【解读】NTT Security 2017 威胁情报报告

elknot / 2017-11-03 15:48:00 / 浏览数 5207 技术文章 技术文章 顶(0) 踩(0)

上一篇：【译】WordPress WPDB... 下一篇：利用BDF向DLL文件植入后门

1. 1 条追加内容

追加 于 2017年11月3日 16:33

作者：elknot@360corpsec && Muras4ki

0x00 前言

这些天笔者在查找有关威胁情报类的资料时候偶然间发现了2017年NTT Security发布的年报，由于当时在各大主流安全媒体上并没有看到这份，其实这份报告在我看来确实对安全行业的发展有一定的参考作用，于是笔者利用闲暇时间把这份

0x01 有关于数字的部分

除开目录，NTT Security这份报告首先上来先说明了几个关键的指标性质的数据，通过了解我们看到了以下的内容：

从对用户的影响来看：

- 73% 的恶意软件中招都是因为钓鱼性质的攻击引起的
- 30% 的网络攻击基本上都是瞄准了用户技术层面的安全隐患，比如说Java、Flash、IE这些
- 攻击者瞄准的最多的软件是微软的Silverlight、IE和Adobe的Flash
- 只有13%的攻击套件能够被检测到
- 针对勒索软件而言，最容易缴纳赎金的几个群体是：商业或者专业服务（28%）、政府相关部门（19%），医疗与健康行业（15%）和销售类行业（15%），加起来
- 三大受网络攻击影响的行业中，金融类行业被打的最惨，不过有数据显示下一个高危行业是制造业（这里的数据来源于NTT的Six Regions的划分方式）
- 53%的钓鱼攻击都来源于EMEA区域（EMEA区域指的是欧洲、中东和非洲，也就是Europe、Middle East和Africa的缩写），这里面有38%都是荷兰的IP而且这些荷兰的IP大多都在干侦查的活（这点跟笔者观察的基本一致）

- EMEA区域中，有54%的目标都瞄准了三个受影响最大的行业，其中瞄准制造业的攻击有17%，销售类行业的占17%、金融类行业的占20%
- 通过NTT Security的蜜罐数据，了解到了33%的账户能够被25个常用密码破解
- 超过76%的登录尝试都是由类似于Mirai的IoT僵尸网络发起的
- 美洲用户的P2P流量占了整个大网P2P流量的，比如说BitTorrent这种
- 超过60%的应急响应工作都跟钓鱼网站有关系
- 跟勒索赎金有关系的占了应急响应工作的大部分，约为22%
- 50%的勒索事件都瞄准了医疗与卫生行业

从一般的影响来看：

- 从全球来看，DDoS攻击栈全球网络攻击份额的6%以下，其中16%的DDoS攻击都是亚洲发起的，其次澳大利亚发起的站23%（澳大利亚似乎对IT设施的管制不严格）
- 45%的暴力破解攻击都是EMEA打到EMEA（自己打自己玩）
- 通过NTT的数据来看，更多的暴力破解攻击来自于EMEA（45%）、美帝（20%）和亚洲某国（7%）
- 美洲区域占有攻击源的54%，紧接着是亚洲某国（17%）
- 在美洲区域，有58%的目标都瞄准了三个受影响最大的行业，其中瞄准制造业的攻击有23%，教育行业的占20%、金融类行业的占15%
- 在亚洲区域，有78%的目标都瞄准了两个受影响最大的行业，其中瞄准制造业的攻击有32%、金融类行业的占46%
- 在澳大利亚区域，有81%的目标都瞄准了三个受影响最大的行业，其中瞄准销售行业的攻击有27%、金融类行业的占34%、商业和专业服务行业的占20%
- 在岛国，有83%的目标都瞄准了三个受影响最大的行业，其中瞄准媒体行业的攻击有26%、制造业的占41%、金融类行业的占16%
- 所有应急响应类的工作中有59%在四个行业 –
  医疗与卫生行业（17%），保险及金融类行业（16%），商业和专业服务行业（14%）和零售类行业（12%）。
- 全球32%的企业与组织都有正式的应急响应预案。 相比前几年平均增长了23%。

从对技术的影响来看：

- 瞄准EMEA区域的攻击中，top3的攻击里面有26%来自于美帝、11%来自于雄鸡国、10%来自于腐国

- EMEA区域中检测到的恶意软件基本上（67%）都是某种形式的木马
- 在美洲区域，检测恶意软件是最常用来被安全厂商认定为遭受攻击的方式，这一比例占到了15%
- 亚洲地区同时是最大的恶意软件的受害地区（12%）也是制造地区（29%）
- 被Mirai感染的地址大多数（60%）都来自于亚洲（可能是用户习惯不好）
- 在澳大利亚区域中检测到的恶意软件基本上（93%）都是某种形式的木马
- 在澳大利亚，有70%的应用程序都被RCE过
- 在澳大利亚，50%的攻击目标都是bash
- 岛国是僵尸网络活动中最大的单一来源，占所有此类活动的近48%。
- 在岛国检测到的恶意软件有44%是某种形式的间谍软件或密钥记录器。
- 由恶意软件引起的案例占日本信息安全重大事件的82%
- 金融类行业56%需要应急响应的事件都与恶意软件有关系

其实看完了这一部分，我自己认为NTT的数据来源还是很可靠的，由于笔者本人研究的是针对金融行业的网络攻击，从笔者自己监测到的数据来看，绝大多数和NTT的数
根据笔者自己的安全数据来看，金融类行业、能源类行业、通信与信息化行业和制造业这四大行业在我国吸引攻击的能力还是蛮强的，攻击的类型绝大多数还是以Struts

0x02 聚焦各个大区的安全问题：

NTT划分的区域的方法和我们通常认识的不同，在这份报告中，NTT把全球主要的市场划分成为了EMEA（非+欧+中东）、Americas（美洲区）、Asia（亚洲区）、Au

（1）EMEA大区：

EMEA大区问题主要来自于文件共享（45%）、网站安全（32%）和远程管理（17%），最大的安全问题来自于木马后门（67%）和蠕虫病毒（15%）

通过数据来看，53%的钓鱼类型邮件都是从EMEA区域发起的（毕竟地大物博），其中38%的钓鱼类攻击都是从荷兰发起的（。。。。。）

从被攻击的角度来看，美帝对EMEA大区输出了26%的攻击向量，紧接着是雄鸡国，输出了11%，腐国势力也不小，输出了10%，这就是攻击输出的top3。下图中深绿色

首先先来看看钓鱼，针对钓鱼而言，我们能够发现一些问题，攻击者想对目标实施钓鱼攻击肯定伴随一些原因，会造成下面的后果：

- 用恶意软件去感染目标雇员的电脑

- 通过社会工程学手段来获取一个或者多个目标雇员的信息

- 通过其他手段获取目标雇员的用户名和密码，尤其是域账户的

- 说服员工使用电汇方式转账给攻击者（不知道为什么要用电汇，在天朝的话支付宝或者微信更方便点）

NTT的数据表明差不多有73%的恶意软件被投放到不同的企业或组织中，这些组织遭受着大量的潜在威胁。也正因如此，NTT北美区域的CEO兼总裁说道：

> Enterprise clients face a wide array of threats. While advanced malware may be a significant issue, attackers do not limit themselves, and complex security breaches and intellectual property theft from organized groups and potential state sponsored attacks require more advanced strategies.

翻译成人话就是：企业客户面临的威胁比我们想象的要多很多，而且攻击者并不会因为企业有这么多安全问题就会手下留情，有国家政府和财团支持的攻击者并不会限制

NTT还说了，在2016年第二季度，针对政府的APT攻击占了整个面向政府攻击流量的90%，其中一大部分都是APT28针对美国和其他国家的政府机构以及NATO进行的大
除了政府行业，医疗行业也是受灾严重，不过受灾最严重的还是勒索，并且很多医疗机构都还支付了赎金（中了勒索一定不要支付赎金）。
在此笔者想插一句，医疗行业干安全的，可以说是none，之前我朋友的女朋友在一家私营医院工作的时候由于那家医院的数据库服务崩溃了导致整个医院的业务陷入瘫痪
通过对EMEA区域受影响行业的调查发现，钓鱼和勒索是两大重要的手段。首先先来说钓鱼，EMEA区域有29%的钓鱼攻击向量是瞄准制造业的，15%是瞄准金融类行业的

其实针对这个问题，笔者认为钓鱼所瞄准的客户一般都是所谓的大客户，要么有权要么有钱。由于EMEA区域内各个国家和地区发展水平不一样，尤其是非洲这种拖后腿的
截下来说说勒索的问题，对于勒索而言，最倒霉的是商业与专业服务，差不多比例占了28%，紧接着是政府，19%，然后还是医疗健康行业15%，具体比例如下图所示。

实际上从WannaCry（这份报告出来的时候WannaCry似乎还没爆发）事件上就能看出，首先爆发的点基本上都是在政府、医疗（没记错的话腐国因为WannaCry医院已经
其实对于勒索而言，重要数据时常备份是一个比较好的方案，但是就是这样，NTT还指出了赎金收入在$50,000这个级别上。
其实网络钓鱼攻击本质上是一种社会工程攻击的形式。 攻击者利用人性来操纵人们做攻击者想要的事情。
最复杂的社会工程攻击可能之前进行广泛的研究，以便攻击者可以作为具有授权访问敏感设施的雇员，承包商或供应商。
这可能听起来像电影里的情节，但它确实发生了。
至于勒索软件，一般勒索软件通常通过网络钓鱼或其他形式的社会工程学手段去引导用户安装到自己的计算机。用户可能被欺骗下载和执行流氓应用程序，或者用户的计
NTT还很贴心的给出了个人、管理、技术人员如何防止勒索和钓鱼攻击的方法和手段。

针对个人用户而言：

- a) 在点击链接或附件之前，请检查电子邮件，文本和其他消息以获取任何有关网络钓鱼的迹象。
  只要有可能，直接访问该网站（通过输入网址或使用书签网址），而不是点击链接。
  对于附件，请避免打开它们，直到我们可以验证它们合法。最好联系发件人询问是否通过电子邮件发送附件没有任何错误。

- b) 如果我们收到以任何方式看起来不寻常的请求，请在遵循说明之前验证其合法性。
  例如，如果有人说他们正在从服务台呼叫，他们需要我们的密码来解决问题，请获取他们的姓名，并告诉他们我们将在组织的主要帮助台电话号码中将其回复。

- c) 不要透露我们的任何真实信息。 例如，如果有人打电话声称来自我们的信用卡公司，请不要给他们我们的信用卡号码。

- d) 不要下载并安装新的软件到公司的桌面或笔记本电脑，除非有特别的授权。

针对安全管理而言：

- a)
  需要为所有用户定期进行安全意识培训，以便他们能够加快网络钓鱼，社交工程和ransomware的速度，特别是如何识别攻击，如果需要帮助，该怎么办，以及如何报

- b) 加强组织的业务连续性能力，以帮助确保在发生赎金事件时快速恢复操作。
  这包括全面的备份策略，包括安全存储脱机备份，以及确认组织重建系统和恢复数据的能力。

- c)
  以网络钓鱼攻击模拟的形式安排和执行定期评估，模拟现实世界的威胁。这是确定我们的培训和意识计划是否有效并允许进一步丰富防御能力的机会的好方法。

- d) 制定处理勒索病毒事件的对策。决定在哪些情况下授权赎金，如果有的话。

针对技术人员而言：

- a) 使用反网络钓鱼和反恶意软件技术来停止钓鱼邮件，链接到钓鱼网站，勒索病毒文件和其他网络钓鱼攻击组件到达用户。
  这些技术应该始终保持最新。 应设置在最终用户设备上安装的任何反网络钓鱼或反恶意软件技术，以便用户无法侦察或禁用。

- b)
  确保在预定频率下进行有效的数据备份。这包括监控备份系统和软件的状态，并定期测试恢复功能。数据备份需要很好的保护，特别是如果它们保持联机，那么它们就

- c) 确保系统可以快速重建。例如，我们可以保留用于构建新系统的标准镜像或安全基准。 如果是这样，这些系统镜像和安全基线应该始终保持最新。

- d) 通过为用户提供尽可能少的特权（特别是限制对管理员权限的访问）以及保持系统完全修补来最大限度地减少要安装的勒索病毒的机会。
  使用软件配置设置来防止安装勒索病毒，并尽可能减少勒索病毒安装的影响。

- e) 按照文件共享的服务器和其他系统上的文件访问权限最低的原则。这减少了这些系统上勒索病毒加密的影响。

- f) 尽可能限制管理员级别的权限。要求用户仅在必要时才使用管理员帐户，并为所有其他任务使用常规用户帐户。
  这样可以减少攻击者通过单次攻击立即获得管理员权限的机会。

- g) 如果可行，请在服务器，台式机和笔记本电脑上使用应用程序白名单，以便无法运行勒索病毒和其他未经授权的可执行文件。

- h) 使用防火墙，路由器和其他网络安全设备实现和实施网络隔离。 这意味着限制具有不同安全配置文件的网段之间的网络流量流。

（2） Americas大区（这里指的是北美+南美）

美洲区的攻击流量就有点意思了，首先美洲受影响最大的三个行业是制造业、教育行业和金融类行业，分别占比23%、20%和15%。

美洲地区发起攻击的国家最多的是美帝（63%）、枫叶国（1%）和桑巴国（1%），美帝一家独大很明显，干活的人多而且基础设施多，难免被人利用或者打别人。

美洲地区恶意软件的类型占份额最多的是蠕虫类病毒（50%），其次是间谍软件和键盘记录器（26%），紧接着就是木马和后门（17%）。

实际上，NTT在这份报告中也指出了某些国家确实在近一段时间增加了网络安全方面的投入，同时这些国家也输出了很多的攻击向量。同时NTT还预测了未来一段时间内
在报告中，NTT指出了BEC（Business Email
Compromised）攻击已经成为了美洲第二大企业安全威胁。NTT详细的举了一个BEC攻击的例子：想象一下，当我们收到类似于以下的电子邮件时，我们正坐在办公桌前
他需要你去照顾好今天的事情。 这是我们经常执行的任务，所以当我们收到他的信息时，确保在一小时内完成。
不幸的是，这封电子邮件不是真的来自你的CEO。 这是来自一个冒充你的CEO的攻击者欺骗你做攻击者想要的 - 在这个例子中，大量的钱转给了攻击者。
这种攻击被称为商业电子邮件折衷（BEC）或CEO欺诈。例如下图就是一种BEC攻击的邮件

NTT指出：BEC攻击是一种针对组织内的特定人员进行网络钓鱼的形式
。BEC攻击的最常见形式是攻击者冒充组织执行，指示授权的员工，如会计或财务上的特定人员，执行电子攻击者所拥有的帐户的电汇。NTT
Security还观察到攻击者通向hr发送电子邮件，以获得员工的扣税情况。BEC攻击的目标是窃取资金，通过直接或间接从组织获取资源或者盗窃员工的个人信息。
笔者觉得，所谓的BEC攻击本质上还是一种钓鱼攻击，但是由于攻击的高指向性（你的BOSS给你发了封邮件，由于劳动关系这一层的压力导致。。。你懂得）导致了BEC
话说回来，其实BEC的攻击防御成本还是蛮高的，NTT的数据表明：防御一次勒索攻击的成本是$700，但是防御一次BEC攻击的成本是$67,000，价格差了将近100倍。N
该信息已经在组织外部路由，并且免费提供给攻击者使用来进行身份盗用。 攻击者也可以选择出售个人信息。
这些信息中的一些可能在地下有多年的价值，所以身份盗用可能会在BEC攻击之后很长时间发生。更糟糕的是，如果BEC攻击成功，组织没有迅速解决问题，攻击者可能会
的妥协，严重损害了组织的财务状况和声誉。最终BEC攻击的风险很低，攻击者的回报也很高。攻击者可以以相对较少的收益获得数百万被盗的资金。
每个迹象表明，攻击者将越来越多地使用BEC攻击从任何类型的组织窃取现金。

BEC实际上是存在一个Kill-Chain的。

<h6>BEC攻击的Kill-Chain实际上是这个样子的：</h6>

- 攻击者对目标进行了完整的侦查活动，确定目标可以进行BEC攻击
- 攻击者通过域名注册平台注册了一个和目标所使用域名相似的域名
- 攻击者通过注册的域名搭建一个伪造的邮件系统
- 攻击者通过伪造的邮件系统发送鱼叉邮件给目标的雇员
- 目标雇员收到并对邮件进行了操作
- 攻击者确认目标雇员已经与其建立了信任
- 攻击者对目标发起了电汇转账请求，完成BEC攻击

从上面这个Kill-Chain也能看到了，BEC攻击完成的条件是：攻击者必须与目标雇员建立起信任，一旦信任建立，BEC攻击就会有很大的概率成功。NTT安全专家认为BEC
their
job”。攻击者在发送第一封电子邮件之前证明了这一点。一般来说攻击者通常通过社交媒体识别出目标人物，这个目标任务一般都是在管理层中的，毕竟管理层才能有小
当BEC攻击首先流行起来时，资金往往转移到某亚洲大国或另一个亚洲国家的银行，但事实并非如此。现在来看，大多数的钱都放到了当地的小银行里面，甚至有的钱还
NTT的数据表明，如果一封邮件让你进行电汇的操作，同时包含了一个看上去很官方的PDF附件，90%的可能性都是攻击者发起的BEC攻击行为。
与上一个topic类似，NTT也同样给出了针对BEC攻击的防御措施，分为个人、管理和技术人员。

针对个人而言：

- a)
  避免向社交媒体发布关于我们的工作职责的过多信息，我们的经理，队友和员工等的名称。攻击者可以收集这些信息，并将其用于我们或我们的同事进行BEC攻击。
- b) 在发送电子邮件中的任何敏感请求之前，请查看BEC攻击的迹象，例如使用模仿域名或电子邮件内容，这些信息不是发送者所期望的。
- c) 如果我们发现尝试的BEC攻击，立即与安全管理和同事进行通信。

针对管理而言：

- a)
  要求通过电子邮件进行的敏感请求进行带外验证，如电汇。例如，要求接收电汇请求的员工通过电话或与请求者进行面对面的交互来实现。这可能包括验证所有交易在

- b) 最大限度地减少通过电子邮件处理敏感请求的人数。

- c) 对所有可能被BEC攻击的职责的员工进行定期的安全意识培训，例如完成电汇请求和提供人员信息。确保本培训具体包括对这些员工的BEC培训。

对于技术人员而言：

- a)
  识别和注册是组织域名的网站。我们的组织通常可以以很少的成本注册相似的域名。这可能使攻击者难以识别可用的伪造电子邮件地址。来自原始目标域名的拼写的多

- b) 实施品牌或信誉监控服务，利用威胁情报来识别用于欺诈活动的模仿域，然后才能成为主动威胁。

- c) 在组织的电子邮件服务器上启用欺骗保护。
  欺骗性保护将允许我们的组织阻止从外部系统发送到我们的组织的无效电子邮件，另一种用于尝试欺骗用户的技术。例如，我们的组织不应该从"From"地址接收使用
  这样的电子邮件是试图伪造或欺骗电子邮件的来源，因为服务器只能使用组织的域名离开组织的网络才能看到电子邮件。

- d) 严格限制可用于执行电汇和其他大量转帐的远程访问。仔细审核所有此类活动，并立即调查任何异常情况。

- e) 要求由电子邮件发出的敏感请求由发件人进行数字签名，并要求收件人验证这些数字签名。任何未通过验证的请求都应停止并立即报告给安全部门。

Dimension Data的Matthew
Gyde认为：像BEC这样的网络钓鱼计划越来越复杂，因为网络犯罪分子使用新的工具和手段创造出真实的电子邮件和其他以欺骗为核心的通信形式。
影响往往很严重，最初的诈骗导致电汇数十万美元。
为了防止这些攻击，企业不仅要解决技术工具，而且要解决支持流程和企业文化，以确保员工能够确定通信是否可靠。

（3）亚洲区域：

从这张图上大致就能看出来了，亚洲区域发起最多的攻击是恶意软件29%，其次是DDoS拒绝服务攻击16%，然后是Web层的攻击6%（其实根据国内的一些安全报告也能
NTT认为：在2016年，网络钓鱼仍然是用于为未来恶意活动征集信息的首要攻击媒介。 亚洲对反网络钓鱼运动和安全意识倡议的兴趣更大。
针对最终用户设备和客户端应用程序的恶意软件通过网络钓鱼活动或互联网攻击是影响客户的最大的安全威胁。有效的补丁管理对许多客户来说仍然是一个挑战。一个漏
从NTT给出的数据来看，攻击亚洲区域的国家主要是美帝占了63%的流量，5%来自于棒子国，7%来自于猴子国。（不知道NTT的数据的问题还是这里针对Korea有误解
Korea）

NTT还说了，这些攻击源有一部分是来自于东亚某国（6%），土鸡国（2%）和阿三国（1%）；同时蠕虫病毒（78%）、木马后门（15%）和后门键盘记录器（5%）是

NTT的数据显示，Mirai僵尸网络的来源有60%都是亚洲的IP地址。其实从我国的基础设施就能看出来，绝大多数网络摄像头其实都存在弱密码，不信大家可以跑一下。也
NTT的专家认为：物联网设备可以帮助人们和组织的方式是无限的。 不幸的是，IoT设备容易受到影响标准IT设备的许多相同类型的攻击。
这一点在2016年9月份在世界各地得到证实，当时的袭击者使用Mirai僵尸网络，从消费者和企业环境中窃取数十万个受损的IoT设备，以破坏其他设备和网络的运行。
这些大规模攻击被称为分布式拒绝服务（DDoS）攻击。

使用IoT设备的DDoS攻击可以以多种方式直接和间接地危害组织，包括：

- a) 攻击可以防止客户，合作伙伴和其他人访问我们组织面向互联网的资源，影响销售和其他日常业务

- b) 攻击可以防止员工和内部系统访问互联网，严重干扰操作的许多方面。

- c) 攻击可能会使一个或多个互联网组织向我们的组织提供服务，从而导致我们的组织的供应链被破坏。

- d)
  攻击可能会损害我们的组织的声誉，并且可能会导致我们的组织中的IoT和OT设备遭到破坏，从而将部分或全部组织的网络列表列入黑名单，以参与对其他组织的DD

DDoS只是一个攻击方面，显然网络罪犯可以将IoT和OT设备用于其他恶意用途，包括：

- a) 攻击者可以访问IoT摄像机和其他设备来监视人

- b) 攻击者可以访问IoT和OT设备以获取个人信息。

- c) 攻击者可能会操纵OT设备造成损坏。
  一个例子是对服务器机架进行温度监控，并打开数据中心恒温器，这可能导致设备由于极端的热量而未被检测到故障。

- d) 攻击者可能会损害IoT或OT设备，作为其他内部和外部攻击的利用点。

到底是什么造成这种情况的呢？我们首先来看看物联网设备是如何受到威胁的，那么受感染的设备如何一起使用来执行DDoS攻击。
IoT设备包括许多潜在的安全漏洞，攻击者可以利用这些漏洞来破坏设备。
在最糟糕的情况下，IoT设备没有基本的安全功能，或者没有使用安全功能，这使得它非常容易受到威胁。
在其他情况下，正在使用安全功能，但它们没有正确设置。
例如，IoT设备可能需要人员在访问密码之前提供密码，但用户从未将设备的密码从默认值更改。 知道默认密码的人都可以访问设备。

IoT设备的其他潜在安全问题包括：

- a) 设备可能缺少修补程序来修复安全问题。

- b) 设备的供应商可能已经停产或停止支持设备，这意味着补丁不再可用于修复安全问题。

- c) 设备可能不会使用加密来保护其网络通信免受窃听。

- d) 设备使用的Wi-Fi网络可能无法正确保护，允许网络范围内的攻击者窃听设备的Wi-Fi通信。

多年来，他们已经在标准的IT设备中使用，而且在许多传统IT部署中仍然存在一些。
在很大程度上，许多IoT设备在安全功能方面几十年来落后于现代IT设备，而有限的安全功能往往是非专业人士使用的难题或几乎不可能的。

一旦攻击者攻陷了IoT或OT设备，他可以准备参与DDoS攻击。这有三个基本步骤：

- a) 攻击者在设备上安装恶意软件和工具，通常通过攻击者很少或不需要进行的自动化过程。
  恶意软件和工具使攻击者能够远程控制设备，并将设备加入到被称之为僵尸网络的受感染设备的全局组中。

- b) 当攻击者想要准备DDoS攻击时，他选择一个目标和一种类型的DDoS攻击来发起攻击目标

- c) 攻击者发送一个命令来指示设备在所需的时间内执行DDoS攻击。

NTT的安全专家使用蜜罐来密切监测和分析基于IoT的攻击。 根据所使用的证书分析攻击目标的结果如下：

- a) 66%的人正在寻找特定的IoT设备，如特定型号的摄像机。

- b) 有3%的人正在寻求一个Web服务器或其他类型的服务器。

- c) 2%的人试图攻击一个数据库。

- d) 其余29%涉及各种其他目标。

基于对蜜罐技术的NTT安全分析，针对IoT设备的66%的攻击似乎来自试图找到并损害更多此类设备的易失性IoT设备。
这与攻击者获取大量用于DDoS和其他形式攻击的设备是一致的。
对于其他34%的攻击分析的结果，很可能这些攻击者也试图通过瞄准其他类型的设备来增加攻击者的武器库。DDoS攻击没有任何要求，只需要使用IoT设备，因此攻击者
NTT的安全专家对蜜罐数据的分析的另一部分是查看尝试验证蜜罐的攻击所使用的密码。
蜜罐记录了超过20,000个唯一密码，但这些密码的一小部分被一次又一次地使用。 以下25个密码最常用于认证尝试的几乎33%。
NTT的分析师将来自这些身份验证尝试的密码与两个众所周知的密码列表进行了比较。一个是2016年期间人们最常使用的密码列表。另一个列表是在Mirai的僵尸网络中

密码比较的结果很明显。 只有10%的身份验证尝试使用最常用密码列表中的密码。
但是绝大多数76%的身份验证尝试包括由Mirai僵尸网络实施的密码。这表示很大一部分对蜜罐的攻击最有可能来自未来僵尸网络和其他自动攻击源。
NTT的安全专家还研究了每个基于IoT的攻击的地理来源。 如上图所示，所有IoT攻击中有60%来自亚洲的IP地址，其中EMEA占21%，美洲占19%。
来自亚洲设备的大量攻击的最有可能原因是，亚洲市场的产品历史上被证明易于受到攻击的影响，并在后续的攻击中重复使用。
针对IoT攻击，NTT安全专家一些建议，可以减少IoT和OT设备被用来发起攻击：

针对个人用户而言：

- a) 如果消费者IoT设备不需要互联网接入，请不要使用互联网。

- b) 保持所有消费者IoT设备更新。 尽可能配置它们，以便在可用时立即自动下载和安装更新。

- c) 在将其放在网上之前，将所有IoT设备的默认密码更改为只有我们知道的内容。

- d) 选择访问消费者IoT设备的强密码。 避免密码从最常用的列表中，因为攻击者知道尝试这些密码。 对每个IoT设备使用唯一的密码也是至关重要的 - 我们不需要使用其他密码。

- e) 利用消费者IoT设备中的可用安全功能。 花几分钟时间查看每个设备的文档，找出安全选项。
做你可以使用这些选项，并要求有更多的安全专家的人帮助，如果必要的话。 这个小小的努力可能会为你节省许多头痛。

针对管理者而言：

- a) 使安全成为所有IoT和OT设备采购的主要考虑因素。 拥有内置强大安全功能的设备。如果没有可用的设备，请查看可能更容易确保的传统技术

- b) 扩展业务连续性和事件响应功能，以包括DDoS攻击。 为了业务连续性，这不仅应该解决针对组织的DDoS攻击，而且还应对DDoS攻击供应商。

- c) 根据需要授权资金，以替代其供应商不再支持的旧的IoT和OT设备。

针对技术人员而言：

- a) 扩展现有的补丁管理和软件配置管理流程和技术，包括IoT和OT设备。 经常监视IoT和OT设备的补丁和配置设置（理想情况下，连续）。

- b) 管理访问IoT和OT设备的所有凭据，例如为每个设备设置复杂的唯一密码，安全地存储这些密码，如果怀疑被攻陷，则更改这些密码。

- c) 评估和使用技术来监测IoT和OT设备安全性并检测涉及IoT和OT设备的攻击。

- d) 评估和使用停止DDoS流量（入站和出站）的技术。

（4）澳洲区域：

澳洲区域的攻击情况基本上和美洲地区类似，基本上攻击瞄准的行业还是金融类34%、销售零售类行业27%，专业和商业服务20%。澳洲区域发起攻击类型DDoS占得份

而针对攻击澳洲区域的流量来看，最大的是来自于澳洲本土，占到攻击流量的86%，其次是美帝（9%）和德国（1%），攻击服务大多数为远程管理（43%）、文件共享

需要注意的是：澳大利亚联邦议会于2017年2月通过了"应通报数据违规法案"该法案将成为强制性数据违规通知法，该法案成为适用于已经必须遵守"隐私法"的政府机构和
根据这项法案，确定他们已被违反或已经丢失数据的组织将需要报告事件，并通知直接受到影响或"有风险"的客户。如果要是违反法律的话，个人需要支付罚款36w澳元
针对澳洲区域，NTT的安全专家认为最大的风险是来自于终端软件技术也就是诸如IE、Flash这些平时大家用的很多的东西。根据NTT去年防御攻击的数据，过去一年里发

针对最终用户技术的攻击工具包生成的攻击可能会以多种方式影响我们和我们的组织。比如：

- 危及我们的个人台式机或笔记本电脑

- 锁定企业台式机或笔记本电脑上的信息

- 通过恶意软件感染我们的公司计算机

重要的是要明白，单个攻击工具包对我们的个人或公司计算机生成的攻击可能是对我们的组织进行更大规模攻击的启动点，可能使我们的组织损失数百万美元。
为了更好地理解这种情况，在攻击者选择了他们选择的攻击工具包和攻击目标之后，让我们逐步了解攻击的步骤。
a) 攻击者需要用户将他们的计算机连接到攻击者的恶意软件分发网站。
该网站可能是攻击者妥协的良性网站，也可能是攻击者或攻击工具包创建者拥有的网站。
攻击者可以通过以下几种方式引诱受害者访问网站，包括将用户从良性网站重定向到恶意网站或向用户发送网络钓鱼邮件。
攻击者还广泛使用恶意广告，其中用户被展示假冒广告，将用户重定向到攻击者的利用工具包，而不是连接到真正的广告赞助商。
b) 漏洞工具包可以执行各种功能，具体取决于特定的工具包和访问该网站的计算机的特征。
利用工具包通常会确定访问计算机的浏览器和操作系统的产品和版本号以及其他特性，这个过程称为"指纹识别"。
攻击工具包然后提供利用漏洞利用的漏洞。 这个过程通常导致在访问计算机上有效的恶意软件的传送。
c) 如果成功，攻击者已经感染了恶意软件的计算机，可能授予对计算机的完全远程控制权。
利用工具包提供勒索软件，按键记录器和银行木马（除其他外），帮助向攻击者提供额外的证书或访问权限，以便他们可以使用这些证书或证书扩展其在目标组织中的范
由于多方面的绞杀，Flash这类的技术用的越来越少了，所以攻击的次数变得也越来越少了，根据NTT的数据来看，从2015Q4到2016Q3的整体趋势是下降的。

NTT的安全专家提供了以下建议，以减少组织受到最终用户技术攻击的可能性。请注意，这些建议是对"网络钓鱼"，"社会工程学"和"勒索软件"部分中的所有建议的补充。

对于个人来说：

- a) 每当我们从台式机或笔记本电脑收到有关下载和安装修补程序的通知时，请尽快遵守。 确保它源自有效的来源，否则我们可能正在安装恶意软件。

- b) 不要对我们的个人和公司帐户使用相同的密码。
  攻击者知道许多人重复使用密码，所以如果他们窃取你的密码之一，他们可能会尝试在很多地方你可能有一个帐户。
  我们可以通过采用更好的方法来管理我们的密码，例如使用密码管理器工具来安全地存储所有密码，并在需要时为我们检索密码，从而避免密码重用。

对于管理员来说：

- a) 分配足够的资金，以便在对旧（已安装）版本的支持结束之前，在所有台式机和笔记本电脑上升级目标软件。

- b) 如果目标软件当前没有用于操作，请考虑卸载整个组织并禁止使用。

- c) 如果任何目标软件不是必需的，考虑将其功能转移到其他软件，并尽可能消除目标软件。
  ####
  对于技术人员来说：

- a) 开发功能性强大的补丁管理功能。 确保针对目标软件的修补程序尽可能快地评估，部署并安装在所有受影响的台式机和笔记本电脑上。

- b) 通过网页浏览器维护目前所有的桌面和笔记本电脑软件清单。
  定期查看此清单，以识别当前版本中不再存在的软件，以便在支持结束和分发安全更新之前对其进行升级

- c) 评估广告拦截技术，并考虑将其部署到所有台式机和笔记本电脑，以最大限度地减少恶意广告的攻击。

- d) 为企业安全控制（防火墙，入侵防御系统，安全信息和事件管理[SIEM]技术等）订阅威胁情报源以更快地识别和阻止与漏洞利用工具相关的网站。

- e) 部署终端安全解决方案，通过沙盒或其他高级技术来识别并包含前所未见的恶意软件威胁。

0x03 对于这份报告的看法：

首先，这份报告在国内的安全媒体上基本上没有看到任何相关的信息，绝大多数网络安全媒体只关注卡巴、赛门铁克、思科这些安全能力大家心里都有逼数的公司，这其其实NTT这份报告的亮点在于将对应区域的所遭受的攻击以及攻击的原理介绍的非常详细且易懂，并且给出了一些解决方案，对一些安全技术不是很强的公司有一些帮助
纵观NTT的安全数据，北美、欧洲、澳洲以及亚太部分发达地区面临的最大的威胁其实就是两个：日益升级的钓鱼威胁和面向基础设施的勒索威胁，由于这些地区经济发
而针对不发达地区，由于基础设施建设问题和产业问题，往往建筑类行业和制造类行业就变成了攻击的对象，NTT的数据也恰好体现了这点。不发达地区由于自身原因，

透过NTT这份报告，我们可以看到的是：

- a) 高级点的攻击者会根据地域特点和结构发起针对性的无差别攻击

- b) IoT设备越来越被青睐于组建各种僵尸网络

- c) 钓鱼类攻击是现在最流行的攻击方式

- d) 我们的安全真的做的很好么？

---

1. 2 条回复


笑然 2017-11-04 14:50:36

好文

0 回复Ta


hades 2017-11-06 14:29:21

@elknot 辛苦了 (□•□□•□)□□

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