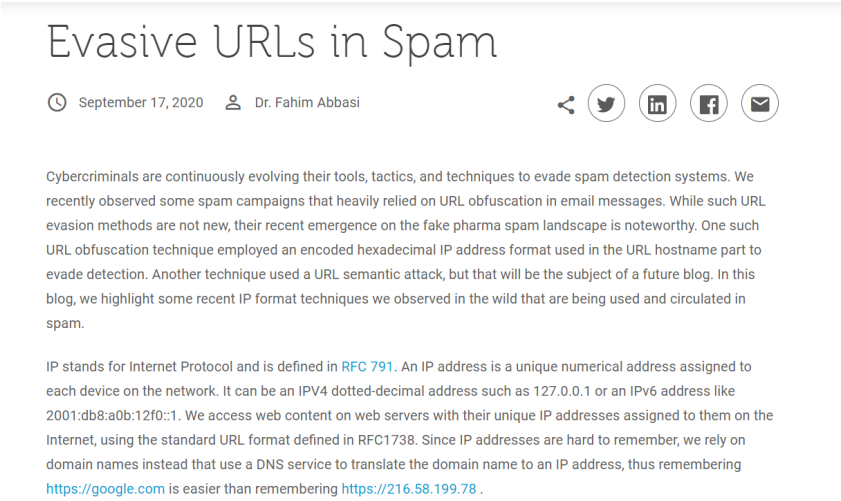
[译] APT分析报告：02.钓鱼邮件网址混淆URL逃避检测

原创 Eastmount 2020-09-22 17:07:35 3649 收藏 3 编辑 版权

分类专栏： 网络安全自学篇 安全攻防进阶篇 APT分析及溯源 文章标签： APT攻击 分析报告 网络安全 钓鱼邮件 逃逸检测

这是作者新开的一个专栏，主要翻译国外知名的安全厂商APT报告文章，了解它们的安全技术，学习它们溯源APT组织的方法，希望对您有所帮助。前文分享了Linux系统下针对性的APT攻击及技术要点，这篇文章将介绍钓鱼邮件网址混淆URL逃避检测，钓鱼是APT攻击中常用的手段，它究竟怎么实现混淆呢？



Evasive URLs in Spam

September 17, 2020 Dr. Fahim Abbasi

Cybercriminals are continuously evolving their tools, tactics, and techniques to evade spam detection systems. We recently observed some spam campaigns that heavily relied on URL obfuscation in email messages. While such URL evasion methods are not new, their recent emergence on the fake pharma spam landscape is noteworthy. One such URL obfuscation technique employed an encoded hexadecimal IP address format used in the URL hostname part to evade detection. Another technique used a URL semantic attack, but that will be the subject of a future blog. In this blog, we highlight some recent IP format techniques we observed in the wild that are being used and circulated in spam.

IP stands for Internet Protocol and is defined in RFC 791. An IP address is a unique numerical address assigned to each device on the network. It can be an IPV4 dotted-decimal address such as 127.0.0.1 or an IPv6 address like 2001:db8:a0b:12f0::1. We access web content on web servers with their unique IP addresses assigned to them on the Internet, using the standard URL format defined in RFC1738. Since IP addresses are hard to remember, we rely on domain names instead that use a DNS service to translate the domain name to an IP address, thus remembering https://google.com is easier than remembering https://216.58.199.78 .

- 原文标题：Evasive URLs in Spam
- 原文链接：https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/evasive-urls-in-spam/
- 作者时间：By Dr. Fahim Abbasi on September 17, 2020
- 文章来源：Trustwave

国外研究人员最近发现一些垃圾邮件活动非常依赖于电子邮件中的URL混淆。其中一些仿冒制药的垃圾邮件活动从7月中旬开始，采用了URL主机名部分使用编码十六进制IP地址格式来逃避检测。这些通过混淆的链接地址包含在垃圾邮件中，当受害者访问时将打开受害者的链接，浏览器将十六进制IP转换为十进制IP，并将受害者带到伪造药品网站的托管网页。

文章目录

一.URL混淆技术

网络攻击者正在不断发展其工具、策略和技术，以逃避垃圾邮件检测系统。 我们最近发现一些垃圾邮件活动非常依赖电子邮件信息中的混淆URL。虽然这种URL规避方法并不新鲜，但它们最近在假冒医药垃圾邮件领域的出现值得关注。 主要包括两种类型：

- 一种URL混淆技术使用了URL主机名部分中使用的十六进制IP地址编码格式来逃避检测
- 另一种技术使用了URL语义攻击，这将成为未来博客的主题

在本文中，我们将重点介绍一些我们观察到的最近的IP格式技术，这些技术正以垃圾邮件的形式被使用和传播。

IP代表互联网协议，在RFC 791中定义。IP地址是分配给网络上每个设备的唯一数字地址。它可以是IPV4的十进制地址，比如127.0.0.1，或者是IPv6地址，比如2001:db8:a0b:12f0::1。我们使用RFC1738中定义的标准URL格式访问Web服务器上的Web内容，并在Internet上为其分配了唯一的IP地址。由于IP地址很难记住，我们依靠域名来代替，使用DNS服务将域名转换为IP地址，因此记住https://google.com比记住https://216.58.199.78更容易。

从技术上讲，IP地址可以用多种格式表示，因此可以在URL中使用，如下所示：

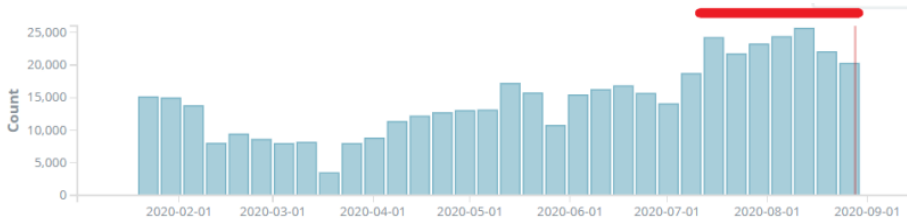
- **https://216.58.199.78**
  点分十进制IP地址，此示例使用Google.com的IP
- **https://0330.0072.0307.0116**
  八进制IP地址，将每个十进制数字转换为八进制
- **https://0xD83AC74E**
  十六进制IP地址，将每个十进制数字转换为十六进制
- **https://3627730766**
  整数或DWORD IP地址，将十六进制IP转换为整数

虽然网络浏览器接受域名或十进制IP作为地址栏的URL，但点击上面的任何链接将把你导向Google.com，因为大多数浏览器也接受这些不同的IP格式，当然它们是有效的。浏览器将自动将十六进制或其他IP格式转换为十进制的IP地址，并浏览到该IP地址的最后一页。

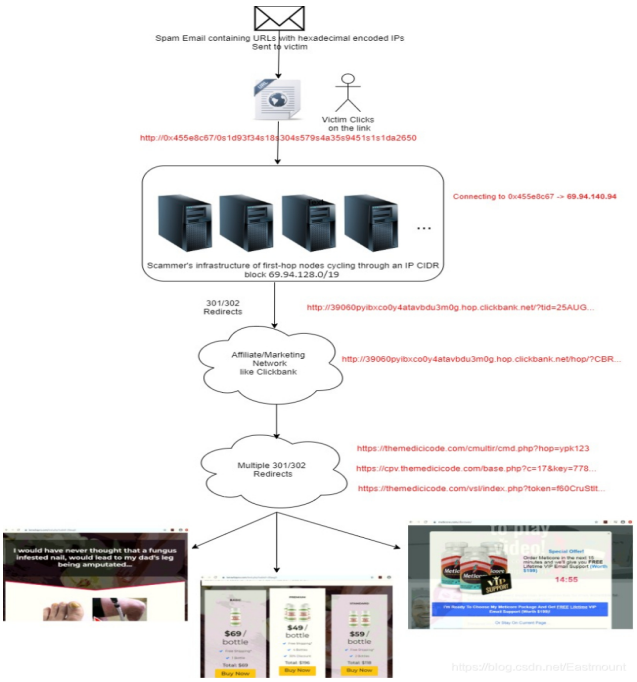
任何具备这方面知识的威胁行动者都可以制作一个看起来模糊的URL，就像上面显示的那样，通过电子邮件发送，并带有令人信服的信息来欺骗电子邮件网关和受害者，诱使他们点击并打开一个由攻击者控制的网站。

二.使用包含十六进制IP的混淆URL垃圾邮件

我们观察到第一个垃圾邮件活动是一个非常活跃的假冒制药垃圾邮件僵尸网络利用URL混淆技术的结果，该技术由联盟中继服务通过多个中间跳跃的基础结构提供支持，以逃避检测，同时传播大量的垃圾邮件。这些垃圾邮件涵盖范围广泛的医药产品，主要是胆固醇、抗真菌、抗衰老、抗炎、大脑健康、新陈代谢等药物。这个垃圾僵尸网络从2020年7月中旬开始在URL中使用十六进制IP，如下图所示，这个僵尸网络产生的垃圾邮件数量显著增加。



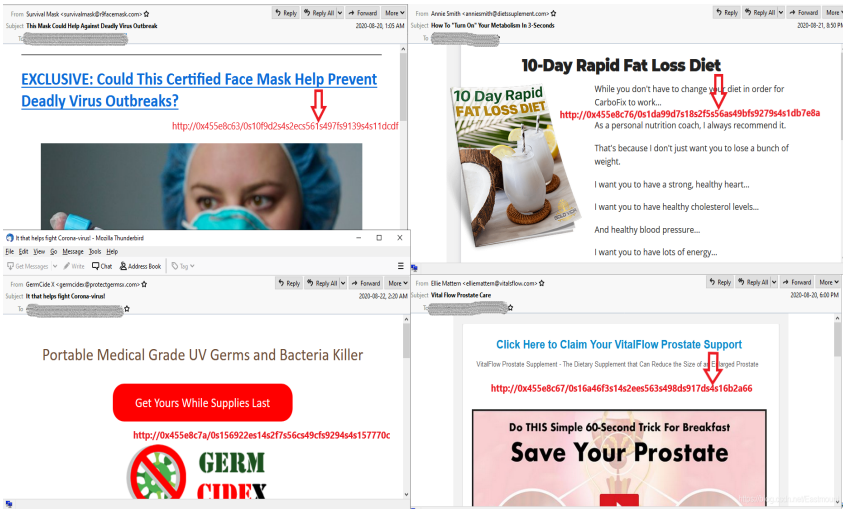
上图表示自今年年初以来假冒制药僵尸网络的垃圾邮件数量，请注意自7月中旬以来成交量逐渐上升。下图显示了虚JIA药物垃圾邮件活动的流程图，随后是有关每个组件的详细讨论。



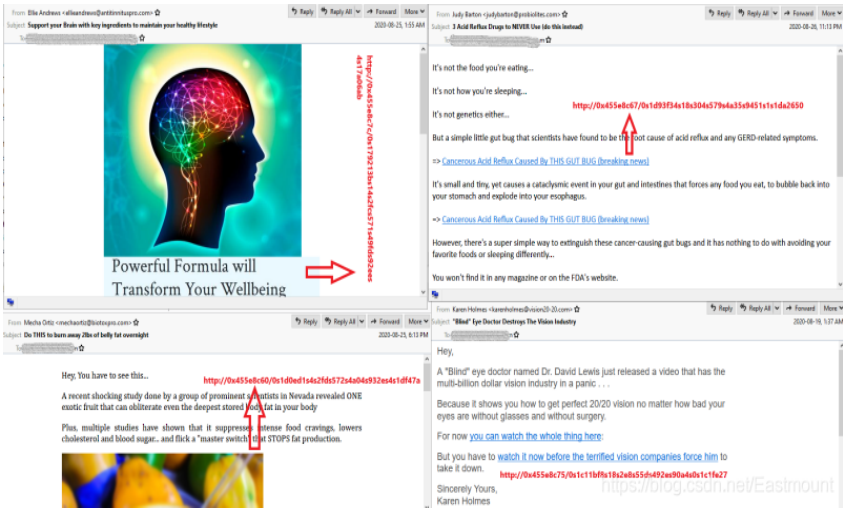
三.垃圾邮件分析

垃圾邮件是为每个垃圾邮件广播精心制作的，其中电子邮件主题突出了电子邮件的正文内容，并且大多具有令人信服的与药品相关的消息。下面是一些垃圾邮件的截图。

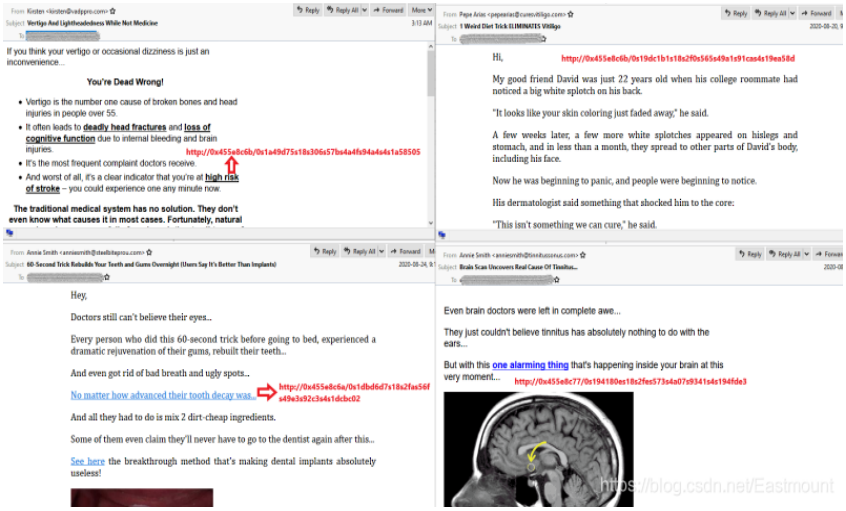
下图展示包含十六进制IP的嵌入式URL的垃圾邮件样本，该僵尸网络以COVID口罩、减脂、紫外线细菌杀手和前列腺药物等主题传播垃圾邮件。



下图垃圾邮件的主题有促进大脑的药物、胃酸反流、减少脂肪和视力矫正等。



下图垃圾邮件的主题包括眩晕药、白癜风、口香糖和大脑，所有URL均包含十六进制IP。



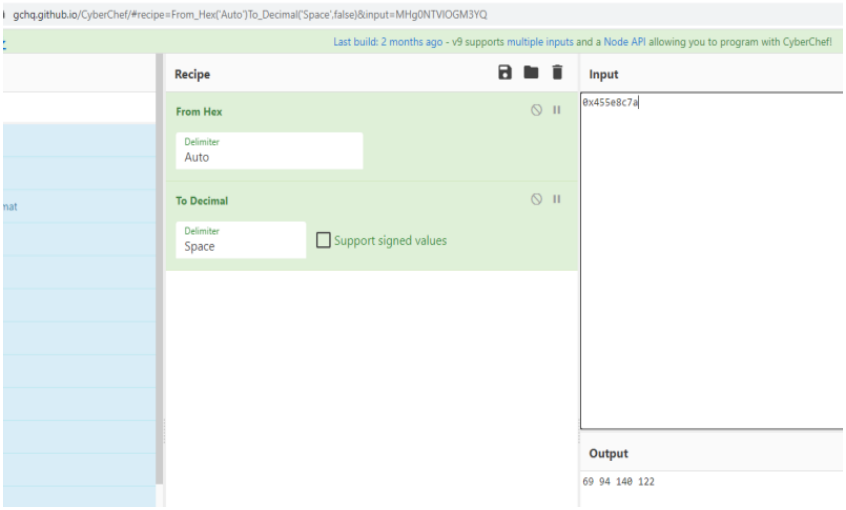
这看起来像普通的垃圾邮件，但是它的独特之处在于它在URL中使用了十六进制ip来访问药丸垃圾邮件网页。我们从这些药丸垃圾邮件活动中收集的一些URL进行了伪造并在此处列出：

```
hxxp://0[x]455e8c6f/0s19ef206s18s2f2s567s49a8s91f7s4s19fd61a
hxxp://0[x]455e8c65/0s1598270s14s2eds562s498as9151s4s15a65b2
hxxp://0[x]455e8c6c/0s4eb49s4s2e4s557s491fs904fs4s5ccfa
hxxp://0[x]455e8c7a/0s30360s4s2f7s56cs49d2s9293s4s3e830
http://0[x]455e8c67/0s1d93f34s18s304s579s4a35s9451s1s1da2650
http://0[x]455e8c75/0s1c11bf8s18s2e8s55ds492es90a4s0s1c1fe27
http://0[x]455e8c7c/0s179213bs14s2fcs571s49fds92ees4s17a06ab
http://0[x]455e8c77/0s194180es18s2fes573s4a07s9341s4s194fde3
http://0[x]455e8c6a/0s1dbd6d7s18s2fas56fs49e3s92c3s4s1dcbc02
```

这些十六进制编码的IP地址是在2020年8月的不同时间收集的，接着解码成一个单独的CIDR块 69.94.128.0/19，这是一个来自美国的IP块。我们观察到，这些链接在使用不同的邮件客户机时略有不同。例如，使用Thunderbird邮件客户端，将鼠标悬停在这些垃圾邮件中的链接上，会将它们显示为状态栏中以IP地址开头的URL。但是，这些链接使用Microsoft Outlook以十六进制IP形式出现在URL中，复制和粘贴这些链接会将它们转换为URL中的标准IP格式。

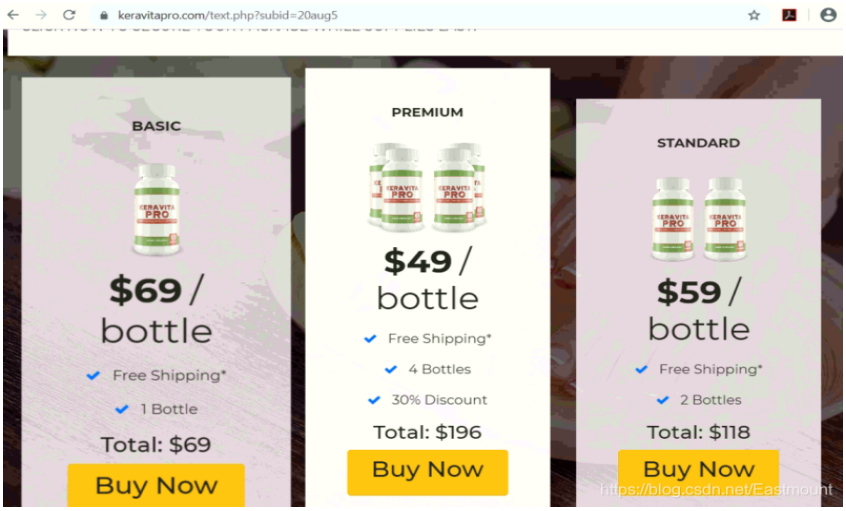
四.钓鱼网络分析

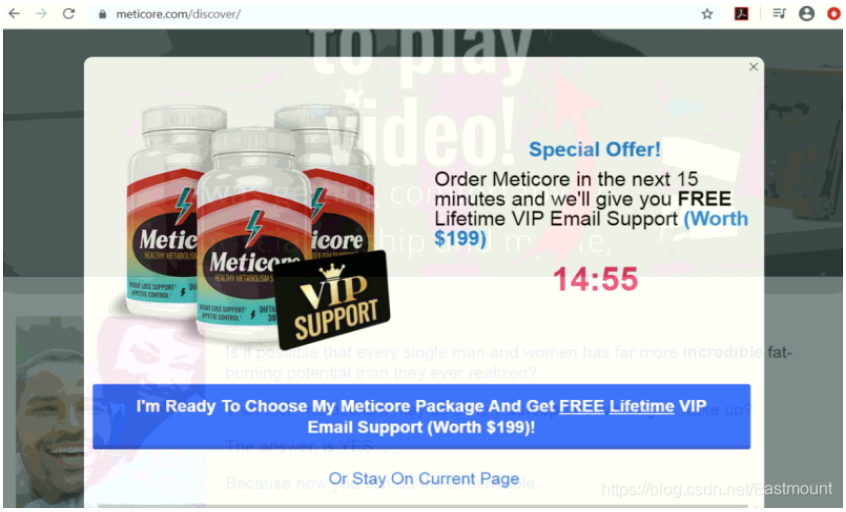
单击这些链接中的任何一个都会打开受害者的浏览器。该浏览器将十六进制IP转换为十进制IP，并将受害者带到该假冒制药网站的网页上。这个网站配备了一个电子商务门户来销售这些JIA药。在写这篇博客的时候，我们尚未进行任何购买。您可以使用任何工具执行十六进制到十进制的IP转换。下面是一个使用Cyber Chef的简单转换，它将十六进制IP转换为十进制IP。



对网络流的分析，从受害者单击链接到最终登陆页面加载到受害者的浏览器中，显示了一系列中间HTTP 301和HTTP 302重定向。这里需要注意的一件事情是，攻击者利用了Clickbank.com的基础设施，这是一个合法的在线零售和附属服务。网络罪犯滥用Clickbank附属链接服务，通过代理到达所售药品的最终登陆页面。

对于该僵尸网络中的每次垃圾邮件攻击迭代，最终的登录页面都遵循初始垃圾邮件中相同的主题。最终的登录页面被设计为与第三方支付网关集成的营销和销售门户。每个网站都包含令人信服的营销视频和推荐，以诱使受害者购买JIA药或销售的药品。这里要注意的一件有趣的事是，托管最终登录页面的大多数域都是在Name Cheap域名注册商注册，并且是最近注册的。下图显示以垃圾邮件形式分发的虚JIA抗真菌药物的登录页面。





对于电子商务零售流，这些网站使用JavaScript片段指向Clickbank.com附属网络和支付门户，如图所示。

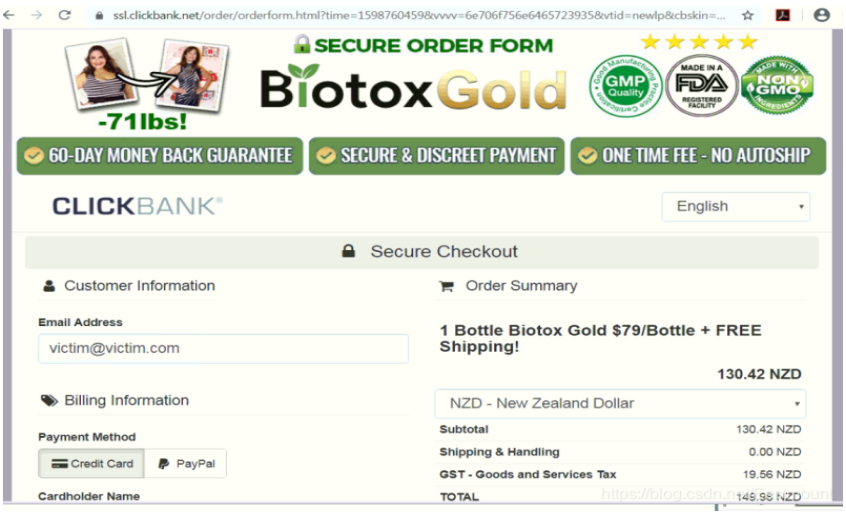
```
        <p>For Order Support, please contact ClickBank <a href="https://www.clkbank.com/#!/" class="txt--blue underline-hover"
target="_parent" rel="noopener"><strong>HERE</strong></a></p>
    </div>
    <p><i>*The name "Tonya Harris" used in this video is a pen name and is used for marketing purposes only and to protect the
authors identity</i>
    <p><i>ClickBank is the retailer of products on this site. CLICKBANK® is a registered trademark of Click Sales Inc., a Delaware
corporation located at 1444 S. Entertainment Ave., Suite 410 Boise, ID 83709, USA and used by permission. ClickBank's role as
retailer does not constitute an endorsement, approval or review of these products or any claim, statement or opinion used in
promotion of these products.</p>
</div>

<script data-cfasync="false" src="/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js"></script><script
src='https://cbtb.clickbank.net/?vendor=npounder95'></script>    </div>
</div>

<script src="https://player.vimeo.com/api/player.js"></script>

<script src="/assets/js/video-settings.js?v=1.0.6"></script>
<script>
    mainPage();
</script>
</body>
</html>
```

当受害者单击任何产品的“立即购买”按钮，将重定向到合法的Clickbank付款网关页面，该页面通过信用卡和PayPal接受付款，如图所示。



尝试使用伪造的付款详细信息来支付商品是失败的，因为支付网关要求在进入下一页之前输入合法的有效信用卡。但检测购买是否有任何产品发货不属于本研究的范围。

五.结论

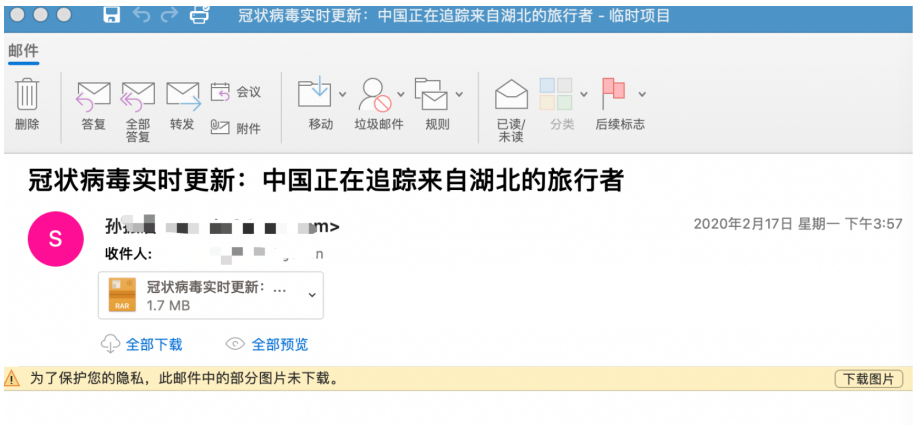
垃圾邮件发送者正在不断改进他们逃避垃圾邮件检测系统的方法，从而将垃圾邮件传递给受害者。一个垃圾邮件组织最近开始混淆URL以逃避检测，其方法是使用含有嵌入在垃圾邮件中的十六进制编码IP的URL，用于他们的假冒制药垃圾邮件活动，从而逃避垃圾邮件检测系统和URL黑名单。这些URL指向垃圾邮件控制的基础设施，这些基础设施将受害者重定向到半合法的在线零售商和营销公司基础设施，最终重定向到销售假药、药品和保健产品的网站，并且这些假药网站的主机是最近购买的域名。Trustwave安全电子邮件网关（SEG） 检测到这些垃圾邮件。我们建议所有用户在单击之前仔细查看所有URL，查看其是否符合常规格式的URL。

安全建议：

- 对相关指示器进行阻断
- 提高个人安全意识，不要点击不明来源或可疑邮件中的链接
- 谨慎不符合常规格式的URL

疑问及后续研究：

- 作者能够成功实现IP访问网页，但十六进制IP如何访问，是浏览器自带解析功能吗？是否存在局限性。
- APT组织中广泛使用钓鱼邮件，比如海莲花、摩诃草、蓝宝菇等，下一步作者会总结常见的钓鱼方法。
- 如何通过技术实现一个简单的钓鱼功能，如果读者需要，作者会尝试复现相关的功能，让大家了解钓鱼背后的原理知识。



IOCs：

```
hxxp://0[x]455e8c6f/0s19ef206s18s2f2s567s49a8s91f7s4s19fd61a
hxxp://0[x]455e8c65/0s1598270s14s2eds562s498as9151s4s15a65b2
hxxp://0[x]455e8c6c/0s4eb49s4s2e4s557s491fs904fs4s5ccfa
hxxp://0[x]455e8c7a/0s30360s4s2f7s56cs49d2s9293s4s3e830
http://0[x]455e8c67/0s1d93f34s18s304s579s4a35s9451s1s1da2650
http://0[x]455e8c75/0s1c11bf8s18s2e8s55ds492es90a4s0s1c1fe27
http://0[x]455e8c7c/0s179213bs14s2fcs571s49fds92ees4s17a06ab
http://0[x]455e8c77/0s194180es18s2fes573s4a07s9341s4s194fde3
http://0[x]455e8c6a/0s1dbd6d7s18s2fas56fs49e3s92c3s4s1dcbc02
```

前文分享：

- [译] APT分析报告：01.Linux系统下针对性的APT攻击概述

2020年8月18新开的“娜璋AI安全之家”，主要围绕Python大数据分析、网络空间安全、人工智能、Web渗透及攻防技术进行讲解，同时分享CCF、SCI、南核北核论文的算法实现。娜璋之家会更加系统，并重构作者的所有文章，从零讲解Python和安全，写了近十年文章，真心想把自己所学所感所做分享出来，还请各位多多指教，真诚邀请您的关注！谢谢。

(By:Eastmount 2020-09-22 星期二 晚上10点写于武汉 http://blog.csdn.net/eastmount/)