2017 年 5 月 3 日，星期三

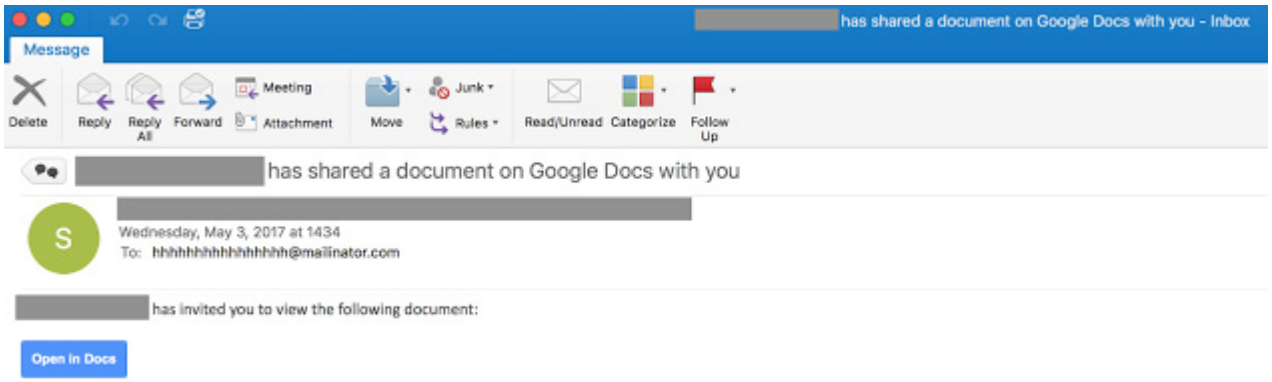
Gmail 蠕虫需要借您之力，而您似乎也的确给予一臂之力

作者：Sean Baird 和 Nick Biasini

攻击者一直不断翻新手法向受害者发送大量垃圾邮件。一种生存期较短但分布广泛的网络钓鱼活动以 Google 云端硬盘为主题，已影响了各类垂直行业的大量用户。此攻击活动在将邮件发送至 hhhhhhhhhhhhhhhh@mailinator[.]com 的同时密件抄送至攻击目标，而且为了让邮件看似合法，发件人会伪装成地址簿中含有攻击目标的某人。

Mailinator 是一个“免费的公共邮件系统，您可以在其中使用所需的任何收件箱”，它常用于一次性帐户。在本例中，垃圾邮件发送者可能利用了相关 Mailinator 收件箱来监控邮件是否发送成功。然而，此攻击活动的独特之处并不在于使用 Mailinator。

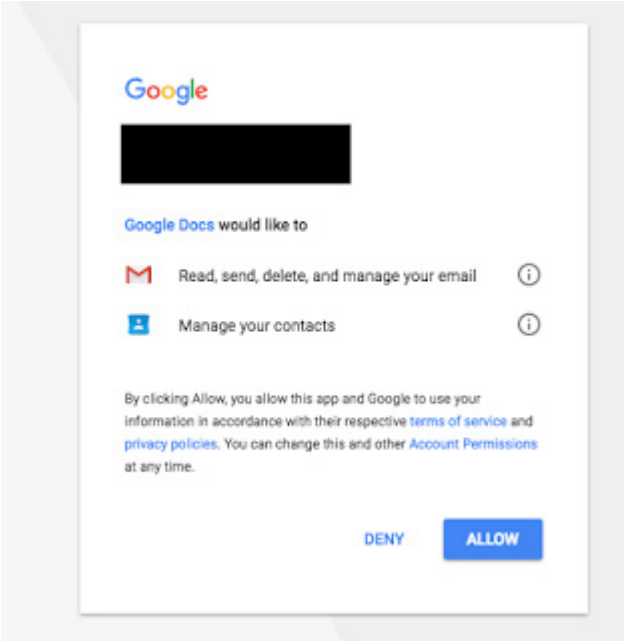
攻击活动详细信息



恶意邮件

正如您所看到的，该邮件是非常标准的网络钓鱼攻击尝试。在本例中，它们专门将 Google 作为攻击目标，并通过 Google Docs 发起攻击。通常，您会看到一个指向“克隆”站点的链接，该链接用于获得目标服务的用户名和密码，在本例中目标服务是 Google。不过，此攻击活动采用了截然不同的方法。

邮件中包含的“在文档中打开”链接将收件人指引到合法的 Google 站点，登录该站点需要使用 Google 凭证。进入站点后，一项名为“Google Docs”的服务请求获取“读取、发送、删除和管理”邮件与联系人的权限。这是一项合法请求，许多利用 Google 作为身份验证机制的应用都会发出这类请求。不正常的部分在于请求的权限。

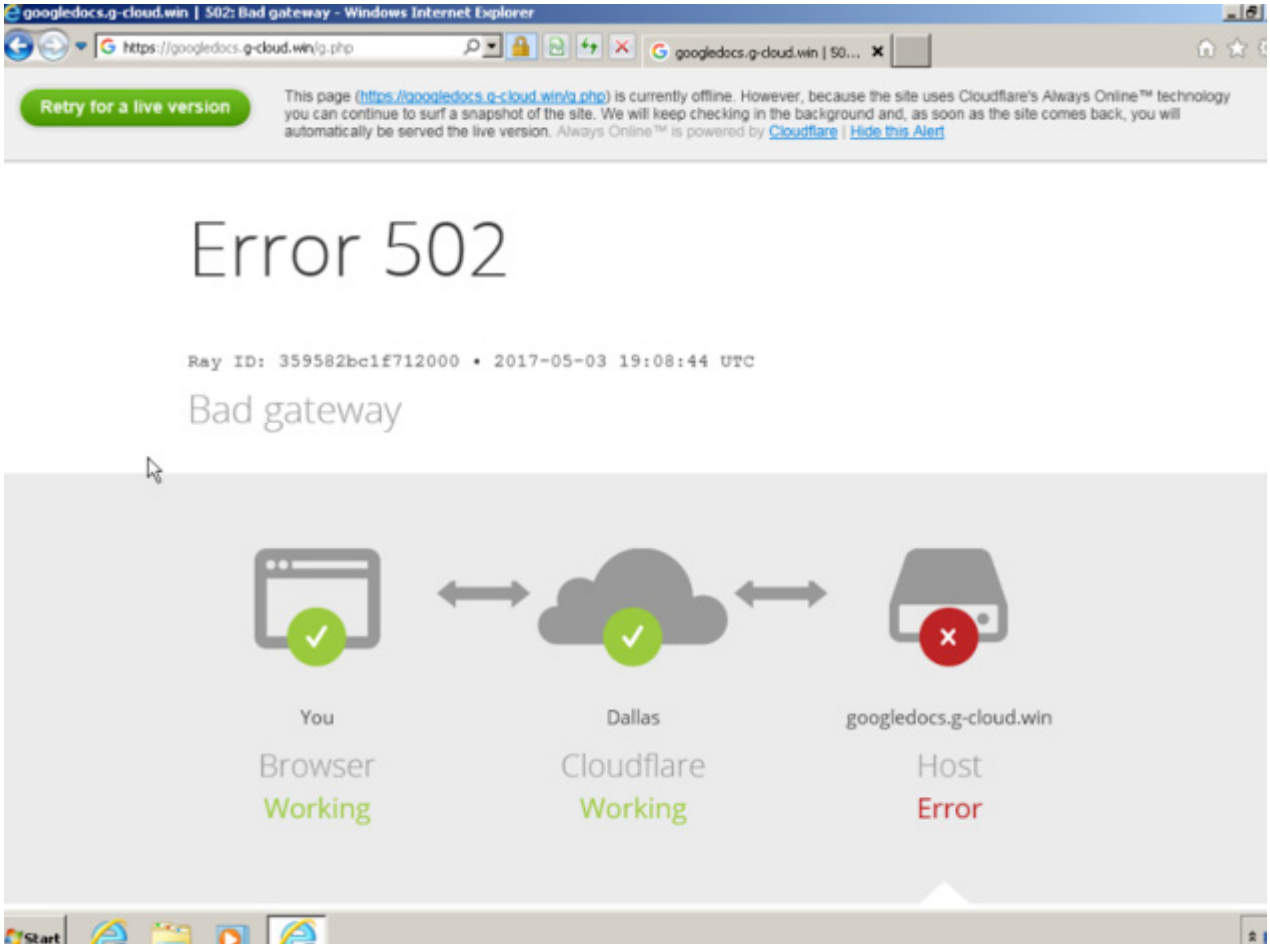


名为“Google Docs”的 OAuth 服务请求获得权限

点击“允许”（并等待很长时间）后，系统将页面定向到 h[xx]ps://googledocs[.]g-cloud[.]win/。在此攻击中，我们还发现了其他几个恶意主机，包括：

- docscloud[.]download
- docscloud[.]info
- docscloud[.]win
- gdocs[.]download
- docscloud[.]info
- g-docs[.]pro
- gdocs[.]pro
- gdocs[.]win
- docscloud[.]download
- g-cloud[.]win
- g-cloud[.]pro

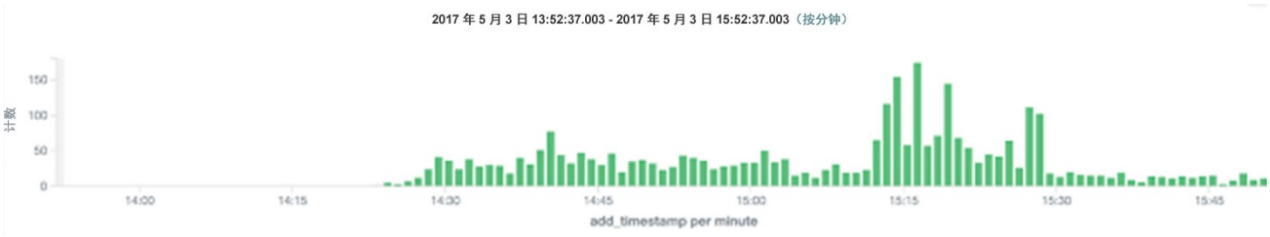
目前，这些请求会引发 HTTP 502 响应。出现这种情况的原因在于同时尝试访问站点的用户过多，或者 Cloudflare 已撤下受影响的站点。



目标页面上出现 502 错误。

Talos 能够识别用户与页面进行交互和接收数据的其他实例。对此数据进行简要分析，未返回任何本身含有恶意的内容，比如真正的恶意负载，或指示其他凭证盗窃行为的 POST 请求。

此攻击之所以引人注意纯粹是因为它的执行数量和速度。开始只是少量邮件，但之后急剧增长，泛滥于 Twitter 和安全社区的主要关注区域。其疯狂性引起了所有人的注意。



攻击后大约两小时（美国东部时间）内我们收到的报告量。

目的

此攻击可能有双重目的。此实例作为通过 OAuth 发起的诱导性 Google 网络钓鱼的潜在概念验证。另外，更令人担忧的是，此攻击允许 OAuth 所有者访问每个攻击受害者的所有邮件内容和联系人信息。这意味着攻击者可能有权访问您帐户中的所有信息，并且能够读取、发送、删除和管理关联帐户的邮件和联系人。此外，由于使用了 OAuth，更改密码等常规保护措施无法立即阻止攻击者访问。

降低风险和提供保护

由于此攻击取得成功，我们在短期内很可能还会发现这种性质的网络钓鱼攻击。用户在点击内容时必须非常谨慎，特别是在要求输入密码或授予某些类型的权限或访问权限时更要加倍小心。如果无法确定，请使用非邮件方式联系附件或链接的发件人，验证邮件的真实性。

如果您不幸落入此攻击的圈套，应当转到 Google 帐户设置，撤销这种假冒的恶意 Google Docs 服务的权限。然后，您应立即更改密码。

此外，由于攻击者可以访问您的所有邮件内容，因此您应采取措施防范身份盗窃和勒索之类的次要攻击。

IOC

域：

- docscloud[.]download
- docscloud[.]info
- docscloud[.]win
- gdocs[.]download
- docscloud[.]info
- g-docs[.]pro
- gdocs[.]pro
- gdocs[.]win
- docscloud[.]download
- g-cloud[.]win
- g-cloud[.]pro

结论

攻击者非常小心谨慎，总是千方百计地寻找新的攻击手段，向终端用户投递垃圾邮件或恶意软件。这只是攻击者为达到此目标而采用的狡猾方式的最新例子。与其他翻新的手法一样，它很可能眨眼之间就会被大量复制。Google 只是一个例子，攻击者也可能利用其他服务作为替代身份验证机制。Facebook 和 LinkedIn 可能会成为两个候选目标。除了继续将 Google 作为攻击媒介之外，以后还很有可能出现利用此类凭证的类似攻击。

思科 Cloudlock 已确定超过 27.5 万个 OAuth 应用连接到 Microsoft Office 365 等核心云服务。相比之下，3 年前这类应用只有 5500 个。未来有可能出现利用此类凭证的类似攻击，而且攻击者将继续利用 Google 作为攻击媒介。有关 Cloudlock 的详细信息及其对于此类威胁的看法，请点击此处访问他们的博客。

另一件不容忽视的事情是，攻击者可能并未料想到此类攻击的速度。此次攻击波及范围很广，随后可能会出现精细的小范围攻击。这再次让人们注意一些基本的安全原则。例如，不轻信邮件（无论看起来是否合法），不允许第三方访问您的任何帐户。如果可以选择使用现有的第三方帐户登录或者创建新帐户，请创建新帐户。这可能要多花一点时间，但可以防止您的邮件和联系人遭受灾难性危害。

防护

产品	防护
AMP	✔
Cloudlock	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

Cloudlock，我们的 CASB 解决方案，专用于识别、分类和降低与连接 OAuth 的应用相关的风险。

CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

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。

IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）

发布者：NICK BIASINI；发布时间：17:28
标签：网络钓鱼、TALOS、威胁研究