Web应用安全

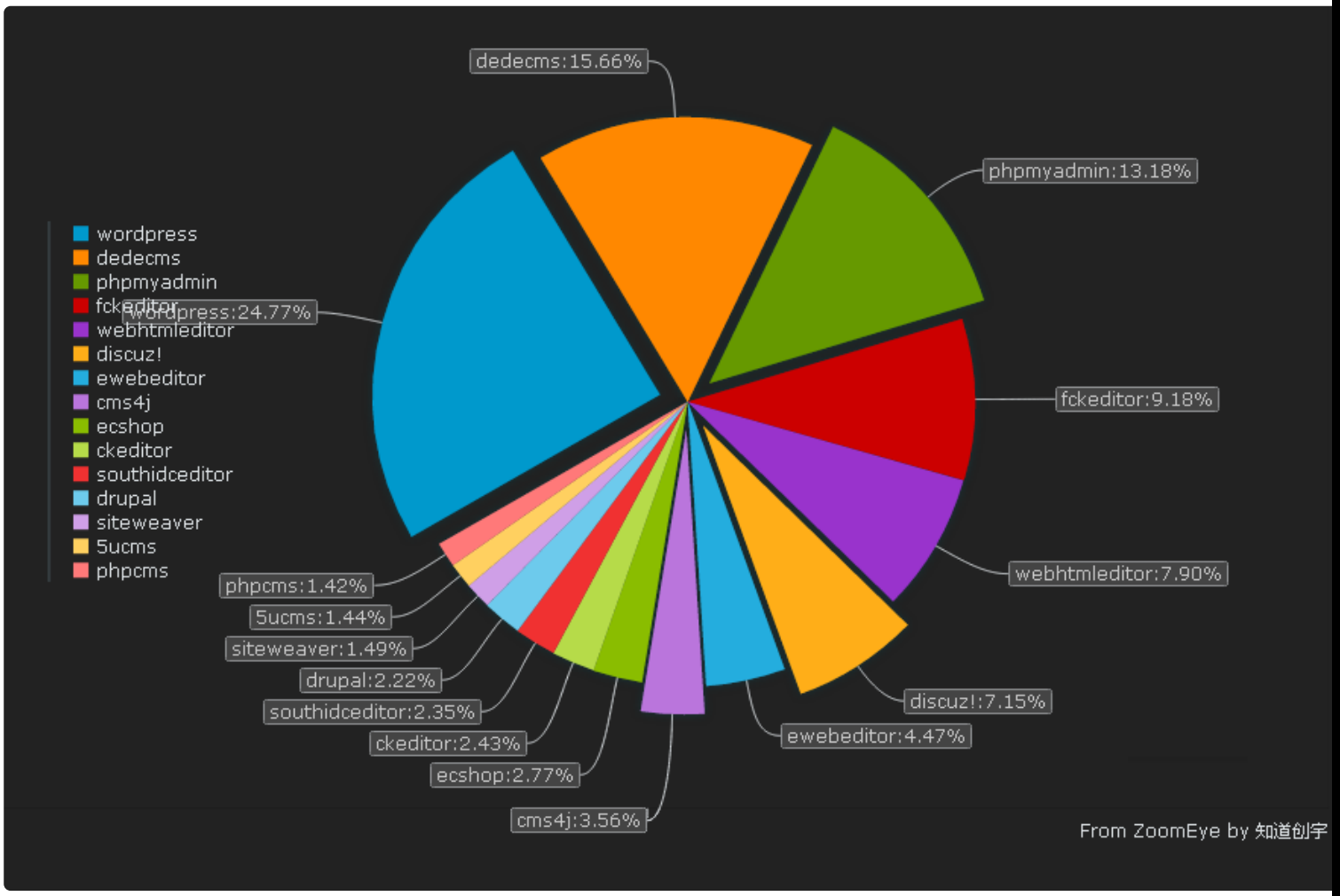
辉煌下的隐忧

——— 知道创宇科技 梁伟

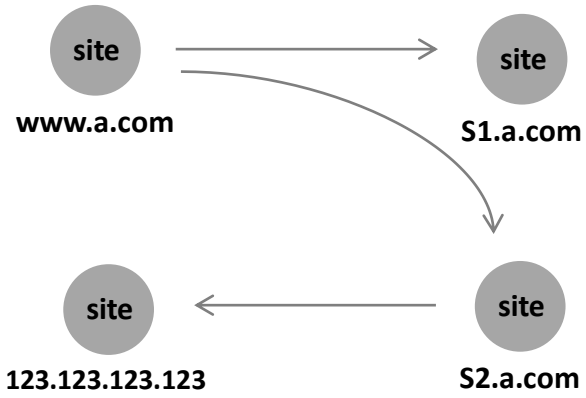
KNOWNSEC TECH

- **挑战：** 业务之杂
- **大数据：** 手段之乏
- **APT：** 度量之困

挑战： 业务之杂



挑战： 业务之杂



主站 www.a.com

子站 S1.a.com

子站 S2.a.com

C 段 123.123.123.123

（与 S2.a.com 同C段）

Step 1 Database takeover（123）

Step 2 进入S2 admin 后台

Step 3 S2 admin 后台注入（AJAX）

Step 4 使用S1数据穷举S2数据

Step 5 利用业务账号登陆 拿下S1后台

Step 6 S1 getshell / 与 www 同主机

大数据： 手段之乏

反思

Big Data ： 手段 还是 技术？

沉迷于堆砌 而弱化 挖掘

执着于积累 而忘记 初衷

大数据： 手段之乏

Payload 优先策略

admin / manage / webback ？

大数据： 手段之乏

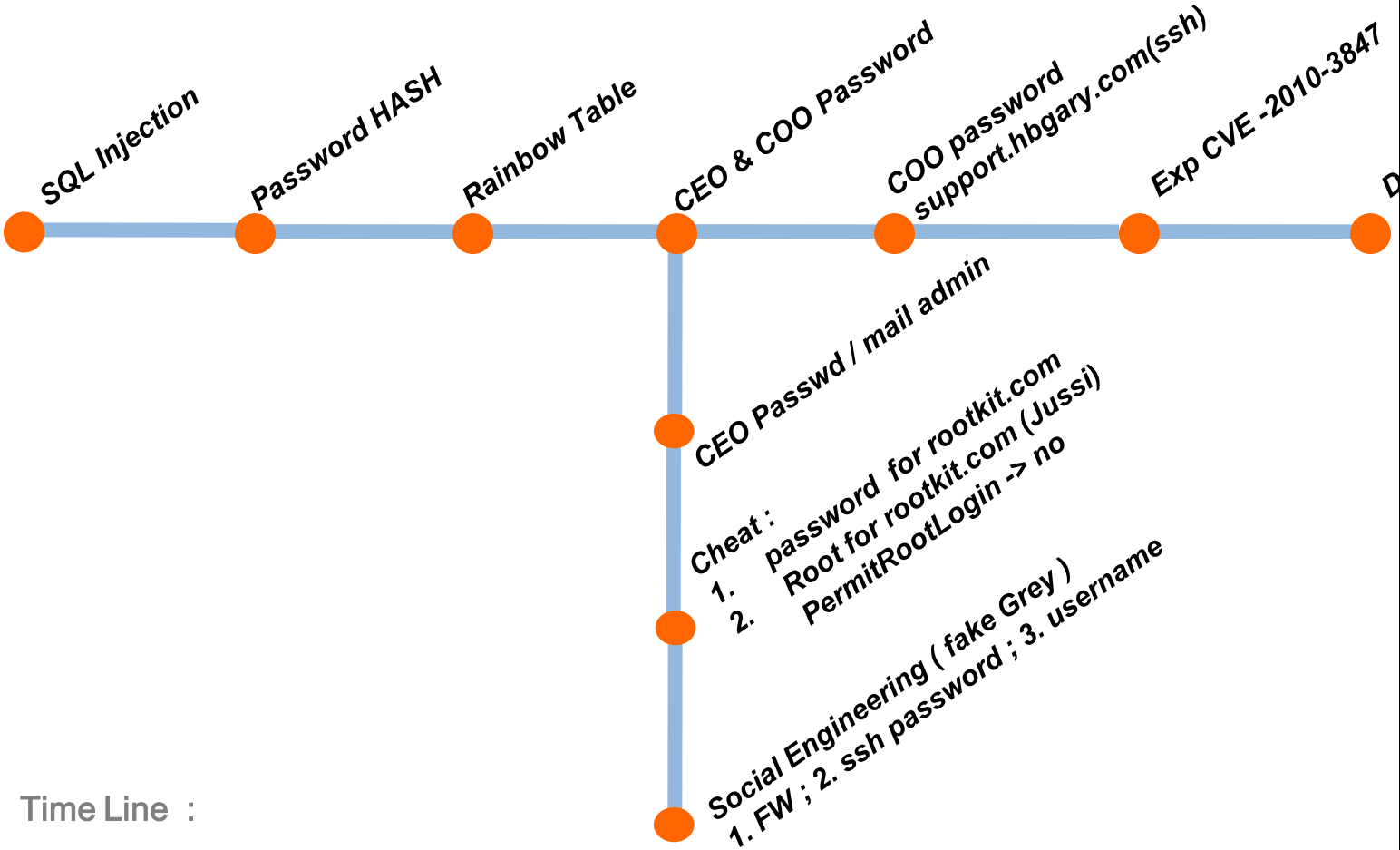
面向 **黑客** ？

面向 **规则** ？

GAC-HK-000018(等级3)

黑客编号	GAC-HK-000018
等级评定	3
所在地区	218.48.219.[redacted]- 韩国 HTI - 探测到代理服务
	220.90.156.[redacted]- 韩国 首尔市 国民大学
	219.80.229.[redacted]- 台湾省 台中县 - 探测到代理服务
性别定位	男（57%）
常用语言	ko-KR; en-US
年龄范围	18 - 29
使用工具	WVS, APPSCAN(IBM), Chrome, IE8, IE9, Havij
操作系统	Windows XP, Windows7, Linux
历史攻击	2012-04-12 - www[redacted]com
	2012-07-02 - www[redacted].cn
	2012-07-17 - www[redacted]com
最近攻击	2012-07-17 01:34:52 - www[redacted]com

APT ： 度量之困



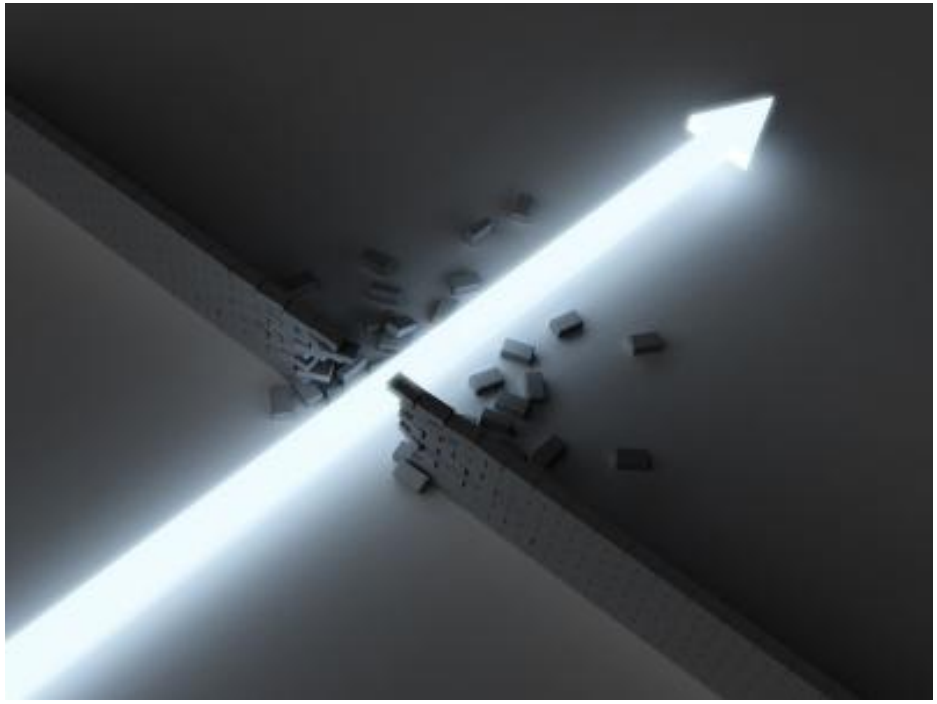
Time Line ：

Anonymous vs HBGary Federal

APT ： 度量之困

困 ：无法打破的壁垒

开放之难 / 封闭之过



KNOWNSEC TECH

Thanks ！

知道创宇科技

www.KnownsecTech.com