2016 年 12 月 19 日，星期一

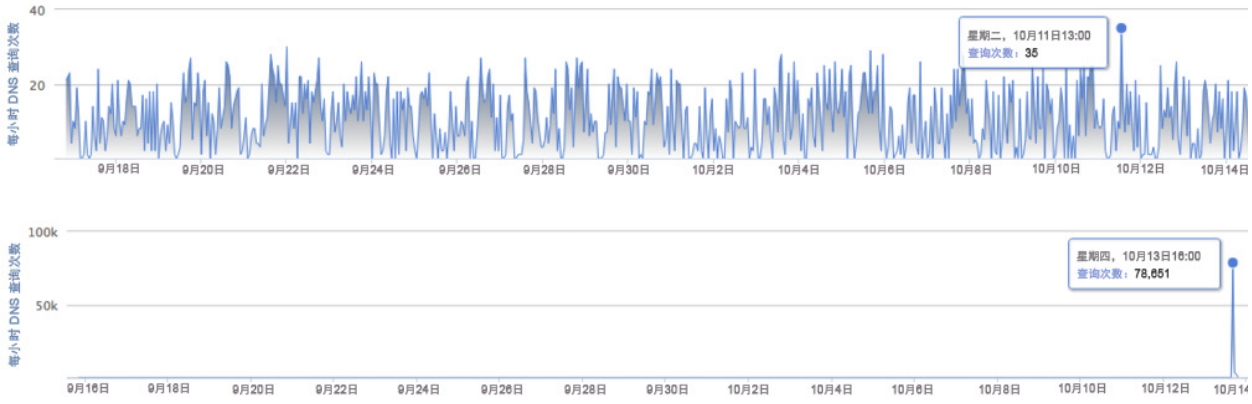
雹暴在席卷一切

作者：Jakob Dohrmann、David Rodriguez 和 Jaeson Schultz。

思科 Talos 和 Umbrella 研究团队正在部署一个分布式雹暴检测系统，该系统将机器学习、DNS 请求的流处理以及整理的 Talos 邮件语料库结合到一起。

Talos 之前已讨论过雪鞋垃圾邮件。传统的雪鞋垃圾邮件活动通过大量的 IP 地址发送，每个 IP 地址发送少量垃圾邮件。雪鞋垃圾邮件发送者通过使用此类技术，试图逃避反垃圾邮件系统可能应用的任何基于信誉或数量的指标检测。本帖探讨有关“雹暴”垃圾邮件的问题。雹暴垃圾邮件是雪鞋垃圾邮件的升级。雪鞋垃圾邮件和雹暴垃圾邮件都通过大量发送者 IP 地址发送，但与雪鞋垃圾邮件不同的是，雹暴垃圾邮件活动在短时间内发送的邮件量非常大。事实上，有些雹暴垃圾邮件攻击可在最快的传统反垃圾邮件防御刚要更新响应时结束。

下面的图片来自 Umbrella Investigate，很好地说明了典型雪鞋垃圾邮件活动与典型雹暴级邮件活动之间的区别。下面顶部的图片说明的是典型雪鞋攻击中涉及的域的 DNS 查询量。请注意，雪鞋域示例的最大查询率仅为每小时 35 次查询。对应的底部图表显示的是典型雹暴攻击涉及的域的 DNS 查询量。在此图表中，最初几乎没有查询量，直到 DNS 查询量忽然上升至每小时 75000 多次查询，然后再回落至零查询量。

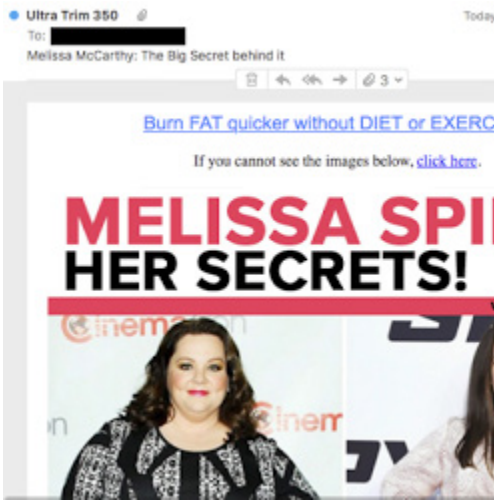


传统雪鞋垃圾邮件（顶部）与雹暴垃圾邮件（底部）的典型 DNS 查询量图。

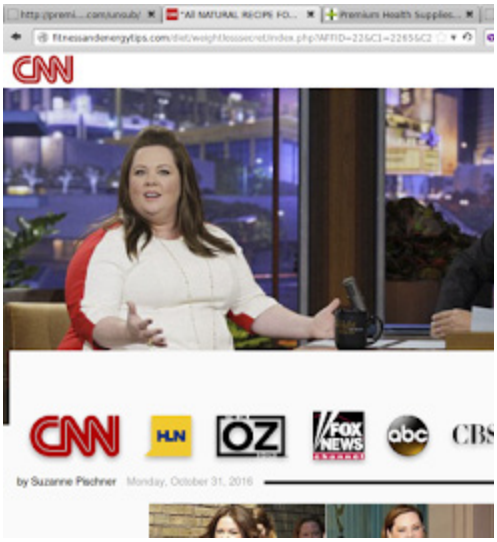
攻击者从全球各地的 IP 地址发送雹暴垃圾邮件。从最近的雹暴垃圾邮件活动的 IP 地理位置分布来看，按国家/地区划分，美国、德国、荷兰、英国和俄罗斯在发送的雹暴垃圾数量方面领先。雹暴垃圾邮件还涉及在广泛的顶级域 (TLD) 注册的域。在最近约 500 个与雹暴相关的域的样本中，最常见的 TLD 为 .top、.bid、.us、.win 和 .stream。

联合计划和赞助商链接

我们最初检测到的大多数活动宣传的产品包括家庭监控系统、手电筒、膳食补充剂以及“电视广告宣传的”各种商品。浴室重装、在线学位学习和心理学读物等各种各样的服务也很常见。以下是使用雹暴技术发送的典型联合产品推广的示例。此特定雹暴垃圾邮件活动宣传的是膳食补充剂。原始邮件中的链接会被重定向多次，最终重定向至登录页面，而登录页面则链接至联合公司页面上的订单表。我们已对包含收件人 ID 或任何其他个人身份信息 (PII) 的 URL 参数进行编辑，以保护无辜者。

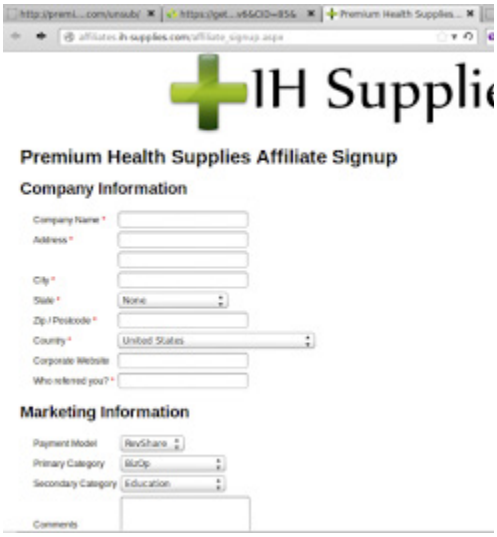


发件人：ultratrim350@secretaryship.coisow.us
包含的链接的形式：
http://<subdomain>.coisow.us/about/us/<redacted>
这些链接被多次重定向，命中 lbmcgroup.com、trackwebly.com、trackwb.com、atomtrk.com、ecptrx.com、ih-trk.com 等域。



登录页面：
http://fitnessandenergytips.com/diet/weightlosssecret/index.php?<redacted>
此页面包含外部订单表的多个链接（见下文）。

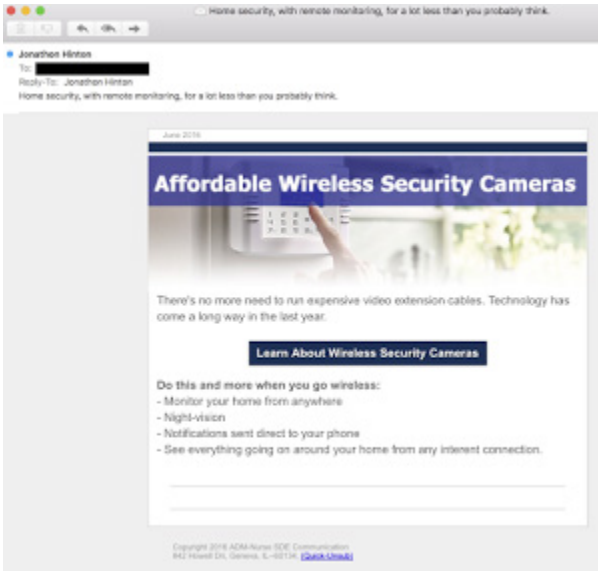
订单表：
https://getultratrim350.com/lp/bellymelt-p/index.php?<redacted>
除订单表外，此页面还包含一个连接至联合公司注册页面的链接（见下文）。



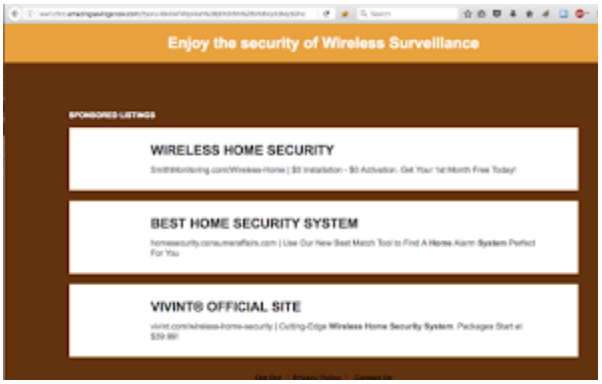
注册页面：
http://affiliates.ih-supplies.com/affiliate_signup.aspx
基础网域 ih-supplies.com 本身会导向至 GoDaddy.com 上寄放网域的登录页面。

上面看到的域均使用 whois 隐私服务注册。唯一的例外是“发件人”信头 coisow.us 中使用的域。该域由 *wireclick.tech@gmail.com* 注册，后者又与类似垃圾邮件活动中涉及的数百个其他域关联。

另一种典型的摊销方案是在赞助商链接上产生流量。下面是此类雹暴垃圾邮件活动邮件的一个示例，以及相应的登录页面。与我们的第一个示例一样，这些垃圾邮件发送者很懒惰且运营安全 (OPSEC) 状况很糟糕。在这种情况下，“发件人”地址 (babyfirstgames.com) 中使用的域注册到与参与雹暴垃圾邮件活动的许多其他域关联的邮件。



发件人：*jonathon.hinton@babyfirstgames.com*
包含的链接的形式：
http://www.babyfirstgames.com/<redacted> 该链接重定向多次。



登录页面：
http://ww1.cfcc.emazingsavingsnow.com/?<redacted>
该链接通常导向至本身没有参与该计划的合法企业和供应商。

以下“发件人”和“主题”信头示例突出显示了在最近的雹暴垃圾邮件活动中观察到的内容类型：

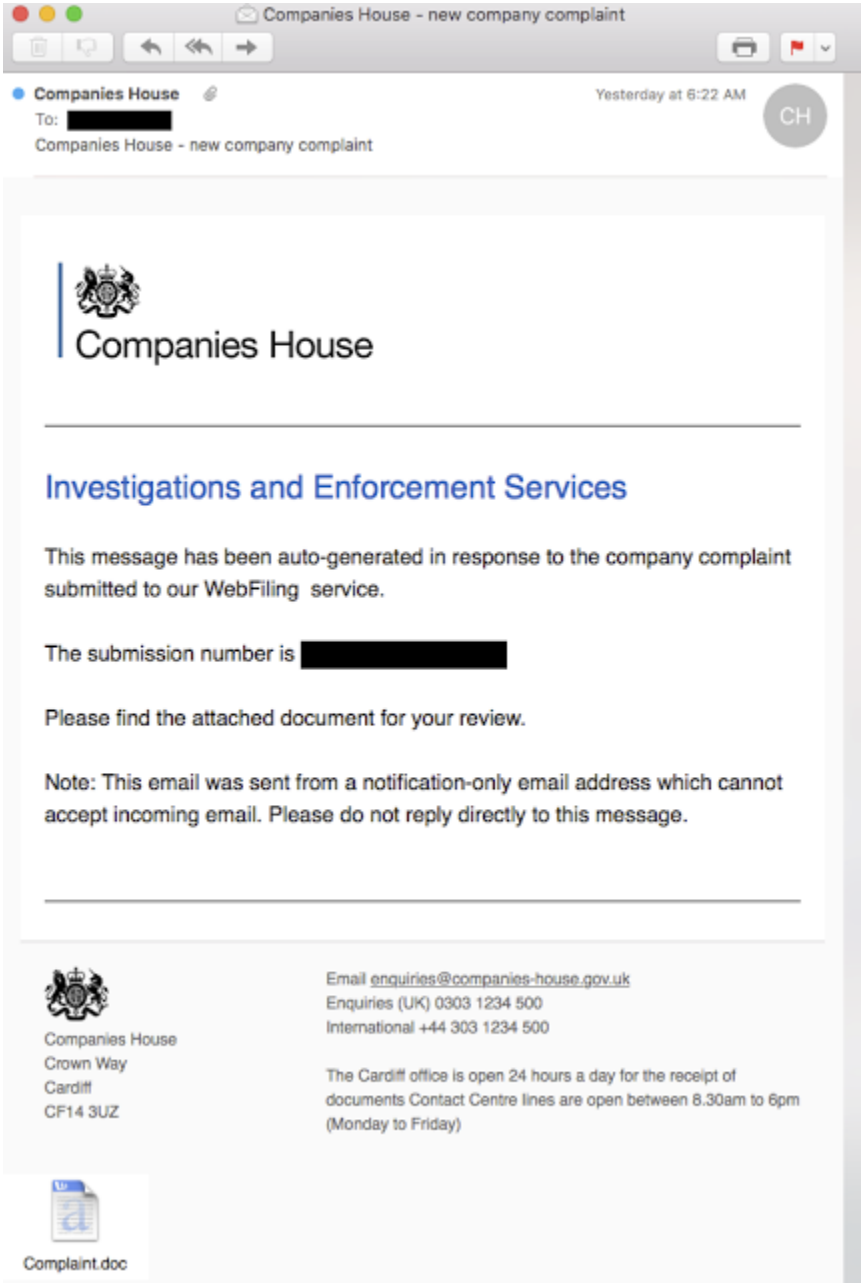
- 发件人：最新税款减免 <freshtaxrelief@chemiluminescent.duzeo.us>
- 发件人：健康婴幼儿配方奶粉 <Healthybabyformula@crewgraphics.stream>
- 发件人：VOIP 电话系统选项 <voipphonesystemoptions@wait.cotib.us>
- 发件人：星级激光手电筒 <ownstarnightlaser@lanight.bid>
- 发件人：Match.com 合作伙伴 <Match.comPartner@meterdown.top>
- 发件人：加勒比邮轮选项 <caribbean_cruise_options@firstthirteen.faith>
- 发件人：Costco 奖励赠品 <CostcoRewardsGiveaway@horithms.stream>
- 发件人：企业互联网服务 <BusinessInternetService@chineral.stream>
- 发件人：Paleo 秘密 <paleosecret@eumidnight.top>
- 发件人：混合动力汽车 <HybridCars@carhibrid.us>
- 主题：将碱性水倒入下水道
- 主题：政府超支：“超级手电筒”降价 75%
- 主题：照明度极高的军用大灯，刚向公众发布
- 主题：观察：如何自然地恢复膀胱控制
- 主题：特朗普承诺的是真的吗？他真的能让普通美国人富起来吗？
- 主题：治愈新血糖问题！

- 主题：满足独自在家等待的寂寞主妇（成人内容）
- 主题：您可能听说过有人通过网络赚钱？
- 主题：数字命理学阅读……
- 主题：世界上最快的手机超级充电器时代！

虽然这些活动通常更多的只是一种滋扰，而不构成威胁，但毫无疑问，点击垃圾邮件分发的链接存在多方面的风险。如果收件人公开任何个人或财务信息，则路过式下载很可能演变成企业邮件入侵、欺诈和身份盗用。

恶意软件和网络钓鱼

就像任何能够有效地提高邮件成功送达率的方法一样，雹暴活动也相应地更多用于破坏目的，而不是产生到联合公司页面的流量。Necurs 等僵尸网络也使用雹暴策略来传播恶意软件。下面是通过雹暴活动发送的恶意邮件示例。



该邮件声称是回应向英国公司登记局提交的投诉而生成的，并试图诱使收件人打开随附的 Word 文档。该邮件的发件人地址为 *noreply@companieshouses.com*，而该政府机构的合法网址为 companieshouse.gov.uk。随附 Complaint.doc (SHA256: 985e9f4c5a49e26782141c7cd8f4ce87b0e0a026d078b67b006e17e12f9eb407) 文档包含一个宏，该宏可下载并执行 Dyre/TheTrick 银行木马。

与前面的示例一样，发送域的注册者 *workorders@pesiec.com* 与以类似方式使用的多个其他域相关联。

此雹暴恶意软件活动与前两个示例有许多相似之处，例如整个活动的实施时间极短、注册者很可疑,等等。但与典型的雹暴垃圾邮件活动也有一些显著区别：攻击者通过更为广泛的 IP 地址发送邮件，包括没有解析为“发件人”信头中使用的域的地址。该邮件更符合传统的垃圾邮件和 bot 行为。

DNS 层

雹暴活动与 DNS 查询量的爆发相关，活动峰值时查询量可高达每小时 9,000 多次查询。雹暴活动的初始峰值源于大量邮件引起的邮件服务器活动。了解雹暴活动生命周期的一种方法是查看指定域中有多少邮件服务器。下面，我们将对比三个雹暴域以及被访问的邮件服务器的比例。我们将每小时的查询峰值（即查询量中的最大峰值）与从每个域接收到雹暴垃圾邮件的邮件服务器的百分比进行比较，从而揭示雹暴活动的特征。

域	每小时的查询峰值	邮件服务器命中百分比
cooperindustries.space	8,049	0.381%
pourdra.top	23,790	3.457%
cmobi.stream	106,590	4.013%

在这几个具体示例中，我们可以收集有关雹暴活动的规模和广度的线索。数据表明，活动规模与命中目标的概率之间相关性较弱。由于这些只是来自我们的域池的三个数据点，因此我们没有得出太多的结论。

如果我们比较 475 个雹暴域样本（以平均每小时 9332 次的峰值查询量访问邮件服务器）的目标邮件服务器的分发情况，我们可以看到，与世界其他地区相比，美国内的目标邮件服务器明显更多。

地理分布	邮件服务器命中百分比
美国	2.586%

非美国地区

0.840%

根据上面的数据，我们得出结论，大多数目标邮件服务器位于美国。这可能是由于语言偏好、摊销基础设施、目标受众或与垃圾邮件发送者工作流程相关的其他原因导致的。

雹暴防护

在此次协作中，思科 Talos 与 Umbrella 研究团队创建了一个系统，该系统可促进快速评估和确定活动雹暴域，然后继续收集对可能用于未来活动的其他域的预测见解。因此，如果雹暴邮件已到达收件箱，系统可以在客户点击邮件时快速地为客户提供保护。更重要的是，系统的预测性可直接抵御雹暴活动的标志性行动：快速执行。系统会提前部署对下一次垃圾邮件活动的防护，而不是等待活动展开并试图围追堵截。

如示例中所述，雹暴有多种类型。我们希望随着时间的推移，反垃圾邮件系统使垃圾邮件发送者更难以传输其负载。Talos 与 Umbrella 协作，将垃圾邮件活动与 DNS 流量进行匹配，使我们能够快速应对和防御不断变化的威胁形势。

发布者：JAESON SCHULTZ；发布时间：8:00

标签：DNS、DRIDEX、邮件、雹暴、恶意软件、雪鞋、垃圾邮件、TALOS