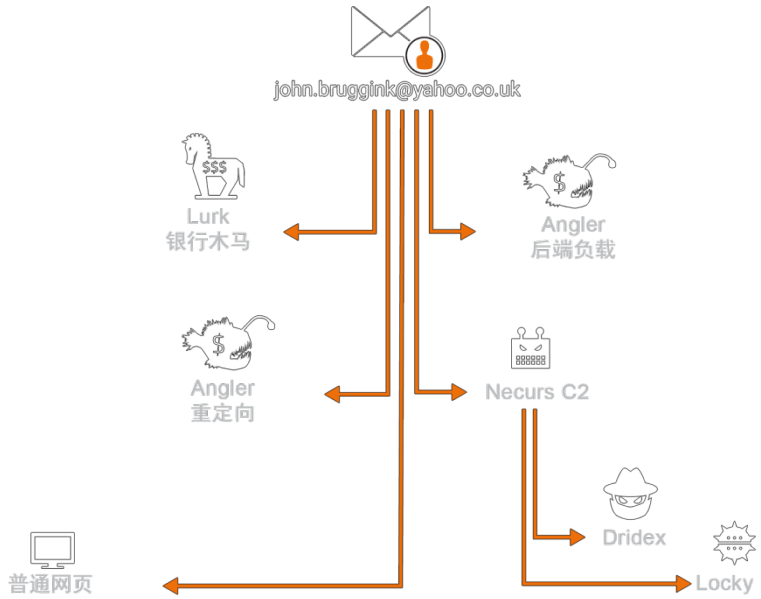
2016 年 7 月 7 日，星期四

通过联系分散的线索揭示犯罪软件格局剧变

作者：Nick Biasini



在 6 月的几周内，威胁形势发生了变化。多个高度活跃的威胁突然消失，导致威胁格局出现了前所未见的剧烈变化。如果只是从短期来看，有三周的互联网形势相对安全。到目前为止，Angler 漏洞攻击包尚未恢复活动，威胁形势似乎发生了永久性变化。本文将讨论与一个名为 Lurk 的银行木马相关的一系列事件，以及一个在整个犯罪软件格局中具有深远影响的注册者帐户。

详细信息

犯罪软件是一种恶意软件，其唯一的目标就是获取金钱。这类恶意软件通常与一些规模最大，而且攻击活动遍布全球的威胁相关，包括各种漏洞攻击包及其最常见的负载勒索软件。犯罪软件的一个主要特性是不加区别地感染大量用户。它们偶尔会针对特定个人或组织，但是大多数情况下是感染那些通过邮件、Web 或其他方法与威胁进行交互的用户。最近 12 至 18 个月以来，勒索软件一直呈激增之势，所以制作并利用犯罪软件的犯罪分子非法获取的金钱也大幅增加。正因如此，Talos 监测到的犯罪软件的类型和数量也在与日俱增。目前尚不清楚各类犯罪软件与制作和运行这些犯罪软件的组织之间存在的联系。但是与犯罪软件相关的最新消息以及威胁形势的一些重大变化表明，有史以来最大的威胁犯罪组织之一很可能已被击溃，或者至少在较长一段时间内不会再有所活动。

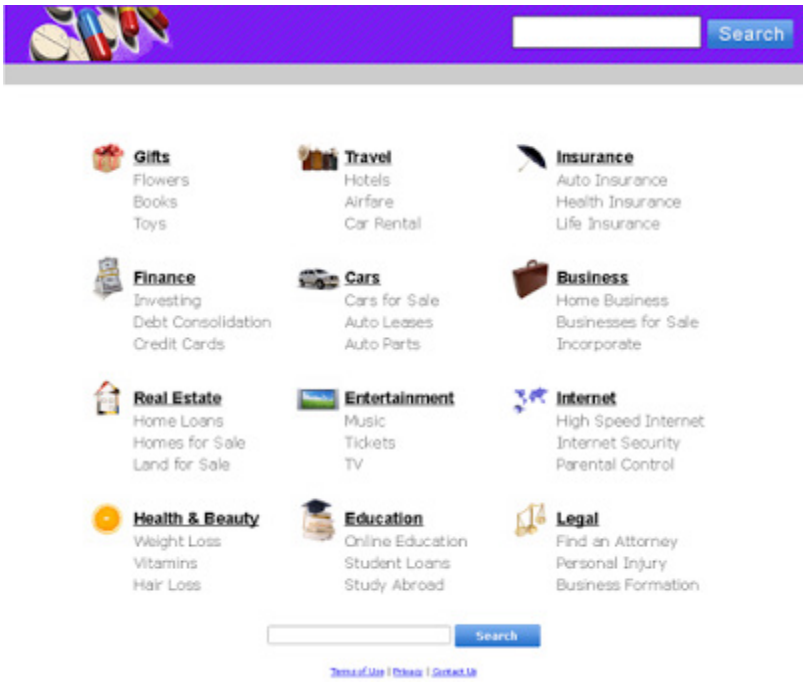
拘捕公告

本月初，一个与恶意软件 Lurk 有关的黑客组织在俄罗斯落网。Lurk 是一款银行木马病毒，其攻击目标主要是俄罗斯的银行。由于该恶意软件仅在俄罗斯活动，所以并没有太多关于该威胁的公开信息。Talos 在调查 Bedep/Angler 攻击者时发现了一些有关 Lurk 以及控制和命令 (C2) 域的蛛丝马迹，我们曾在今年 2 月的卡巴斯基安全分析师峰会上讨论了这些发现，相关公开信息请参阅此处。根据有关此次拘捕行动的公开数据，该黑客组织被指控从俄罗斯多家银行共盗取了约 4500 万美元。

Lurk

因为大量报道称此次拘捕行动与 Lurk 相关，所以本文不再赘述技术层面的内容，而将侧重点放在已确定的 C2 基础设施。根据各种信息来源，我们编制了一份含有超过 125 个 C2 域的列表。

根据这些信息，我们开始调查这些域的 Whois 记录，并发现了一些共性。在已发现的 C2 域中，约 85% 都是注册到 john[.]bruggink@yahoo[.]co[.]uk 这一个注册者帐户名下。已经看过我们的 Bedep 研究报告的读者应该很熟悉这个邮件地址，因为这是与 Bedep 和 Angler 相关的注册者帐户关联的三个邮件地址之一。我们之所以特别关注此特定注册者帐户是因为它在 Angler 的后端通信中扮演着一定角色。我们发现了一个注册到该帐户的域 wittalparuserigh[.]com，此域用于为其中一个 Angler 漏洞攻击服务器传输的负载提供服务。此外，我们还发现该域拥有与将用户重定向到 Angler 实例关联的域，并且最终发现此域在一些 C2 基础设施上托管与 Bedep C2 相同的“默认”网页，以下所示是其中一个示例。



Angler 的影响

目前可以确定的是，Lurk 与 Angler 之间存在一定联系，我们至少可以确定大部分 Lurk 都是通过 Angler 传输至俄罗斯境内的受害者。问题是，该漏洞攻击包是否会因为 Lurk 而受到显著显著影响。如果有，影响程度如何？我们发现，实际影响比我们预计的还要大。在黑客组织落网后一周内，Angler 便已从威胁名单上消失。我们不妨插入一个题外话，来讨论一下这个变化的重要意义。从盈利性、多产性、成功性和复杂性来看，Angler 堪称犯罪软件相关平台之最。据我们过去的研究显示，该平台的使用者仅仅通过使用户感染勒索软件，每年就能获得约 6000 万美元的收入。

这并不是 Angler 第一次消失，它最近一次消失是在今年年初（消失了数周）。然而，有其他迹象表明，这次消失并不像年初那样短暂。最主要的迹象是在攻击入口方面。攻击入口是研究漏洞攻击包活动的一个重要部分，因为攻击入口是负责诱使用户与漏洞攻击包进行交互的机制。在这几周中，我们看到犯罪软件开始从 Angler 大规模迁移至其他漏洞攻击包。从 ElTest 到 Neutrino 的迁移已有详细介绍。此外，笔者还发现自己在 Hack In The Box（黑客暨安全大会）上谈到的攻击入口（影子入口）从 Angler 迁移到 Rig 和 Neutrino。记得就在一年多以前，笔者就曾发现该攻击入口被用于托管 Angler 的证据，随后该攻击入口突然发生了转移。

现在，大多数大规模攻击入口已经转移到 Rig 或 Neutrino，而年初 Angler 消失时并未出现这种情况。另据 Kafeine 报告，潜在漏洞使用者使用这些漏洞攻击包的成本也有所上升，这个迹象再次表明一个重要参与者已经退出舞台。值得注意的是，犯罪软件正在转向的漏洞攻击包列表中没有发现 Nuclear。就在 Talos 和 Checkpoint 公布两个不同的研究项目之后不久，Nuclear 也悄然不见。Angler 是第一个与 Lurk 几乎同时消失的全球主要威胁，但绝不是唯一一个。

Necurs

一个针对特定地区的银行木马与最大也最复杂的漏洞攻击包同时消失是一件大事，但是研究有更多发现。在 2 月份的回溯研究期间，我们发现与 Necurs 关联的几个 C2 域属于同一个 John Bruggink 注册者帐户。几乎是在与 Lurk 和 Angler 消失的同时，Necurs 僵尸网络也消失了。这个僵尸网络被公认为世界上最大的僵尸网络。另外几个活跃的犯罪软件威胁也随着此僵尸网络的消失而遭受重挫。Necurs 的消失对 Dridex 和 Locky 的传播产生了显著影响，Talos 发现 Dridex 和 Locky 的活动都显著减少。Locky 的活动减少到非常低的水平，以至于总体看来它已被淘汰出局。似乎它们的大部分传播都依赖于 Necurs 僵尸网络。

Necurs 复苏

最近，我们其中一些威胁有死灰复燃的迹象。Necurs 僵尸网络恢复了活动，并且被用于传输 Locky 和 Dridex。它消失了大约三周，但是它的出现再次表明，这些威胁带来的暴利足以让犯罪分子不甘沉寂。经过一段时间之后，这些受到抑制或者消失的主要威胁很可能会卷土重来。

威胁形势的剧烈变化

我们没有办法确定所有这些威胁是否都存在联系，但是可以看到，与所有这些威胁关联的域都属于同一个注册者帐户。如果是同一个组织实施了所有这些活动，那么此次拘捕可能成为网络犯罪历史上最重大的拘捕行动之一，它挫败了一个能够轻松获取数亿美元的犯罪组织。

但是就像我们过去观察到的那样，美好时光不会持续很久。每当这种规模的组织被挫败的同时，都会形成真空。所有威胁都会以某种形式回归，而且会从前人的错误中吸取教训。

一个最好的例子就是，Blackhole 漏洞攻击包的制作者被拘捕后，在一段时间内，漏洞攻击包之间围绕冠军宝座展开了激烈竞争。这最终导致了 Angler 的兴起。Angler 吸取了各种漏洞攻击包的精妙之处，就下载量而言达到了超越 Blackhole 的高度。我们预计，如今随着 Angler（还可能包括 Nuclear）从威胁名单中消失，同样的情况将会再度上演。其他知名度稍逊的

攻击包很可能会试图填补空白，可以看到 Rig 和 Neutrino 已经开始了这样的尝试。此外，新的攻击包很可能已在开发。

可以确定的是，除了利用这些技术的各种攻击方式和不同的攻击者外，很可能还会有一个小得多的组织在恶意软件领域中扮演着超出我们预料的重要角色。无论如何，过去几周以来，与犯罪软件相关的威胁形势发生了显著改变，在未来几个月我们会继续密切观察它的反应和演变。

发布者：NICK BIASINI；发布时间：11:01

标签：僵尸网络、犯罪软件、漏洞攻击包、勒索软件、TALOS