网络安全创新大会
Cyber Security Innovation Summit

蓝方的进攻——进攻是最好的防守

裴帅
信息产业信息安全测评中心

目录

攻防形式

知己知彼

总结

战术

评估

实战演练

攻击队

信息收集　内网边界探测　互联网边界探测

身份仿冒　钓鱼WiFi　钓鱼邮件

供应链攻击　精准攻击　水坑攻击

0day、1day

防守队

封禁IP

防守策略		
网络边界流量监测	流量分析、EDR	蜜罐、进程白名单

目录

攻防形式

知己知彼

战术

总结

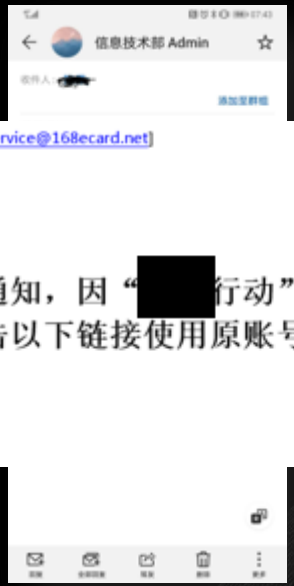
评估

防守反击

迅速而猛烈地转入进攻是防卸的最光彩的部分。

——《战争论》

EXP1:钓鱼邮件



发件人: 信息技术部 Admin [mailto:service@168ecard.net]
发送时间: 2019年6月24日 0:25
收件人: [redacted]
主题: 紧急通知！

接上级部门紧急通知，因“[redacted]行动”红蓝对抗，公司信息技术部将进行技术升级，现决定暂时冻结您的VPN账号使用权，如需使用，请点击以下链接使用原账号密码激活，感谢配合工作！

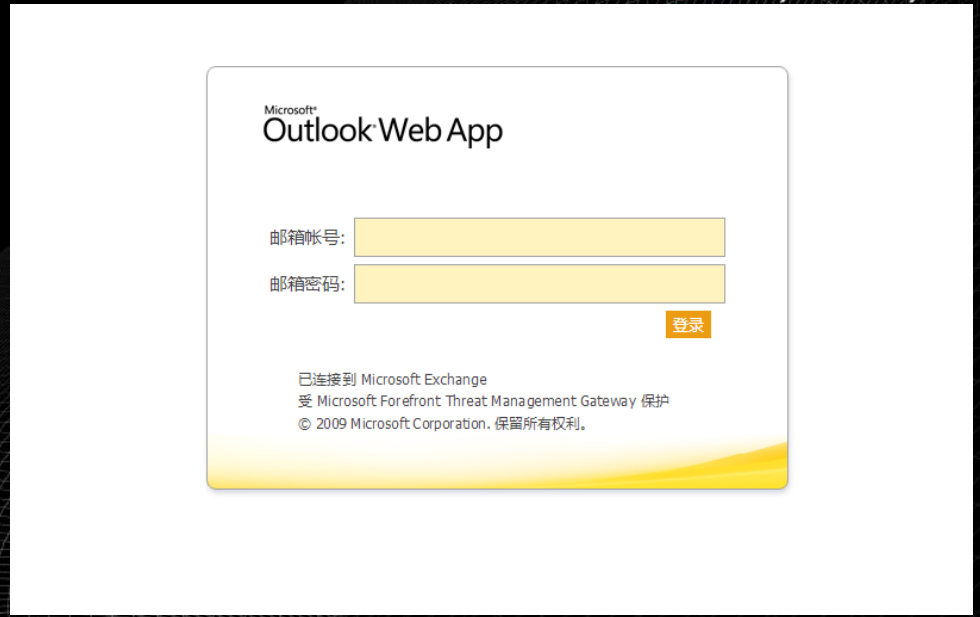
激活请点击：

激活链接

EXP1:钓鱼邮件

某个宁静祥和的凌晨，我们的某位客户收到了这么

EXP1:钓鱼邮件


Microsoft
Outlook Web App
邮箱帐号:
邮箱密码:
登录
已连接到 Microsoft Exchange
受 Microsoft Forefront Threat Management Gateway 保护
© 2009 Microsoft Corporation. 保留所有权利。

EXP1:钓鱼邮件

端口	协议	状态	服务	版本
21	tcp	open	ftp	Microsoft
80	tcp	open	tcpwrapped	
1026	tcp	open	msrpc	Microsoft
1029	tcp	open	msrpc	Microsoft
3389	tcp	open	ms-wbt-server	Microsoft

欢迎使用Ajiu AspWebServer!

[redacted].83 - /databases/

[To Parent Directory]

20[redacted] 200704 [redacted] - 副本.asp

20[redacted] 18550784 [redacted].mdb

[Aws V3.4] Need Help? Contact QQ:7[redacted]

EXP1:钓鱼邮件

操作总结：

结论1：
攻击者并不会太过于关注自身防护

结论2：
防守方也需要对攻击手段如数家珍

结论3：
我们的操作帮助客户了解了实际损失

结论4：

目录

攻防形式

知己知彼

总结

战术

评估

守城之法，从攻城生，故欲善守，必明善攻。

——《圣武记》

知己：

资产混乱

知彼：

了解攻击手段

EXP2:以牙还牙

```
POST /index.action HTTP/1.1
Host:
Accept-Language: zh_CN
User-Agent: Auto Spider 1.0
Accept-Encoding: gzip, deflate
Connection: close
Content-Length: 0
Content-Type: %{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUti                                                                    es().clear()).
(#ognlUti                                                                    nContext@getRequest()).
(#res=@or
(#res.getWriter().print('struts2_security_')).(#res.getWriter().print('check')).(#res.getWriter().flush()).(#res.getWriter().close())}

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Wed, 19 Jun 2019 09:58:37 GMT
Connection: close
```

被攻击IP和路径

Struts2攻击特征


喂！出来搞事情了

端口探测

80端口

服务确认

axis

默认后台
默认口令

搞事！！

WEB漏洞

EXP2:以牙还牙


```
2019/6/20 1:57:11——警告：存在Struts2远程代码执行漏洞-编号S2-046
2019/6/20 1:57:11——返回验证标志：struts2_security_check
2019/6/20 1:57:11——警告：存在Struts2远程代码执行漏洞-编号S2-045
```

目录

攻防形式

知己知彼

战术

总结

评估


委屈三连
他都干啥了?
他知道了啥?
他拷走了啥?

评估

EXP1：
钓鱼邮件
3000条左右邮箱登录信息，涉及敏感行业，某公司全国30+分公司均有邮箱沦陷。

EXP2：
Struts 2
大量存在Struts 2漏洞网址；攻击目标目录等

目录

了解自身脆弱点

损失评估

总结

了解攻击来源


CIS
网络安全创新大会
Cyber Security Innovation Summit
THANKS