2017 年 3 月 20 日，星期一

Necurs 变换攻击手段

本文由 Sean Baird、Edmund Brumaghin 和 Earl Carter 共同撰写，文中采纳了 Jaeson Schultz 提供的信息或建议。

执行摘要

Necurs 僵尸网络是世界上最大的垃圾邮件僵尸网络。过去一年间，该僵尸网络主要用于分发 Locky 勒索软件和 Dridex。今年早些时候，我们曾撰文介绍，Necurs 僵尸网络似乎从网上消失，大多数规模庞大的 Locky 恶意垃圾邮件也随之消失。Talos 最近发现，从 Necurs 僵尸网络发出的垃圾邮件数量显著增加，表明 Necurs 可能卷土重来。不过，此次它并未采用恶意附件的形式分发恶意软件，而是重新改为低价股炒股欺诈邮件。这并非 Necurs 第一次被用于发送大量炒股欺诈邮件。在分析与这些攻击活动相关的历史遥感勘测数据时，我们发现在 2016 年 12 月 20 日（也就是 Necurs 僵尸网络长时间消失前不久）曾经发生过类似的攻击活动。此番从分发恶意软件到发送垃圾邮件的战略转变可能暗示着攻击者在试图利用此僵尸网络牟取经济利益的方式上发生了变化。

详细信息

2017 年 3 月 20 日，我们注意到从 Necurs 僵尸网络发出的垃圾邮件数量似乎有了明显增加。有趣的是，这些邮件并未沿袭我们已经习惯于从 Necurs 看到的邮件主题。要知道，该主题早已成为 Locky 勒索软件系列和 Dridex 银行木马的一种主要分发手段。与 Locky 和 Dridex 相关的邮件攻击活动通常伪装成交易通知，并声称包含发货通知、ACH 交易通知等。而在此次攻击活动中，邮件不含任何恶意服务器的超链接或任何恶意附件，而只是声称这是有关某只具体股票 ($INCT) 股价即将上涨的股市行情提醒邮件。

邮件的行文结构旨在诱使用户认为这是一个不容错过的大好机会 - 典型的一夜暴富骗局。首先，邮件以一句简单的引言开头：

“我已经很久没有给你发送包含热股情报的特别通讯了。”

然后，邮件声称，根据曼哈顿 M&A 公司同行提供的信息，DJI（一家无人机公司）将以每股 1.37 美元的价格买下 InCapta Inc ($INCT) 的股份。邮件解释，DJI 之所以推动此次收购，是因为 InCapta：

“设计制造了首批独立无人机，可派往犯罪现场、追车现场、山火现场等令人兴奋的区域，在无人机行业掀起了一场革命。”

除此之外：

“通过连接到云来运营的无人机网络和复杂的算法能够有效地在所报道的事件发生瞬间派遣无人机。”

“这样，拥有无人机的媒体就可以率先赶到现场进行独家现场直播。”

为了增加紧迫感，邮件还提到 3 月 28 日应该就会宣布此次收购，因此建议设定一个买入限价（其建议是在股价达到每股 20 美分前买入），以确保“巨额回报”。为了进一步增加紧迫感，邮件还声称 DJI 愿意支付高于当前价值 1000% 的股价，其原因如下：

“正如我们所知，它具有切实改变新闻广播行业的潜力，而 DJI（全球最著名的无人机制造商）看到了这项技术的潜力，因此他们愿意支付每股 1.37 美元买入此股票。这可是比周五收盘价高 1,000% 的高价。”

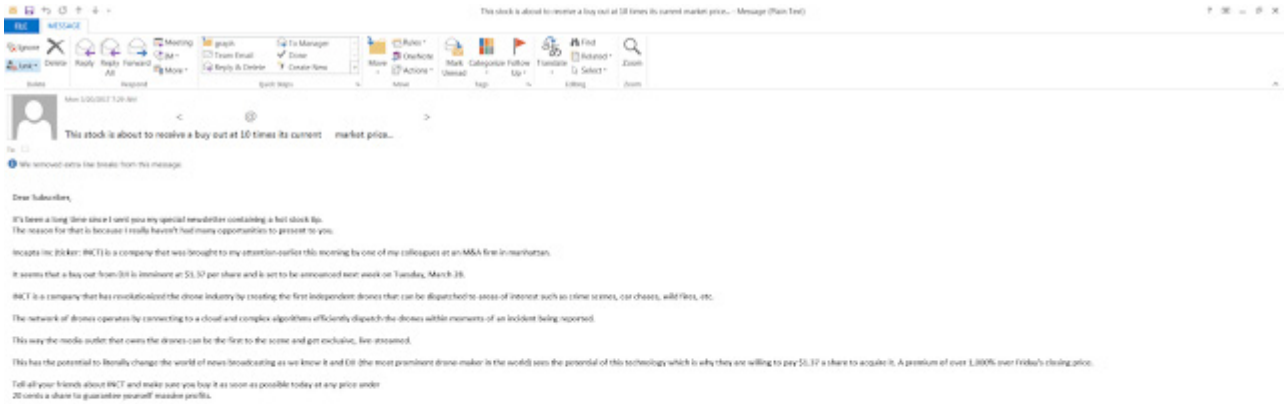

图 1：邮件示例

正如涉及邮件攻击活动时的正常情况一样，这些邮件的发送数量相对较多，仅仅 3 月 20 日早上这段时间就达到数万封。通过分析我们的邮件遥感勘测数据，我们可以清楚地看到，邮件数量与 Necurs 从网上消失那段时间相比发生了变化。虽然邮件数量很多，但垃圾邮件攻击活动本身的持续时间似乎根本就不长，大多数邮件的发送集中在区区几小时内。

此次所涉及的股票与移动应用开发公司 InCapta Inc. 有关。该股票的股票成交量大幅上升。在分析此次垃圾邮件攻击活动时，我们注意到股票成交量超过 100 万股（当天晚些时候的总数超过 450 万股），与平均股票成交量相比呈指数升高。

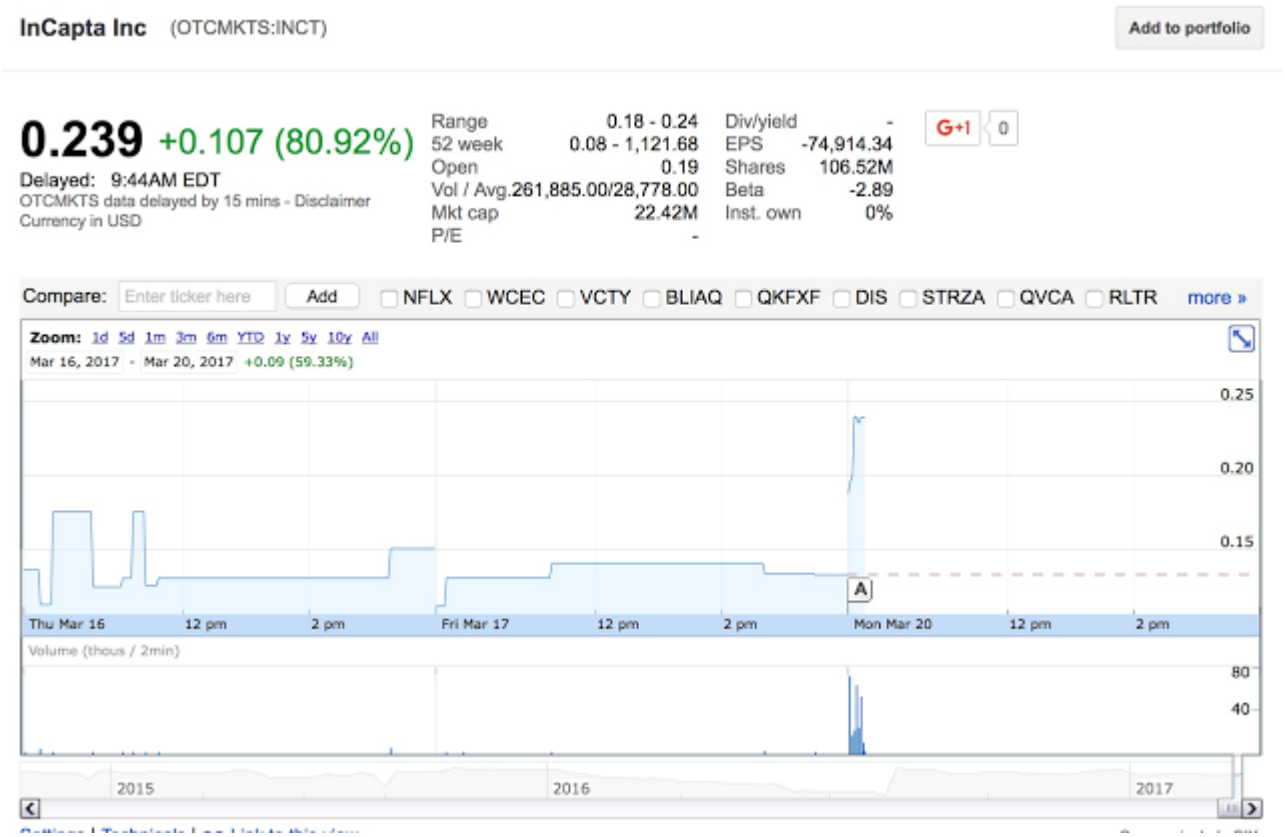

图 2：$INCT 的 Google Finance 数据

分析此第一次攻击活动后不久，我们在 SpamCop 遥感勘测数据中发现了通过大量发送垃圾邮件发起的第二次攻击活动。

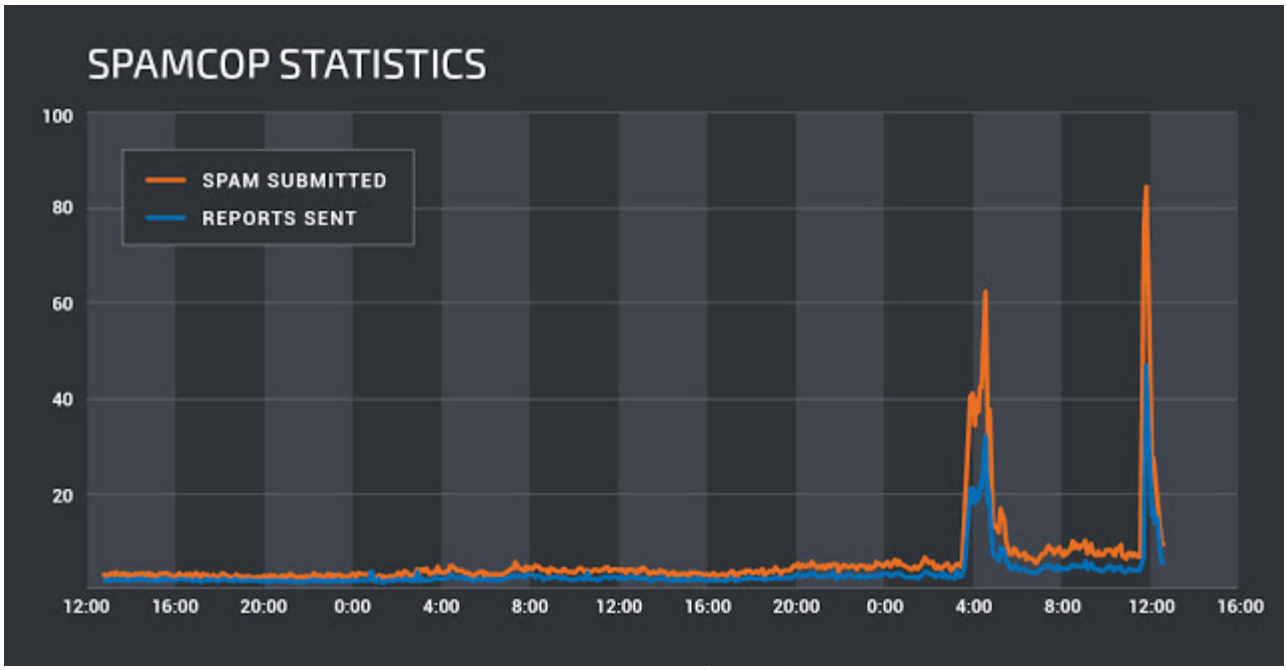

图 3：SpamCop 统计信息

有趣的是，大约就在这第二波垃圾邮件发送的时候，股价也有所上涨。这第二次邮件攻击活动与第一次非常相似，只不过包含的主题和邮件正文略有不同：

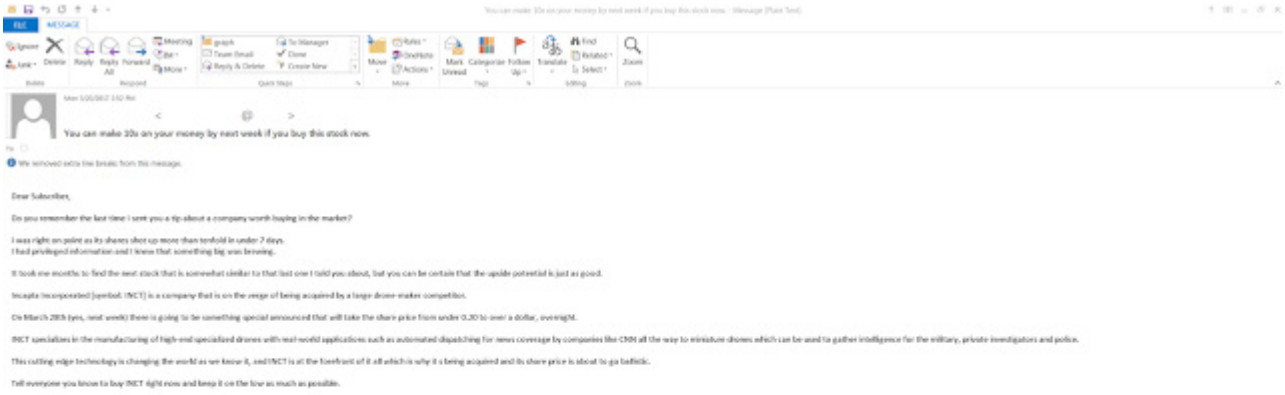

图 4：第二封邮件示例

过往的 NECURS 攻击活动

2016 年 9 月 21 日，Talos 发布概述“垃圾邮件大潮”的博文，详细介绍 2016 年夏季 Necurs 发送的垃圾邮件数量增加的情况。这些邮件通常用于传播 Dridex 或 Locky 恶意软件变体，每天将数百万封邮件发送到全球各地的收件箱中。

但是在 2016 年 12 月底，此邮件流量突然终止，邮件数量降至不到 Necurs 基础设施典型流量的一半。在这段停止攻击期间，我们的垃圾邮件阻止列表平均值一直保持在 5 万个地址。而在这些新攻击活动期间，阻止的地址数量飙升至超过 15 万。此峰值在前文所述的 2017 年 3 月 20 日邮件数量中有所反映，在下图中也有显示。

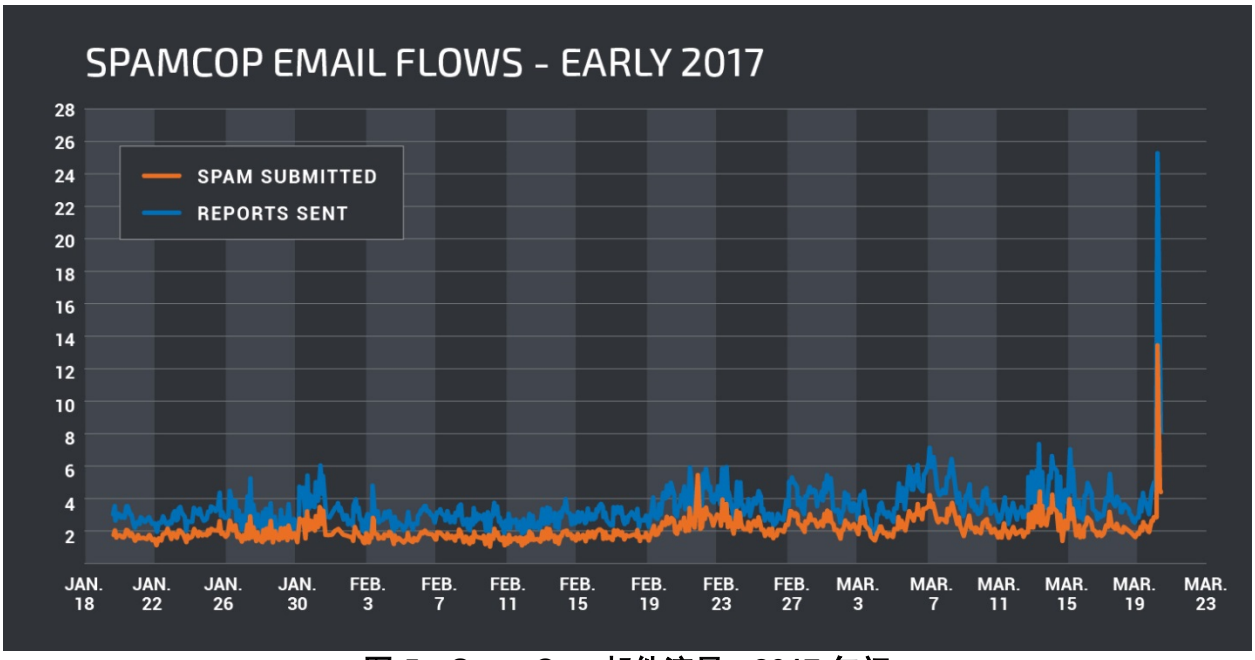

图 5：SpamCop 邮件流量 - 2017 年初

但是，Necurs 曾经发送过炒股欺诈垃圾邮件吗？在 2016 初的拘捕行动（带来一段僵尸网络活动量下降的平静时期）之前，Necurs 经常发送不同的炒股欺诈垃圾邮件。就在最近这次攻击停止期开始之前，2016 年 12 月 20 日还有中等数量的炒股欺诈垃圾邮件经过我们的数据源。这些垃圾邮件煽动收件人购买 $SWRM 股票，邮件主题与下图类似：

- “如果您想买一只圣诞节前涨一倍以上的股票，请立即阅读这封邮件。”
- “该股票的价格在圣诞节前将翻两番。现在正是入手的大好时机！”

12 月 20 日的这次攻击活动与 3 月 20 日的攻击活动有着类似的报头和属性，表明 12 月 20 日的攻击活动也少不了 Necurs 僵尸网络的帮助。其中一个此类属性是在炒股欺诈攻击活动的邮件中发现的 X-PHP-Originating-Script 报头。

- X-PHP-Originating-Script: 1001:Sendmail.php

但是，2016 年大规模恶意软件攻击活动期间发送的分发 Locky 和 Dridex 的邮件中并不存在此报头，暴露了 Necurs 服务和基础设施之间的私下差异。另一方面，这两种类型的攻击活动有着共同的收件人，暗示了这一事实：即便客户端请求的是不同服务，Necurs 操纵者使用的可能仍是同一个邮件地址数据库。

总结

Necurs 这个例子很好地说明了攻击者如何随着时间推移不断改变他们利用自己控制下的系统牟利的方法和战略。类似 Necurs 这样的僵尸网络代表着 Talos 持续监控其活动和攻击手段变化的一种媒介。随着威胁不断变化和发展，Talos 将继续监控不断演变的威胁形势，确保

我们的客户始终能够防御任何新威胁。

Talos 将继续监控 Necurs 僵尸网络因为被用于任何用途而再次变得活跃的迹象。

防护

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	不适用
CWS	不适用
邮件安全	✔
网络安全	不适用
Threat Grid	不适用
Umbrella	不适用
WSA	不适用

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

发布者：EDMUND BRUMAGHIN；发布时间：17:18
标签：僵尸网络、NECURS、垃圾邮件