出现的威胁，这些组织应该关注与简化他们的安全架构：即用更少的工

太多的告警消息回归到来自多个厂商的产品没有集成的问题。应急相应团队可能不知道哪些告警是重复的，也不知道哪些告警的优先级低。产品不集成会限制安全团队关联和

数字业务可能推动改善
随着金融服务组织持续与金融科技公司合作，他们会开发新的战略来改善安全状况，比如对数据安全提出责任划分。近一半的金融服务组织说数字业务在很大程度上影响安全
IT）都很大程度上影响安全（图75）。

标准的应用应该加速
如果金融服务组织在数字世界中安全地满足了客户需求，他们需要加速新策略和过程的应用。到目前为止，63%的金融组织有书面的正规安全战略。48%的组织应用了像ISO
270001和NIST 8000-53这样的标准化的信息安全策略实践。金融业服务属于保守行业，安全和IT
leader在考虑新标准和与目前安全战略的适配型上往往很慢。另一个金融业服务组织可以改善的方面是：要求厂商坚持建立的商业最佳实践。比如，37%的组织说他们与有IS
27001认证的厂商合作。

Cisco安全专家认为，一个组织的安全成熟度可能决定了对厂商要求的严格度：与小公司相比，大规模的金融业服务组织可能会更严格的审核供应商。

结论

Cisco发布年度安全报告和半年安全报告的目的是告知他们支持的安全团队和企业已知的和正在出现的威胁和漏洞，告知他们如何让组织更加安全。内容的多样性反映了目前
这也说明了组织把网络安全作为优先战略的重要性。他们必须在安全工具上大量投资，这些安全工具应该能够帮助安全团队管理告警消息、对动态网络进行管理和获取可见性

安全主管：安全越来越重要了

Cisco的Security Capabilities Benchmark
Study发现安全在许多组织内的优先级都比较高。安全专家也相信执行团队会把安全放在重要组织目标计划中。但是，2016年强烈同意行政领导考虑较高的安全的优先级的安

根据National Association of Corporate Directors(NACD)的2016–2017 Public Company Governance
Survey，1/4的董事会成员不满意管理团队关于网络安全的报告。报告中他们获取的信息没有考虑有效的基准，对问题不透明，很难理解。在同样的报告中，只有14%的被访

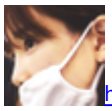
- 坚持以一种对商业有意义和可操作的方式提供信息。关于组织的网络安全威胁和安全需求报告不应该太偏技术。尝试排列关于公司面临的传统威胁问题的讨论，并与商业
- 在向管理层和董事会警告网络安全的重要性时，解释每个明确的安全条目对组织带来的影响，安全团队采取的调查威胁的措施，以及恢复正常操作需要的时间。
- 寻找企业组织中包括非技术部门主管在内的其他主管的加入。通过与组织内首席信息官、首席技术官、首席审计执行官、首席风险官等主管的协作，首席信息安全官可以
- 首席信息安全官经常尝试为安全主动权提供安全资金。但是他们可能没有意识到现在可能是与管理层讨论预算问题的最理想的时间。Society for Information Management (SIM)的2017 IT趋势研究报告说，网络安全是组织投资的第三大领域，而在2013年，排名还是14。

SIM调查的调查参与者认为在IT领域内应该增加投资的排名中，网络安全排第二，而且是第一次出现在最令人担心的信息科技列表中。

点击收藏 | 0 关注 | 0

上一篇：社区MD编辑器功能简介 下一篇：Node.js + Postgre...

1. 4 条回复


hades 2017-11-06 17:27:32

@angel010 非常感谢！！！这多文字翻译下来真是辛苦 (□•□□•□)□□

1 回复Ta


wefgod 2017-11-21 16:41:08

这是翻译过来的？真给力，有耐心啊……

0 回复Ta


hades 2017-11-21 17:11:42

@wefgod 对 欢迎一起参与社区共建

0 回复Ta


三十九度风 2018-01-19 11:35:12

看到加精华就来，赞

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板