幻阵-高级威胁检测系统 用户手册(超级管理员)

杭州默安科技有限公司

- ◎ 浙江省杭州市余杭区余杭塘路 2616 号正勤·美培创意园 3 号楼
- www.moresec.cn





文档说明文档说明

文档负责人	秦梓豪	文档版本编号	V3.0.0
起草人	秦梓豪	文档起草日期	2022.4.29
复审人	王哲	复审日期	

版本控制

版本号	版本日期	创建/修订人	说明
V2.10.0	2021-6-10	陈诗梦	创建
V2.10.1	2021-9-30	崔芙蓉	更新
V2.11.0	2022-1-14	黄澜	更新
V3.0.0	2022-4-29	秦梓豪	更新
V3.1.0	2022-8-19	秦梓豪	更新
V3.2.0	2022-11-9	秦梓豪	更新
V3.2.1	2022-12	秦梓豪	更新
V3.2.2	2023-01	秦梓豪	更新

版本申明

本文档本文件中出现的任何文字叙述、文档格式、插图、照片、方法、过程 等内容,除另有特别注明,均为保密信息。任何个人、机构未经杭州默安科技有 限公司的书面授权许可,不得复制、引用或传播本文件的任何片断,无论通过电 子形式或非电子形式。



目录

—、	概述…		5
1.1	产品概	{述	5
1.2	公司简	「介	5
二、	系统维	护	5
2.1	账号维	" 护	5
2.2	重新启		5
			_
<u> </u>	Web 官:	埋界面	5
3.1	豆 水介	*囬	5
3.2	风应入) 1	、盈	
3. 2	2.1	蚁/抗统\[
3. 2	2. Z	▽以古 IP	
3. 2	2.3		8
3.2	<u>(</u> .4 一	▽以古沙相 top5 和事件威胁寺级分布	8
3.3	女王入		9
3.4	威肋 悄	91次官埕	9
3.4	+. 1 • 0		
3.4	ł. Z		
3.4	i.	行刃分析	
3.5	蜜网官]埕 南回日回	
3.5	5.1 - 0	蜜网导图 如你应应	
3.5	o. 2	智能蜜网 N. 体体型	
3.5). 3 - 4 1-	沙箱官埋	
3.5	o.4 I⊦ 	'官埕	
3.5	o. 5	模板管埋	
3.5	5.6	伪装代理	
3.5	5.7	中继节点	未定义书签。
3.5	5.8	攻击诱捕	54
3.5	5.9	诱饵欺骗	
3.6	报表管		66
3. 6	5.1	威胁分析报告	66
3. 6	5. 2	攻击源分析报告	67
3. 6	5.3	黑客画像报告	67
3. 6	5.4	行为分析报告	68
3.7	联动配		68
3. 7	7. 1	威胁情报中心联动	
3. 7	7.2	集中管控平台联动	未定义书签。
3. 7	7.3	安全运营平台联动	69
3. 7	7.4	日志同步	70
3. 7	7.5	情报联动	70



3.8 配	置管理	72
3. 8. 1	账号管理−基本信息	72
3. 8. 2	账号管理-子账户管理	73
3. 8. 3	账号管理−授权信息	76
3. 8. 4	系统设置	76
3. 8. 5	系统升级	
3.9 日注	志审计	87
3.10	帮助中心	87
3.11	肖息中心	89
附录 A 自定	义沙箱部署说明	
i. 自定.	义沙箱说明	
ii. 自定.	义沙箱部署	
a) 🗦	新建自定义沙箱	
b) <u>1</u>	查看修改配置	



一、 概述

1.1 产品概述

默安幻阵是默安科技首创的一款基于攻击混淆与欺骗技术的威胁情报产品。通过在黑客 必经之路上构造陷阱,混淆其攻击目标,精确感知黑客攻击的行为。可阻断和隔离攻击,并 溯源黑客身份及攻击意图,形成黑客攻击情报。该产品可用于保护易受黑客入侵攻击的业务 系统,特别在金融、证券、运营商等包含大量用户数据、资金等敏感信息的业务环境中。通 过构建用户威胁情报体系,实现从安全事件的被动响应到安全威胁的积极应对,帮助企业控 制安全风险。

1.2 公司简介

杭州默安科技有限公司是由来自 BAT 等知名互联网安全团队资深专家及业内精英组建 成立的一家安全公司,致力于用创新技术解决企业安全问题的高新企业。将威胁情报技术和 人工智能技术融入企业真实安全防御体系,提供企业在云计算和 IOT 时代的安全整体解决方 案。默安科技将不断创新、积极探索,用专业服务成为企业信赖的安全伙伴。

二、 系统维护

2.1 账号维护

超级管理员密码如果忘记,请联系默安科技,安排工程师重置密码。

2.2 重新启动系统

如果遇到需要重启系统的情况应注意:在重启设备前停用所有已经启动沙箱,重启之后, 重新启动沙箱即可。

三、 Web 管理界面

3.1 登录界面

默安幻阵云端 Web 管理界面的登录方法:

- 1) 确保设备已被正确配置。
- 2) 打开浏览器 Google Chrome (支持以下浏览器: Google Chrome、firefox、IE11、



360 浏览器、Edge、搜狗浏览器),用 HTTPS 方式连接默安幻阵的 IP 地址,如: https://192.168.100.80

- 3) 回车后进入如下图所示的登录页面,输入正确的用户名、密码和验证码。
- 4) 子账户可选择认证登录方式,包括 radius 认证和 ldap 认证



图 3-1-1 默安幻阵云端 Web 管理登录界面

当用户未在规定时间修改密码时,系统会弹出强制修改密码弹窗,如下图所示,修改密码后便可重新登陆。

8码已过期,	为了确保账户安全,请修	政密码				
用户名	rice					
・旧密码	旧密码					
*新密码	请输入密码					
•确认密码	请再次输入一遍密码,	以便确认				
• 验证码	验证码		G	ñ	CL .	Y

图 3-1-2 密码过期强制修改密码弹窗

3.2 风险大盘

风险大盘主要记录目前用户环境所面临的威胁情况。具体包括攻击事件和入侵事件趋势, 受攻击目标 top5, 受攻击沙箱 top5, 事件威胁统计。



3.2.1 数据统计

\$										🜲 💄 admin 🗸
Alexa	风险大盘							最近7天 最近30天	当月	2022-04-12 ~ 2022-04-18 🗀
e Frita Setta Setta	^{资产防护} 16个	•	入侵事件 1次	7	^{探测事件} 203次	છં	_{威胁人员} 204个	30	企业或助量	H伦值 6.83 4至

图 3-2-1 默安幻阵云端 Web 风险大盘界面

如上图上方前四个展示框,分为资产防护、探测事件、入侵事件、威胁人员四项,其中 资产防护即为当前的伪装代理数量,探测事件、入侵事件、威胁人员即为前用户环境某一段 指定时间内(默认是最近7天)的数据统计。

威胁风险量化值是默安幻阵基于当前发现攻击事件行为和威胁人员数目以及时间和威胁程度量化出来的一个分值,分值越高,表示系统的风险越高。企业威胁级别分为低危、中危、高危、重度高危和 APT 攻击五个级别,分值小于等于 20 企业威胁级别为低危,分值 20--50 企业威胁级别为中危,分值 50--80 企业威胁级别为高危,分值 80--90 企业威胁级别为重度高危,分值大于 90 企业威胁级别为 APT 攻击。

3.2.2 受攻击 IP

192.168.11	0.201			
192.168.11	0.207			
192.168.11	0.208			
100 100 11				
192.168.11	0.202(凸面际)			
192.168.11	0.202(己删除)			

图 3-2-2 默安幻阵云端 Web 风险大盘受攻击 IP top5 界面

如上图所示, 受到攻击状态图以横向柱状图显示。分别取受到攻击最多的五个资产作 为展示。



3.2.3 攻击和探测事件趋势



图 3-2-3 默安幻阵云端 Web 风险大盘探测/入侵趋势界面

如是上图所示,系统记录了目前用户环境某一段指定时间内(默认是最近7天)的数据统计探测和入侵事件数,并根据用户选择时间分析出用户环境在这段时间内所遭受的攻击事件趋势。

3.2.4 受攻击沙箱 top5 和事件威胁等级分布



图 3-2-4 受攻击沙箱 top5 和事件威胁等级分布



3.3 安全大屏

安全大屏是实时显示目前用户环境的威胁情况。主要显示当前状态:动态显示当前网络 拓扑图和受攻击实时动态展示,如图:



图 3-3-1 默安幻阵云端 Web 安全大屏页面

3.4 威胁情报管理

3.4.1 黑客溯源

黑客溯源页面主要统计攻击过目前用户环境的攻击者,以图表形式显示攻击者名称、攻 击源 IP、内网 IP、公网 IP、物理地址、开始攻击时间-最近攻击时间、攻击次数,可对攻 击者添加白名单,当攻击为扫描器时将会显示出扫描器类型,现能获取的扫描器类型有:AWVS、 Netsparker、WebInspect、NSFOCUS RSAS、Nessus、WebReaver、Sqlmap。如图:

果 書反制 风助大盘	黑客溯源 可從化展示不同攻击者相关信息			
查看事件 安全大屏 行为分析 章 成的情報	. A∧R 9	国内印数:0 国外印数:0 内阁印数:7	国内中数:0 国外中数:0 内岡中数:9	国内P数: 1 国外P数: 8 内网P数: 11
· · · · · · · · · · · · · · · · · · ·	双击者 全部 🗸 攻击时间	开始时间 - 结束时间 巴		P地址 Q
16 报表管理	双击源 全部 · 显示顺序	按照最近攻击时间排序 🗸		□ 隐藏白名单
00 DECEM	H−0006 8:69%X	谷 扫描工具(白名单) ∞ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆	2: 未知 (8: 6)	2 未知 次約2次 ■
尼爾 爾德 日志等针	次出第1P: 192.168.30.45 (用減間) 内間P: 共和 公開P: 115.236.55.14 (統州) 115.236.55.56 (統州)	192168.111.149(周端隅) 日相工具类型 未知	地址 94.237.64.20 (芬兰)	地址 81.0.124.200(布达线版)
MI0+0	无 开始攻击时间一量近攻击时间 2022-04-24 12:18:03-2022-04-25 10:42:18	开始攻击时间一量近攻击时间 2022-04-24 14:25:24-2022-04-25 10:40:46	开始攻击时间一量立攻击时间 2022-04-25 10:20:56—2022-04-25 10:37:46	开始攻击时间—雕近攻击时间 2022-04-25 10:19:56—2022-04-25 10:36:36
	2. 未知 x624X E 日	2:未知 (Xdil)(X = 日	2: 未知 ※80X B B	2. 未知 X #2X E B
	地址 192.168.111.103 (周端网)	地社: 192.168.199.199(周城网)	地址 9413049186(乌克兰)	地址 219.216.128.25 (大连)



图 3-4-1 黑客溯源

点击查看详情图标⁽),会跳转到黑客画像分析界面,里面会以图表和列表两种方式显示攻击者的详细信息,包括攻击了哪些资产以及被隔离到哪个沙箱等信息,点击生成报告可 单独生成该攻击者的攻击报告。

情报联动模块会根据攻击者的设备指纹信息进行碰撞,如果有相匹配的指纹信息,将会 从情报中心同步相关数据,以达到丰富黑客画像目的。

分析					生的
H-0005 支法33次 攻击者身份:自然人 香注: ≪ 研定为白名单	6	攻击源中 192.196.30.17(周朝間) 192.196.30.54(周朝間) 日期工具共型 未知	公開IP 未知 内開IP 115.236.5.58(8	用他口 csdn: Orange35 98)	
情报联动数据			Ē		
设备指纹			TE POINT		
设备1	94d94f092216af	380c9b0c557d8263			
acamina, cor					
操作系统	Windows	10	设备类型	PC	
操作系统 CPU核心数	Windows 12	10	设备类型 语言	РС ФХ	
操作系统 CPU核心数 显卡设备	Windows 12 ANGLE (ps_5_0)	10 AMD Radeon(TM) Graphics Direct3D11 vs_5_0	设备类型 语言 音频设备	PC #-X 46000_2_1_0_2_explicit_speakers	

图 3-4-2 黑客画像分析

同时黑客画像分析页面还可自动归并攻击者的攻击链,展示攻击者的攻击路径,反向探 测攻击源所开放的端口和服务。

	2022-04-24 19:47:10 攻击了 fghjøkrigth, 灾击题为192.108.30.45
2	2022-04-24 12:18:03 攻击了 cm電源tost, 攻击原为192:188-30.45
攻击源探 攻击者 192.168 端口和 135 139 445 902 912	

图 3-4-3 黑客画像攻击路径

黑客反制页面主要显示反制的攻击者,在页面上会具体的显示出反制类型,攻击者 IP, 在线状态,初次上线时间以及最近上线时间。可根据在线状态、IP 位置、最近上线时间等 进行精确搜索,攻击反制如下图所示:

黑客反制						
在线状态 全部 V IP位置 全部	β	◇ 反制类型 全部 ◇ 最近上线时间 :	开始时间 一 结束时间 芭		即地址	0
F-008 @M		F-006 高位	F-007 #15		F-005 奥线	
反制类型		反制类型	反制类型		反制类型	
Windows端点反制		Windows端点反制	Windows镭点反制		Windows港点反制	
攻击者IP		攻击者中	攻击者IP		攻击者IP	
.13 (局域网)		0.110 (局域网)	20.68(局域网)		0.64 (局域网)	
初次上线时间 / 最近上线时间		初次上线时间 / 最近上线时间	初次上线时间 / 最近上线时间		初次上线时间 / 最近上线时间	
2022-08-09 15:02:50 / 2022-08-09 15:02:50		2022-08-09 12:35:55 / 2022-08-09 12:48:04	2022-08-09 12:40:24 / 2022-08-09 12:40:2	4	2022-08-09 12:19:18 / 2022-08-09 12:19:18	
F-003 周线		F-004 85	F-001 周续			
反制类型		反制类型	反制类型			
Mac確点反制		Android錯点反制	Windows德点反制			
攻击者IP		攻击者中	攻击者IP			
1.4 (局域网)		107(局域网)	2.52 (局域网)			
初次上线时间 / 最近上线时间		初次上线时间 / 最近上线时间	初次上线时间 / 最近上线时间			
2022-08-01 15:29:37 / 2022-08-08 17:59:17		2022-08-01 15:57:07 / 2022-08-01 15:57:07	2022-06-28 16:28:32 / 2022-07-06 15:46:4	9		

图 3-4-4 攻击反制

点击 进入 Windows 反制详情页面,可以看到具体的反制信息,包括反制对象、设备 精确信息,以及高级反制。攻击反制中木马可以抓取 wechat,qq,cs,navicat,xshell 连接信 息,支持将数据以列表的形式下载。如下图所示。

图 3-4-5 攻击反制

反制对象包括反制的类型(当被反制者状态为离线时,高级反制仅可进行历史命令的查询),反制 IP 以及与所关联的攻击者。

设备精确信息包括基本信息、网卡信息、IP 信息、用户信息、进程信息、系统信息以及桌面文件。

基本信息包括操作系统的类型、设备类型、主板序列号、硬盘序列号、cpu 类型、BLOS、GPU 类型、IDE、显示器、声卡、内存条、硬盘、主机品牌、物理机接口、当前路径以及当前用户,如下图所示。

٢	www.moresec.cn
---	----------------



图 3-4-6 基本信息

网卡信息包括组策略配置文件、接口 WLAN 上的配置文件等信息,如下图所示。

管精调18 2.信息	BB ▲ 网卡描显 PP信息 进程信息 系统信息 桌面文件 关键数据
	lpadoress servicename description
	krinic Microsoft Kornel Dehun Network Arlanter
	tac0091 TAP-Windows Adapter V9
	(192.168.212.1, fe80:e5c2:3f1b;ba37:cab9) VMnetAdapter VMware Virtual Ethernet Adapter for VMnet1
	{192.168.126.1, fe80::2046:a6a5:7a9b:d9ec} WhnetAdapter VMware Virtual Ethernet Adapter for VMnet8
	eTdexpress Intel(R) Ethernet Connection (7) 1219–V
	{192.168.100.179, fe80::75ae:cd1b:ac6b:b09c] athr Qualcomm QCA9565 802.11b/g/n Wireless Adapter
	wifimp Microsoft WI-Fi Direct Virtual Adapter
	RasSstp WAN Miniport (SSTP)
	RasAgileVpn WAN Miniport (IKEv2)
	Rasl2tp WAN Miniport (L2TP)
	PptpMiniport WAN Miniport (PPTP)
	RasPppoe WAN Miniport (PPPOE)
	Ndiswan WAN Miniport (IP)
	Ndiswan WAN Miniport (Irwo)
	Ndiswan www.wimport.(Network.wionitor)

图 3-4-7 网卡信息

IP 信息包括用户的网络配置信息,例如 Windows 配置、vlan、以太网配置等信息,如

下图所示。

信息	网卡信息 阿信息 进程信息 系统信息 桌面文件 关键数据	
	macadress name	
	Microsoft Kernel Debug Network Adapter	
	00:FF:EA:93:F1:2D TAPWindows Adapter V9	
	00:50:56:C0:00:01 VMware Virtual Ethernet Adapter for VMnet1	
	00:50:56:C0:00:08 VMware Virtual Ethernet Adapter for VMnet8	
	E4:54-E8:86:86:4A Intel(R) Ethernet Connection (7) I219–V	
	40:23:43:D7:15:95 Qualcomm QCA9565 802.11b/g/n Wireless Adapter	
	12:23:43:D7:15:95 Microsoft Wi-Fi Direct Virtual Adapter	
	WAN Miniport (SSTP)	
	WAN Miniport (IKEv2)	
	WAN Miniport (L2TP)	
	WAN Miniport (PPTP)	
	WAN Miniport (PPPOE)	
	E0:87:20:52:41:53 WAN Miniport (IP)	
	EA:3F:20:52:41:53 WAN Miniport (IPv6)	
	EE:00:20:52:41:53 WAN Miniport (Network Monitor)	
	22-23:43:07:15:95 Microsoft Wi-Fi Direct Virtual Adapter #2	

图 3-4-8 IP 信息 用户信息包括用户的账户信息等内容,如下图所示。





设备精确信息 🛓	
基本信息 网卡(信息 IP倍息 用户信息 美理信息 系统信息 桌面文件 关键数据
cap	otion name
DE	SKTOP-UQH0PAQ\Administrator Administrator SKTOP.LOURDRO.Dofted/Kennetz
DE	SKTOP-UdrifoRA/Guest Guest
DE	SKTOP-UQH0PAO\kkkkk kkkkk
DE	SKTOP-UQH0PAO\WDAGUtilityAccount WDAGUtilityAccount

图 3-4-9 用户信息

进程信息包括映像名称、PID 会话名、内存使用情况等。如下图所示。

备精确	信息 🛓	
本信息	网卡信息 IP信息	户信息 进程信息 桌面文件 关键数据
	name	sessionid processid
	System Idle Process	0 0
	System	0 4
	Hegistry	0 124
	smss.exe	0 492
	CSISS.0X0	0 740
	wininit.exe	0 868
	CSFSS.exe	1 876
	services.exe	0 940
	Isass.exe	0 964
	winlogon.exe	1 1016
	svchost.exe	0 1028
	fontdrvhost.exe	1 1056
	fontdrvhost.exe	0 1064
	svchost.exe	0 1144
	svchost.exe	0 1200
	svchost.exe	0 1328

图 3-4-10 进程信息

系统信息包括攻击者系统的一些信息,例如主机名, os 名, os 版本等信息,如下图所

示。

设备精确信息 ▲				
信息	两卡信息 IP信息 进程信息 茶做信息 桌面文件 关键数据			
	Domain :WORKGROUP			
	Manufacturer : Lulai no. Model : Vostro 5050-China HDD Protection			
	Name 1:DESKTOP-UCH0PAO PrimaryOwnenName 1:868k			
	TotalPhysicalMemory : 8395845632			

图 3-4-11 系统信息 桌面文件为攻击者的桌面信息,如下图所示。



殳备精确 (喜息 🛓				
基本信息	网卡信息	P信息 用户信	息 进利	程信息 系统信息 <u>桌面文件</u> 关键数据	
	目录: C:\U	sers\kkkkk\Desi	ktop		
	Mode	LastWrite	eTime	Length Name	
		2021/7/12	17:06	245	
	d	2021/3/3	16:49	BadOutlook	
	d	2020/11/23	17:10	canarytokons-master	
	d	2021/8/6	12:15	acby-win-x64-1.8.293	
	d	2021/8/9	16:06	platform-tools	
	d	2022/4/18	15:38	route cli(1)	
	d	2020/11/9	9:29	route_cil_win_1604885374	
	d	2020/12/1	16:28	syntest	
	d	2020/12/1	16:37	syntestwc	
	d	2020/11/3	12:57	v2rayN	
	d	2021/11/30	13:53	winhexi汉化破解版	
	d	2020/11/25	14:49	xmrig=6.3.0-msvc-cuda10_2-win64	
	d	2020/11/3	14:05	【幻阵2.8.0】管理员%26普通用户%26普通管理员权限对比	

图 3-4-12 桌面文件

关键数据,展示手机号、iPhone (IMEI、MEID、序列号)、Git、Email、域名 用户名等 信息,如下图所示。

设备精确信息	
qq: ["569620010"]	
wechai: hull	
+ 90 - 91 - 173 / 00 - 199 - 1	
Git	
inhone连接记录: {'imei':''.''meid':'''.''''')	
域名 用户名	
http://116.228.13.134:20180/login admin	
http://116.228.13.134:20180/login superuser	
http://192.168.110.145 admin	
http://192.168.110.145/ admin	
http://192.168.120.140/login admin	
http://192.108.120.140//0gin/1061222	
http://1218c.toc.toc.ob.cov/w/wight.acution juctuarityue	
I https://outer.com/consol/oper/com/sport/sport/	

图 3-4-13

高级反制,当攻击者在线时(攻击者离线时除历史命令查询保存,其余均隐藏),幻阵 可对其进行一系列的操作,包括交互 shell、文件上传、文件下载、电脑截屏、历史命令查 询,如下图所示。



图 3-4-14 高级反制

交互式 shell, 幻阵使用者可以在攻击者电脑上进行一些操作, 且攻击者电脑不会显示

出来,如下图所示。





图 3-4-15 交互式 shell

文件上传,使用者指定上传到攻击者电脑的地址以及文件,点击上传显示上传成功即可,

此时攻击者电脑对应的地址便会有幻阵使用者上传的文件,如下图所示。

L反制			
操作 文件上传 🗸			
请输入要上传的路径			
	选择文件 上传		

图 3-4-16 文件上传

文件下载,幻阵使用者指定下载的内容在攻击者电脑上的地址,点击下载即可下载即可。 如下图所示。

高级反制				
反制操作	文件下载	Ŷ	请输入要下载的文件路径	29 不

图 3-4-17 文件下载 电脑截屏,点击执行即可截取攻击者电脑当前的图片,如下图所示。



			🗘 🛛 🔉 admin 🗸
高级反制			
反制操作 电脑截屏 🗸 执	ਰਿ		
Bieten Hfish-0.5			Layer 123501. 5.0+SAIN
Google ahrid-mas			65.
260g全卫± python-2_	pip-9.0.1.t	tesLovo	
360009188 python-2.7			
HFah-0.5 python-2			
ahrid-mas pip-9.0.1.tar	setuptoolu		
Confirmu setuptooL. (64)			

图 3-4-18 电脑截屏

历史命令查询可以看到在攻击者电脑上执行的命令,该内容在攻击者上线和离线状态下

均存在,如下图所示。

高级反制	
反制操作	历史命令查询 🗸
页面文件 域: 登录服务 修补程序	位置: C:\pagefile.sys WORKGROUP 器: \\172_17_0_6 : 安装之下方::: 雪序。
网卡:	安裝了 1 个 NIC。 [01]: Red Hat VirtIO Ethernet Adapter 连接名: 以太网 启用 DHCP: 最 DHCP 服务 IP 地址
Hyper-V	要求: 题示。一题示。将不显示 Hyper-V 所需的功能。
	图 3-4-19 历史命令查询

Mac 反制详情:点击 IIII 进入 Mac 反制详情页面,可以看到具体的反制信息,包括反制

对象、设别精确信息,以及高级反制,如下图所示:



反制对象			
反制类型		反制P	
关联攻击者			
备精确信息			
本信息 应用详情 蓋	牙 网络信息 浏览器信息 社交信息		
系统版本		内核版本	
计算机名称	and the second s	用户名	1000 C
		硬盘	
内存			
内存 设备序列号		防火墙状态	

设备精确信息包括基本信息、应用详情、蓝牙、网络信息、浏览器信息、以及社交信息; 基本信息包括系统版本、内核版本、计算机名称、用户名、内存、硬盘、设备序列号、防火 墙状态等;

应用详情包括应用名称、应用版本、最后一次使用时间 蓝牙包括 mac 地址、启用状态、蓝牙设备名称、Mac 地址等

本信息 应用详情 靈牙 网络信息 浏览器信息 社交信息		
AC地址: A ; 开启		
蓝牙设备名称	MAC地址	
WF-1C		
Phone		
Keych		
M585,		
WH-1		

网络信息包括 wifi Mac 地址、当前网络信息、剩余网络信息等

I-FI MAC地址	a0:7		当前网络信息	m	
	ю*-	М		0	
	C	O		TI	
	x	Y,		m	
	m	m		m	
余网络信息	n	m		m	
	w	39			

浏览器信息包括浏览器 URL 和用户名



歸稱确信息		
基本信息 应用详情 篮牙 网络信息 浏览器信息 社交信息		
URLibb	用户名	
http://116.23	al l	
http://117.18/	ac	
http://117.73		
http://118.12	ac	
http://192.16	br	
http://192.16	te	

社交信息包括微信账号、手机号、邮箱; 钉钉手机号、邮箱

信				
账号		手板	几号	
邮箱				
ŧŢ	16	40.93		

当攻击者在线时(攻击者离线时除历史命令查询保存,其余均隐藏),幻阵可对其进行 一系列的操作,包括命令执行、文件上传、文件下载、历史命令查询

命令执行,幻阵使用者可以在攻击者电脑上进行一些操作,且攻击者电脑不会显示出来, 如下图所示。

高级反制	
反制操作	命令执行 ∨
\$	

文件上传,使用者指定上传到攻击者电脑的地址以及文件,点击上传显示上传成功即可, 此时攻击者电脑对应的地址便会有幻阵使用者上传的文件,如下图所示。

反制操作	文件上传	\sim			
路径	请输入要上传的路径				
			选择文	件上传	

文件下载,幻阵使用者指定下载的内容在攻击者电脑上的地址,点击下载即可下载即可。 如下图所示。

反制操作	文件下载 🗸 🗸		
路径	请输入要下载的文件路径	下载	

Android 反制详情:点击^围进入 Android 反制详情页面,可以看到具体的反制信息, 包括反制对象、设别精确信息,以及高级反制,如下图所示:

制对象				
反制类型:	Android端点反制(离线)		反制吧:	10-10-10-10-1000
关联攻击者:	无			
备精确信息 <店息 通讯录信息	短信信息			
各精确信息 本信息 通讯录信息	短信信息	20.56 1946 -		
备精确信息 本信息 通讯录信息 手机型号:	始信信息	设备指纹:		
备精确信息 本信息 通讯录信息 手机型号: 操作系统:	短信信息	设备指纹: 联网方式:		

设备精确信息包括基本信息、通讯录信息、短信信息等; 其中基本信息包括手机型号、设备指纹、操作系统、联网方式、经纬度信息等 通讯录信息包括姓名和电话

默安科技



设备精确信息 基本信息 通讯录信息 知信信息		
姓名	电话	
۹ <u>ت</u>	02	1
Ð	05	
ŧ٦	05	
£1	10	
jū.	05	
Ð	0;	

短信信息包括收发短信的手机号、详情和时间

设备精确信息 基本信息 通讯录信息 短		
收信息 发信息		
发送者手机号	详情	87(6)
16	h.	2
16	9	21
15	9	21
+	8	2(
17	7) warrant	21

当攻击者在线时(攻击者离线时除历史命令查询保存,其余均隐藏),幻阵可对其进行 一系列的操作,包括命令执行、文件上传、文件下载、历史命令查询

命令执行,幻阵使用者可以在攻击者电脑上进行一些操作,且攻击者电脑不会显示出来, 如下图所示。

_	
高級反制	
反制操作	<u> </u>
s	
ľ	

文件上传,使用者指定上传到攻击者电脑的地址以及文件,点击上传显示上传成功即可, 此时攻击者电脑对应的地址便会有幻阵使用者上传的文件,如下图所示。

反制操作	文件上传	\sim			
路径	请输入要上传的路径				
			选择文件	+ 上传	

文件下载,幻阵使用者指定下载的内容在攻击者电脑上的地址,点击下载即可下载即可。 如下图所示。

反制操作	文件下载	~		
路径	请输入要下载的文件路	各径	下载	

3.4.2 查看事件

默安科技

查看事件列表详细记录威胁事件攻击者、攻击源、攻击目标、开始攻击时间、最后攻击 时间和事件的风险等级。同时记录攻击者的详细操作步骤,对 SSH, RDP 操作记录进行视频 展示,对攻击者上传文件进行下载可分析,逃逸检测功能,当发生逃逸时也会在事件列表进 行记录,并且支持隔离沙箱对高管邮件、机密文件、疑似逃逸、高敏沙箱的筛选。默安幻阵 采用先进的指纹智能识别技术,能有效区分攻击者身份,用户可主动添加 IP 到白名单中, 避免扫描器产生的大量告警。如下图事件列表所示。



风险大盘	黑客反制	查看事件	将不同攻击者对不同;	少箱的攻击事件单数	胆臼并,分别展示为事件									
-	双相事件	攻击者	全部	攻击目标	所有资产	~ 隔离沙箱	所有沙箱						3	±a Q
安全大屏	行为分析	风险等级	全部	事件类型	全部	∨ 攻击时间	开始时间	→ 結束时间 □						隐藏白名单内的攻击事件
E BEROGER		过滤炉	请输入过滤的P,	多个沪之间用英	文道号分篇									
- 														
展 服表管理		攻击者	攻击源(攻击目标		隔离沙箱	开始攻击时间	¢	最近攻击时间	÷	风险等级	0	操作
C) BRADER		未知	192		O 192		ssh	2022-11-09 20:05:55		2022-11-09 20:06:26		● 高危		
		未知	192		O 10.0		高敏沙箱	2022-11-09 11:58:23		2022-11-09 14:07:23		* 162		8
CHER I		未知	192		0 192 0 10.0		高敏沙箱	2022-11-09 00:42:39		2022-11-09 14:07:23				8
日志审计		未知	192		O 10.0		高敏沙箱	2022-11-09 13:14:33		2022-11-09 14:06:13				
「「「「」」		未知	190		0 10.0		高敏沙箱	2022-11-09 12:06:13		2022-11-09 14:06:13		* 65		
		未知	20:		O 10.0		高敏沙箱	2022-11-09 12:05:03		2022-11-09 14:05:13		* 62		8
		未知	111.		O 10.0		高敏沙箱	2022-11-09 12:02:43		2022-11-09 14:04:13		* 68		8
		未知	193		O 10.(高敏沙箱	2022-11-09 12:17:23		2022-11-09 14:00:43		* 65.		8
		未知	192		O 10.0		高敏沙箱	2022-11-09 13:12:13		2022-11-09 13:23:23				8

图 3-4-20 事件列表

事件列表的攻击目标筛选框和攻击目标列表中,均会展示中继节点标签以及伪装代理的

IP 标签,如下图所示。

	全部 ∨	攻击目标	所有资产	∨ 開朗	制沙箱	所有沙箱 🗸 🗸					1	《击源
1.险等级 :	全部 🗸	事件类型	全部	▽ 攻击	时间	开始时间	→ 结束时间					隐藏白名单内的"
İ滤IP	请输入过滤的P,多'	↑IP之间用英文	X這号分開									
攻击者	攻击源 🌑		攻击目标			隔离沙箱	开始攻击时间	¢	最近攻击时间	\$ 风险等级	9	操作
扫描工具	192		O 192.			wbcl	2022-11-09 22:45:55		2022-11-09 22:47:04	■ 低危		
未知	192		O 192.			ssh	2022-11-09 20:05:55		2022-11-09 20:06:26	■ 高危		
	192		0 10.0			高敏沙箱	2022-11-09 11:58:23		2022-11-09 14:14:13	· ###		
未知	102											

图 3-4-21 事件列表

事件列表有事件回放按钮、恶意文件分析按钮以及入侵视频回放按钮。点击事件回放按钮,如下图攻击事件回放,可看到攻击者的基本信息以及攻击者的入侵记录,以及攻击者的 mac 地址以及对扫描器的识别。同时支持对攻击手法进行筛选,通过时间轴的方式展示重点 攻击手法及事件。



21 未知 攻击者身份:未知	真 人事:15% 备注:				居满沙神道 ssh
扫描工具类型		攻击者mac地址		物理位置	
未知		未知		未知	
关键攻击路径					
2022-11-09 20:05:55					
③ 攻击源:;		② 攻击源: 32.31			
TRY (-H) day with T	HARME SSU BEAT MAL	THE THE REPORT OF THE REPORT OF THE	2 1: 1001 原码为:		
攻击者成1 123	为破解 SSH,用户名为:root,密码	3为: 攻击者成功破解 SSH,用户: 123	名为:root,密码为:		
攻击者成1 123	动破解 SSH,用户名为:root,密码	政击者成功破解 SSH,用户: 123	名为:root,密码为:		
攻击者成1 123 2022-11-09 3	功敏解 SSH, 用户名为: root, 密研 20:05:55	政击者成功破第 SSH,用户: 123 2022-11-09 20:05:56	名为:root、密码为:		
攻击者紀 123 2022-11-09 : 攻击记录 3	力破解 SSH, 用户名为: root, 密切 20:05:55	攻击者成功破解 SSH,用户+ 123 2022-11-09 20:05:56	名为:root, 密码为:		,
攻击者成1 123 2022-11-09: 攻击討闹 升出时间	加加第 SSH,用户名为: root, 部分 2005:55 → 結束时间 □ 3	335: 改击會成功被解 SSH,用户: 123 2022-11-09 20:05:56 2014日線 所有资产 ∨ 攻击:	名为: root, 密码为: 手法 全部 v		第3回9項点行为 Q
双击者成: 2022-11-09: 双击记录 3 双击时间 开拍时间	始額第 SSH、用户名功: root, 密想 20:05:55 → 結束的同	X 出意構成功能解 SSH、用P4 I23 2022-11-09 20:05:56 X出目編 所有面广 ◇ 攻击:	名为: root, 密码力: 手法 全部 〜		。 原源P/復点付为 Q 组织时 文
双击电印 2022-11-09: 双击记录 圖 双击时间 开出时间 事件失型 全部 双击时间	2015年5月 - 新知時月 - 新知時月 - 新知時月 - 初生時時 - 初生日報	(3): X土倉道功能第 SSH、用P4 (23 (22-11-09 20.05.56 (24-14)	主次: root, 世前次: 手法 全部 夫型 双曲手以 ス由手以	i R&75	(東京中)攻点行力 (東京中)攻点行力 (東日村文) 勝作

图 3-4-22 攻击事件回放

在事件回放显示页面中点击攻击者的网络 ID, 会跳转至黑客画像分析页面。如下图内 容所示, 用户可查看攻击者的详细身份信息, 包括攻击源 IP、攻击者真实 IP、内网 IP、公 网 IP、网络 ID(包括 163、新浪、百度等)、设备指纹、使用的操作系统、浏览器。如果 配置了联动配置-威胁情报中心联动相应内容, 对于匹配到相同设备指纹的真人, 会在情报 联动数据模块显示相应信息。进一步丰富黑客画像内容。

H-0005 改击31次	攻击源中 192.168.30.171(局域网) 192.168.30.54(周城网)	公開戸 未知	网络D csdh: Orange35	
收回省900、回照八 备注: 2 标记为白名单	扫描工具类型 未知	内刚P 115.236	5.56(H(m)	
情报联动数据				
设备指纹				
设备指纹: e87	94d94f092216a880c9b0c557d8263			
操作系统	Windows 10	设备类型	PC	
CPU核心数	12	语言	中文	
显卡设备	ANGLE (AMD Radeon(TM) Graphics Direct3D11 vs_5_0 ps_5_0)	音频设备	48000_2_1_0_2_explicit_speakers	
		INCOME. OR	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.424	0.198

图 3-4-23 黑客画像分析

点击恶意文件分析按钮"¹¹"即可跳转到攻击文件分析页面,详细的展示了攻击上传的文件名称、文件类型、文件 md5、virustotal鉴定、AntlVirus鉴定,并且可以对恶意文件进行下载,如下图上传文件分析所示。

O	默安科技
---	-------------

攻击文件:	分析						×
	文件名称	文件类型 😡	文件MD5	VirusTotal鉴定	AntiVirus鉴定	操作	
	audit_pressure_tool	elf	ee35a8dcafd8c10e32bc48e7685ceb1b	未知	未知	4	
	web123.php	php	2782bb170acaed3829ea9a04f0ac7218	恶意文件 🔘	未知	4	
	web123.php	php	2782bb170acaed3829ea9a04f0ac7218	恶意文件 🔘	未知		

图 3-4-24 恶意文件分析

入侵视频支持 ssh 攻击事件回放和 rdp 攻击事件回放,点击'[■]'即可弹出入侵视频回放 界面,展示出了视频名称、开始事件、视频大小以及操作,以 rdp 为例,如下图 RDP 入侵视 频回放所示。

	RDP入侵视频回放			×
视频名称	开始时间	视频大小	操作	
1612255967.mp4	2021–02–02 16:57:22	2.62M		

图 3-4-25 RDP 入侵视频回放

点击'[•]'即可播放入侵视频,如下图 rdp 入侵视频回放

0								
न संस								
	fuck.txt	Mitty for						
			2					
0:09 / 0:16						Ŕ	53	:
1 22 c						1.8	the states of	Windows 114-74
	2:0:09 / 0:16	Ω:09 / 0:16	in in in in in in in in in in	vie vie vie vie vie vie vie vie			i	v

图 3-4-26 rdp 入侵视频回放

3.4.3 行为分析

该页面按照时间轴排序展示所有被监控沙箱的详细攻击行为记录,可根据攻击者、攻击源、攻击目标、隔离沙箱、攻击时间、攻击类型、攻击者手法等信息更加快速定位攻击者;



在攻击行为处增加对扫描工具的判别展示和对进程逃逸的展示。同时支持对伪装代理、中继 节点的半开连接、UDP 扫描等事件的记录(此功能需要打开半连接感知开关)。集成了内部 编码转义功能,用户可以直接在页面内贴入需要转换的 URL,点击转义输出转义结果。同时 引入了 ATT&CK 能力,支持用户通过 ATT&CK 进行筛选。上述功能如下图所示:

黑客反制	行为分析 对所有志	(击通过时间线展示,通过转选机	当统一分析						
查看事件	攻击者 全部	∨ 攻击目标	所有资产 > 隔离沙箱	所有沙箱 🗸 类型	全部 ソ 攻击手法	去 全部		攻击源/攻击行为	Q
行为分析	ATT&CK 全部	> 攻击时间	──开始时间 → 结束时	6 1					编码转义
	攻击者	攻击源	攻击目标	隔离沙箱	攻击时间	类型	攻击手法	攻击行为	条作
	扫描工具	192.100 000 01	-	wbcl	2022-11-09 22:47:04	探測	端口扫描	攻击者在30s内建立11条恶意 TCP 连接。 攻击者探测了80 端口	
	▼ 扫描工具	192.1	O 192.	wbcl webcione	2022-11-09 22:46:54	探测	尝试攻击	攻击者访问了: 192.168	
	▼ 扫描工具	192.1	O 192.	wbcl webcione)	2022-11-09 22:46:36	探測	尝试攻击	攻击者访问了: 192.161 nl	
	扫描工具	192.1	-	wbcl	2022-11-09 22:46:26	探测	端口扫描	攻击者在30s内建立 6 条形意 TCP 连接。 攻击者探測了 80 端口	
	▼ 扫描工具	192.1	O 192.	Wbcl webcicne	2022-11-09 22:46:02	探测	尝试攻击	攻击者访问了: 192.100 000 000 (
	▼ 扫描工具	192.1	O 192.	wbcl webcione	2022-11-09 22:45:55	探測	尝试攻击	攻击者访问了: 192.168 *** ****	
	 扫描工具 	192.1	O 192.	wbcl webcione	2022-11-09 22:45:55	探测	尝试攻击	攻击者访问	

图 3-4-27 行为分析

在页面中可点击攻击者跳转至黑客画像分析页面,查看该攻击者详细信息;点击单条攻 击手法可跳转至攻击事件回放页面,显示该条记录关联的完整事件。

3.5 蜜网管理

3.5.1 蜜网导图

默安幻阵支持集群管理,一个云端管理多台客户端。幻阵智能蜜网系统,通过一键检 测企业内现有服务,加以安全算法编排,将中继节点、伪装代理迅速关联沙箱,同时实现自 适应业务场景。在节省人力部署成本的前提下,以安全人员的视角迅速张开蜜网,真正实现 快速、自动化智能部署。(如下图 3-5-1-1 所示)

基于探测及扫描结果, 密网导图将显示幻阵设备、中继节点设备、沙箱信息, 并围绕相 关内容, 展开显示伪装代理 IP、中继节点 IP 等绑定沙箱的情况, 同时也将显示探测的客户 资产 IP、未存活 IP 的相关内容。





图 3-5-1-1 蜜网导图

3.5.2 智能蜜网

智能蜜网是在贴合现有业务场景的前提下,将欺骗能力赋予各个业务单元。通过智能 自动化的方式快速部署形成欺骗密网。

用户可以勾选一键探测模块下的中继节点或者伪装代理发起探测,发起探测过程中,将 会对不同 vlan 或子网信息进行扫描。并以图形化的方式统计相应的端口分布情况、系统分 布情况信息。探测完成后需要用户手动刷新页面,查看最新页面信息。如图 3-5-2-1 所示。

· ·	386913 10 101	
入险大盘	智能蜜网	智能蜜网 浙江新能自动化部署快速形成改善新网
8	沙箱配置 ヘ	① 提示
安全大屏	沙箱管理	◆ 一續與測 探测之后会出现大量的扫描行为,请确认是否要发 申報节点 你接代理 起探测?
: 威胁情报	IP管理	
-	伪装代理	取 消 國 定 中继节点 伪装代理
新知知 起	中继节点	最近探测时间:
报表管理	攻击诱捕 🔦	
	攻击反制	 ● 192.168.110.190 未存差半致: -
	邮件诱饵	192.168.50.67
0	办公网诱饵	未存落P数(-
配置管理	文件诱饵	
二 日志审计	主机诱饵	
開始成為	互联网诱饵	
max row	感知节点	

图 3-5-2-1 蜜网导图

对于中继节点模块,对于扫描到的未存活 IP,用户可以进行选择,并将其添加至 IP 管



令 同時大盘	蜜阿导图 智能蜜网	 ◇ 一键探测 ○ 中盤节点 ○ 伪装代码 	发起探测	93 一键关联 □ 中继节点 □ 伪装代理	生成蜜网			
· 安全大屏	沙箱配置 <	中爆节点 伪装代理						
E Reference	P管理	最近探测时间:2022-05-0)5 15:16:28					
· · · · · · · · · · · · · · · · · · ·	伪装代理 中继节点	■ 192.168.124.22 未存活P数: 0	192.168.124.33					
NA BE	攻击诱捕 ^	 192.168.124.33 未存活印数: 237 	发起探測P		Vlan ID	未存活P数	操作	I Vian ID: 124
C UKARM	攻击反制 邮件诱饵		192.168.124.12		124	237	8	選口分布情况
	办公网诱饵				共1条 < 1 >	10 条/页 >>		22 8443 7070 6379 3306
Entra	文件透饵 士机递相							系统分布情况
E Sant	互联网诱饵							
******	感知节点							未存活IP 已选择 2个
								192.168.124.7
								192.168.124.9
								192.168.124.10
		已选择P数: 2 加入中	·###/*# 0					

理中。如图 3-5-2-2 所示。成功添加后,可以在中继节点-IP 管理页面查看所添加的 IP。



中继节点模块可以查看不同 VLANID 下自动关联沙箱的情况。点击" ¹ "图标,即可带 VLANID、关联方式的方法跳转到中继节点-节点详情-IP 管理界面。

e Ritta	智能蜜网	节点详情			
8	沙箱配置 ^	Vian管理 P管理			
X1./10	沙箱管理				
(2) 成初情报	IP管理	半连接感知 ③ ()]]			+ 35.00P
-	伪装代理	关联沙箱 全部 🗸 VianiD 全部 🗸	关联方式 自动关联 🗸		PQ
新田田 田	中國节点				
NAME.	攻击诱捕 🔦	IP地址	VianiD	关联沙箱	操作
	攻击反制				
联动配置	邮件诱饵	192.168.124.3 📴	124	22 co ssh2hao	×
	办公网诱饵	192.168.124.5 G	124	22 oo ssh2hao	Z
C.R.R.R.	文件诱饵	192.168.124.6 🔮	124	22 co ssh2hao	2
日志审计	主机诱饵				
10 10 10 10 10 10	互联网诱饵		共3条 < 1 >	9 10 洜/页 ∨	
	感知节点				

图 3-5-2-3 中继节点带筛选跳转

伪装代理模块,针对子网信息进行扫描,点击查看详情按钮,可以带关联方式筛选跳转 至伪装代理-IP 管理模块。



智能推网	智能蜜网 通过智能自动化部署快速形成政策重网			
沙箱配置 へ 沙箱管理 IP管理	 ◆ 一號探測 > 一號探測 ○ 中級节点 ○ 伪装代理 	℃ 一種关联 生成電网 中間や点 ⑦ 外裂代理		
伪装代理	中華节点 伪装代理			
中継节点 攻击诱捕 へ	最近探测时间: 2022-05-05 15:16:28			安相详情
攻击反制	发起探测P	子网信息	未存活印数	I子网信息 192168 180 55/24
邮件诱饵	192.168.180.55	192.168.180.55/24	136	端口分布情况
办公网诱饵	192.168.31.81	192.168.31.81/24	159	1 com
文件诱饵 主机诱饵				22 80 3306 111 8080
互联网诱饵		共 2 余 < 1 > 10 条/页 ∨		系统分布情况
感知节点				*ta vindows
				未存活iP
				192.168.180.8 192.168.180.11
				192.168.180.15 192.168.180.16

图 3-5-2-4 伪装代理带筛选跳转

探测并完成绑定沙箱之后(伪装代理及中继节点绑定沙箱方式可查看伪装代理、中继节 点模块说明),用户可以点击智能蜜网页面顶部——一键关联模块,选择中继节点或伪装代 理,生成密网,即可将最新的关联信息更新至密网导图页面。如图 3-5-2-5 所示。

重网导图	=			🌲 🕘 💄 admin 🗸
智能徵列	智能蜜网 通过智能自动化部署快速形成欺骗服网			
沙箱配置				
金大厨 沙箱管理	◆ 一键探测 发起探测	Sa 一键关联 生成骤网		
· P管理	中继节点 伪装代理	🗋 中雄节点 🔽 伪装代理		
伪装代理	中继节点 伪装代理			
中继节点				
10 表管理 攻击诱捕	職立1時周時1月1:2022-05-05 15:10:28 へ			建合种情
攻击反制	发起探测P	于网信息	未存活P数	Ⅰ 子网信息
动配置 邮件诱饵	192.168.180.55	192.168.180.65/24	136	192.108.180.55/24 編口分布情况
办公网诱钮	102 169 21 81	10.2 169 21 91/24	160	
^{直管理} 文件诱饵	- HARLING AND THE	to all house had by all t	1970	I 1 1 1 1 1
5. 电机诱饵		#26 2 1 108/77 2		22 80 3306 111 8080
互联网诱饵	20			系统分布情况
60中心 感知节点				linux (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)
				windows I
				未存活吗
				192.168.180.8 192.168.180.11
				192.168.180.15
				19/2, 100, 100, 10

图 3-5-2-5 一键关联智能蜜网生成

3.5.3 沙箱管理

沙箱主要用于吸引攻击者入侵;普通用户权限只能看到相关沙箱基本信息,不能对沙箱进行操作,比如新建沙箱,重启沙箱、停用沙箱等相关操作。管理员权限不能删除沙箱。

用户可根据实际需求,对沙箱设置事件灵敏度,事件灵敏度设置分为高、中、低三个级别,事件灵敏度设置为'高'时:系统会上报该沙箱的所有相关事件,包括所有攻击事件和所有探测事件,事件灵敏度设置为'中'时:系统会上报该沙箱的所有入侵事件和高危探测事件,



事件灵敏度设置为'低'时:系统会上报该沙箱的所有入侵事件。

沙箱管理页面主要用于展示所有沙箱信息以及对沙箱的相关操作,展示的信息包括沙箱 类型、关联 IP、沙箱状态,其中关联 IP 可上浮展示所有。支持按照设备、沙箱类型和运行 状态进行查询;沙箱信息默认按照图标形式展示,也可以点击页面右边' 💷)按钮切换至 列表模式。如下图:

e ta	智能蜜网	沙箱管理 通过在核心系统上部署沙瑞来探测攻击						退逸检测 🕖
	沙箱配置 🔺	设备 所有设备 🗸 服务类型 全自	β ~ ~	沙箱来源 全部			配置沙箱漏	月 + 創建沙和
大屏	沙稽繁理	秋态 全部 未启用 活动中 已停止					沙箱名称/关联印/沙箱类型	Q :: =
5 188	模板管理							
-	IP管理	OA_LWS II B	#合	11 11 10	oa	11 10 (0)	q_sqlserver	II 8 0
	伪装代理	沙箱类型: OA	活动中 沙箱类型:组合	含沙箱 7个服务 活动中	沙箱类型: OA	活动中	沙箱类型: SQLSERVER	活动中
PR .	中继节点	关联IP: 192.168.110.208	<u>業校中</u> 关联ⅠP: 192	.168.110.32 监控中	关联P: 192.168.110.20	8 篇段中	关联IP: 192.168.110.201	编控中
	攻击诱捕	关联iPv6: -	*.照透 关联/Pv6: -		关联(Pv6: -	未廃置	关联IPv6: -	
EH.	诱饵欺骗 ヘ	× • • •	Z 🖬 🔺		2 8 A A		2 8 1	
	邮件诱饵	内面	AB		内面		P12	100 100 10
~	办公网诱饵	w_portcheat	CONFLUEN	ICE 🕒 🖪 🕑	w_vpn	II II O	crm置烟test	
tt -	文件诱饵	沙箱类型: PORTCHEAT	活动中 沙箱类型: CO	NFLUENCE (未启用	沙箱类型: VPN	活动中	沙箱类型: CRM	活动中
	主机透彻	关联IP: -	<u>展校中</u> 关联IP: -	*22	关联IP: 192.168.110.20	27 重照中	关联IP: -	2124
b.	100 PM 07 08 09	关联IPv6: -	关联IPv6: -	in the second se	关联Pv6: -	County of County	关联IPv6: -	and a
	互联网防旧	× = +	Z 8 A	*	∠ ■ ± ±		Z 🛛 A 🕹	
	感知节点	() () () () () () () () () () () () () (0.00		0 E	
		w_mysqlcheat II a	• w_进程监控	II 🔳 O	Its	II 🗰 🔿	q_tomcat	11 🔳 0
		沙箱类型: MYSQLCHEAT	活动中 沙箱类型:TO	MCAT ISIOP	沙箱类型: WIKI	活动中	沙箱类型: TOMCAT	活动中
		关联IP: 192.168.110.203	<u>盖控中</u> 关联P: 192	.168.110.202 篮担中	关联沪: 192.168.110.20	24 监控中	关联IP: 192.168.110.205	监视中
		关联IPv6: -	关联(Pv6: -	未測證	关联(Pv6: -	未用度	关联IPv6: -	潮源中
		Z 🖬 🔺	2 8 8	4	2 8 8 4		2 8 8 A	

在漏洞设置后增加下载 pcap 功能,如下图所示。

重网导图						- durini -
智能蜜网	沙箱管理 通过在核心系统上都著沙箱来探测改击					isistén 🕥
沙箱配置 ^	设备 所有设备 > 服务类型 全部	pcap包下载	×		配置沙積漏洞 + 示:	10/9 TA 88 E
沙和管理						
IP管理	win7sx II 🛢 O			II 1 0	sb_ssh	11 B O
伪装代理	沙箱类型: WN7-PC 图20中	日 时间 名称	大小	活动中	沙箱类型: SSH	活动中
中態节点	关联IP: 192.168.110.161 第25年			1212-9	关联IP: -	(1112中)
攻击诱捕 ヘ	关联iPv6: -			(ARR)	关联IPv6: -	
攻击反制		智无数据			× 8 4	
邮件透信						
办公网诱饵	t_ssh II 🛙 O			11 10 0	AO	11 0
文件诱信	沙箱类型:SSH (清和中)		取消 下载	活动中	沙箱类型: OA	活动中
1. 11 05-10	关联IP: 192.168.110.164 (11899年)	A STATE OF THE OWNER OWNER OF THE OWNER	A COLORIDA	*212	关联IP: 192.168.110.169	*20
Tarage	关联IPv6: -	关联IPv6:-	关联的6: -	(A.M.4)	关联IPv6: -	
. ALIK MY USTA	< 8 ±	× 8 8 ×	× 8 # ±		× 8 8 ±	
德知节点						
	t_wiki II 🗈 o					
	沙箱类型: WIKI (活动中)					
	关联IP: 192.168.110.165 (未回答)					
	关联iPv6: -					
	2 B A 2					

图 3-5-3-2 pcap 下载

注: 为了保证性能,根据性能对设备的沙箱数量做了相应限制。低配设备启动 windows 沙箱数量最多为1个。中配设备启动 windows 沙箱数量最多为2个。高配设备 windows 沙箱 数量最多为3个。(仅标准版支持)



1) 应用服务沙箱

wiki 沙箱为例

创建 wiki 沙箱, 蜜网管理-->沙箱管理-->创建沙箱-->服务类型(应用服务)-->选择 WIKI:

"沙箱配置"中输入沙箱名称、选择端口(可设置, 默认 80 端口)、可选设备;

"告警设置"选择邮件告警选择(全部/严重/高危及以上/中危及以上),完成告警设置;

"HTTPS 证书设置",用户可自定义选择是否开启此开关来启用 HTTPS。如果决定启用,用户需要将证书文件(*.crt/cer/pem)和私钥文件(*.key)打包成 zip 格式后再导入。

选择 确定添加/取消, 完成添加沙箱操作。

疟蜜网 疳配置 へ	* 沙箱名称 test_wiki			*可透设备 192.168.110.200	~	邮件告營等级 全部 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	启用HTTPS ◎		
日智理 6理	1 应用服务	20	^	已选服务 服务数: 1/8					
5管理 表代理	CRM				• 应用服务				
南	BRS				WIKJ 180:80			× 1	
:访捕 欺骗 ^	BBS	TOMCAT	MAILBOX						
透信	JBOSS	ZBX	Struts ² STRUTS2						
访口 诱饵 网诱饵	JENKINS	WEBLOGIC	VPN						
节点	Discuz!	ECSHOP	ESPCMS						

图 3-5-3-3 wiki 沙箱

添加沙箱完成后,会跳转到沙箱管理页面,新建的沙箱默认是未启用和未监控状态。设置完成之后,沙箱管理页面-->启用沙箱 ▶ (所有应用服务沙箱启用沙箱、验证沙箱操作步骤一致)如图所示:



test_wiki	
沙箱类型: WIKI	未启用
关联IP: –	未监控
关联IPv6: -	未溯源
2 3 1	

图 3-5-3-4 启用沙箱页面

wiki 沙箱是半自定义沙箱,编辑沙箱 —>可以对沙箱名称、行为灵敏度(选择 高/ 中/低)、流量阻断(开启/关闭)、日志监控、邮件告警等级、沙箱关联 IP、溯源设置、 网站 url_path 路径、漏洞类型进行调整;事件灵敏度默认设置为'高',流量阻断默认为开启, 日志监控默认'关闭'状态,日志监控是对该沙箱所产生事件是否上报进行设置。"溯源设置" 选择 是否开启溯源开关,完成溯源设置配置和浏览器反制配置;"网站 url_path 路径"支 持自定义添加路径、特征字符串、替换方式(替换/向前追加/向后追加),完成指定在特定 URL 下插入 JS 设置。 对于半自定义 wiki 沙箱,用户可在 wiki 沙箱里面设置一些类似企 业内部敏感信息的文档等(比如其他沙箱的信息,让攻击者在蜜罐之间跳转),建议用户在 对沙箱里面内容调整设置时,可关闭日志监控,避免用户操作事件上报,操作设置完成之后, 开启日志监控;如下图沙箱设置。漏洞设置可对沙箱关联的漏洞进行修改。

31

沙箱名称	test_wiki		行为	〕灵敏度 🕜	高		~		
流量阻断 📀	开启		∨ 日≉	监控	关闭		~		
邮件告警等级	全部		∨ 沙箱	i关联IP 📀					
沙箱关联IPv6 💿									
应用设置									
WIKI									
溯源设置	л								
网站url_path路	径	特征字符串 🔞		替换方式		替换方式	浏览器反制 🞯	免责声明	+
/xx/xx				替换	~	● 设备指纹+社交信息 ∨			-
漏洞设置 漏洞	详情设置								
	不添加		v						
漏洞类型									
漏洞类型									

图 3-5-3-6 沙箱设置

沙箱状态变为'活动中'监控状态变为'监控中'时,沙箱成功启动,可以关联 ip,在关联 ip 上开放了 80 端口,浏览器通过关联 IP 访问,显示 wiki 界面,如下图 wiki 页面。

PmWiki Main / HomePage	× +					
← → ♂ ŵ						≡
RWiki		Recent Changes - Search:				Go
wiki主页 新人概要各地址文档 期试版产信息 物端资料 的端选料 的端选时表示后铺接口 后端开发使用技术简介 redis命名规范 edit SideBar	Main / HomePage 公司wik		View	Edit	listory	Print
	Edit - History - Print - Becent Changes - Search Page last molified on December 06, 2018, at C412.1 AM					

图 3-5-3-7 wiki 页面

在沙箱管理界面上选择要停用的沙箱点击^(Ⅲ),沙箱状态变为'未启用',表示已停用;点 击^(圖),即删除沙箱;点击⁽),即将沙箱恢复到沙箱初始状态。如下图操作沙箱。

獣安科技



test_wiki	
沙箱类型: WIKI	活动中
关联IP: 192.168.110.183	未监控
关联IPv6: _	溯源中
2 🖪 🕱 🛓	

图 3-5-3-8 操作沙箱

查看沙箱 ^(II) ->可以查看当前沙箱基本信息和服务配置信息;沙箱基本信息包括:沙箱 ID,沙箱类型,沙箱名称,设备 IP,沙箱状态,运行时间,行为灵敏度,办公网诱饵数、伪 装代理个数、关联中继节点 IP 数等;服务配置信息包括服务名,服务图标,端口,服务配 置,WEB 漏洞数,溯源状态,浏览器反制,git 泄露反制,svn 泄露反制,goby 反制等,如 下图查看沙箱页面:

沙箱类型:WIKI	
设备IP:192.168.110.200	
运行时间:0分0秒	
监控日志:关闭	
办公网诱饵数:0个	
伪装代理个数:0个	
	关闭
	沙箱类型:WIKI 设备IP:192.168.110.200 运行时间:0分0秒 监控日志:关闭 办公网诱饵数:0个 伪装代理个数:0个

图 3-5-3-9 查看沙箱页面

web 漏洞设置页面,可对漏洞进行添加、编辑、修改,删除操作,漏洞、诱饵、伪装代理的详细操作参考 3.5.4 伪装代理模块)漏洞设置和 3.5.6 诱饵设置(**所有应用服务沙箱伪** 装代理、漏洞设置、诱饵管理操作步骤一致)。



图 3-5-3-10 web 漏洞设置页面

注: 应用服务类沙箱支持类型包括(CRM、OA、WIKI、BBS、TOMCAT、MAILBOX、JBOSS、 ZABBIX、STRUTS2、JENKINS、WEBLOGIC、VPN、DISCUZ、ECSHOP、ESPCMS、WEBSPHERE、PHYPMYADMIN、 CONFLUENCE、JOOMLA、HADOOP)

2) 系统服务沙箱

SSH 沙箱为例

创建 ssh 沙箱, 蜜网管理-->沙箱管理-->创建沙箱-->服务类型(系统服务)-->选择 ssh:

"沙箱配置"中输入沙箱名称、可选设备、SSH 登录名、SSH 登录密码、确认密码,其 中密码长度为 5 到 18 之间的字符串,并支持特殊字符,如@, #等。如图所示

"告警设置"选择邮件告警选择(全部/严重/高危及以上/中危及以上),完成告警设置; 选择确定添加/取消,完成添加沙箱操作。

冒能蜜网	*沙箱名称	* 可选设备	邮件告警等级	启用HTTPS 💿	
▶箱配置 ^	test_ssh	192.168.110.200	~ 全部 ~		
▶箱管理					
管理	X (?)	已选服务 服务	务数: 1/8		
莫板管理	JOOMLA HADOOP		 系统服务 		
内装代理	▲系统服务 13	~	SSH		4.0
中继节点			(ssh 端口: 22		
文击诱捕	ssh samba	MySQL	SSH登录名: root	数据仿真: 开启	
秀饵欺骗 へ	SSH SAMBA	MYSQL	SSH登录密码: 1		
8件诱饵		M			
小公网诱饵	FTP REDIS	MEMCACHED			
文件诱饵					
E机诱饵	🔊 🚿	2			
互联网诱饵		MYSQLCHEAT			
泉知节点					

图 3-5-3-11 SSH 沙箱

SSH 沙箱被创建并启用后,用 SSH 连接上去,成功登陆后,执行任意命令,在威胁情报 管理-->查看事件处,如果看到入侵则表示 ssh 沙箱运行正常,如下图事件列表。 点击查看攻击事件回放便可看到详细信息,如下图所示



牛回放		
		隔离沙箱 SSh
曰指工具类型 未30 攻击者mact地址 来30	和理心置 机州 (115.238.55.14) 机州 (115.238.5.58)	网络D 未知
关键攻击路径		
2022-04-25 1123.48 文士書: 192.585.00.39 双士書: 192.585.00.39 双士書: 554,周产名为: not, 图称为: 1 23	(<u>@9887</u>) (金9887) 東山東道道SS-484(7)66 全	
• 0 2022-04-25 11:23:48 攻击记录	0 2022-04-25 11:23:50	· · · · · · · · · · · · · · · · · · ·
攻击时间 开始时间 一 结束时间	所有资产 > 攻击手法 全部 >	来避归/攻击行为 Q
●FF央配 王部 V ATT&CK 全部 V		制的投入
攻击时间 \$ 攻击资产 来源P	类型 攻击手法 攻击行为	操作
2022-04-25 11:24:15 - 192.16	5.100.39 探測 第口扫描 攻击者在30s内建立1条恶意 TCP 连接。 攻击者将测了 22 端口	

图 3-5-3-13 攻击事件回放

 注:系统服务类沙箱支持类型包括(SSH、SAMBA、MYSQL、FTP、REDIS、MEMCACHED、SQLSERVER、 PORTCHEAT、MYSQLCHEAT、MONGODB、TELNET、ADB、POSTGRESQL); SSH 沙箱事件支持 视频回放。

3) Windows 沙箱(仅标准版支持)

WIN7-PC 沙箱为例

创建 win7-pc 沙箱, 蜜网管理-->沙箱管理-->创建沙箱-->服务类型 (windows) --> 选择 WIN7-PC:

"沙箱配置"中配置中输入沙箱名称、可选设备、登录用户名、登录密码、确认密码, 其中密码长度为 5 到 18 之间的字符串,并支持特殊字符,如@, #等。

"告警设置"选择邮件告警选择(全部/严重/高危及以上/中危及以上),完成告警设置; 选择确定添加/取消,完成添加沙箱操作,如图所示:



智能蜜网	* 沙箱名称	* 可选设备	邮件告警等级	启用HTTPS 💿	
沙箱配置 ^	test_win7	192.168.110.200	全部 >		
沙箱管理		口洗服条 四条款 1/0			• 当前遗憾和名子士诗文明名明会
IP管理	(R)	1/8			• 目前运律服务个又行多级方组合
模板管理	POSTGRESQL	• Wind	dows		
伪装代理			WIN7-PC		2 10
中继节点	Windows 3	^			
项□防捕 透明散幅		R 皇	DP 端口: 3389 發用户名: administrator	登录密码: 1	
邮件诱饵	WIN7-PC WINSERVER WINXP 2008	-PC s	MB 端口: 445		
办公网诱饵	1 丁价阳夕 7		t录用户名: administrator	登录密码: 1	
文件诱饵					
主机诱饵					
互联网诱饵					
感知节点	BAC S7	>			
		5 1 6.5	定创建 取 消		

图 3-5-3-14 win7-pc 沙箱

◆ win7-pc 沙箱被创建并启用, 假如沙箱 IP 是 192.168.199.227, win7-pc 验证方式如下:

a. 3389 远程桌面连接,

b. mysql 远程连接, 账户名密码为沙箱启动设置的账户名密码

c. ipc连接, net use \\ip\c\$ "pass" /user:"username"spsexec \\ip cmd.exe
 验证之后, 在威胁情报管理-->查看事件处, 有事件记录表示沙箱运行正常.

◆ WIN2008-SERVER 沙箱被创建并启用, win2008-server 验证方式如下:

a. 3389远程桌面连接

b. sqlserver弱口令连接

c. ipc连接, net use \\ip\c\$ "pass" /user:"username"spsexec \\ip cmd.exe
 验证之后, 在威胁情报管理-->查看事件处, 有事件记录表示沙箱运行正常。

d. 利用 nmap 工具执行命令: nmap --script smb-vuln-ms17-010.nse ip 验证之后, 在威胁情报管理-->查看事件处, 有事件记录表示沙箱运行正常

◆ Winxp-pc 沙箱被创建并启用, 检测 ms08067 漏洞。

利用 nmap 工具执行命令: nmap --script smb-vuln-ms08-067.nse -p445 <host> 在威胁情报管理-->查看事件处,有事件记录则表示沙箱运行正常。


亘有手	*** 将不同攻击者对不同沙箱的攻击事件	牛单独归并,分别展示为事件					
发击者	全部 > 攻击资产 所有	有资产 🗸 隔离沙箱	所有沙箱 🗸 🗸	事件类型 全部 >			攻击源 Q
风险等级	全部 > 攻击时间	开始时间 - 结束	MA 🗖				隐藏白名单内的攻击事件
过滤IP	请输入过滤的IP。多个IP之间用英文调	号分隔					
攻击者	攻击源 💿	攻击资产	隔离沙箱	开始攻击时间 😄	最近攻击时间 😄	风险等级 😄	操作
H-0008	192.168.30.251	-	win7	2019-12-19 15:03:08	2019-12-19 15:03:08	♥ 中愈	8
H-0005	192.168.30.4		oa	2019-12-19 14:16:56	2019-12-19 15:02:39	♥ 中危	
H-0005	192.168.30.4	-	mailbox	2019-12-19 12:10:20	2019-12-19 15:02:32	☞ 严重	
H-0008			mailbox	2019-12-19 13:57:11	2019-12-19 14:45:10	♥ 严重	
H-0008	192.168.30.251	-	final_test_s	2019-12-19 14:22:48	2019-12-19 14:34:20	☞ 严重	
H-0008		-	jenkins	2019-12-19 13:57:59	2019-12-19 14:26:28	☞ 严重	
未知	192.168.100.192		win7	2019-12-19 14:04:41	2019-12-19 14:22:35	の任命	
H-0003	192.168.30.14	T 2	win7	2019-12-19 13:51:41	2019-12-19 13:59:40	☞ 中急	
H-0007	192.168.30.251		jenkins	2019-12-19 13:58:30	2019-12-19 13:58:33	☞ 中急	
H-0008	192.168.100.140	-	wiki	2019-12-19 13:56:05	2019-12-19 13:56:42	☞ 中危	

共42条 < 1 2 3 4 5 > 10条/页 跳至 页

● 注: windows 类沙箱支持类型包括 (WIN7-PC、WIN2008SERVER、WINXP-PC)

4) 工控沙箱

IPMI 沙箱为例

创建 ipmi 沙箱, 蜜网管理-->沙箱管理-->创建沙箱-->服务类型(工控沙箱)-->选择 ipmi:

"沙箱配置"中输入沙箱名称、选择端口、可选设备、IPMI 用户名、IPMI 密码、确认密 码,其中密码长度为 5 到 18 之间的字符串,并支持特殊字符,如@, #等;

"告警设置"选择邮件告警选择(全部/严重/高危及以上/中危及以上),完成告警设置; 如图所示



图 3-5-3-15 事件列表



图 3-5-3-16 ipmi 沙箱

添加沙箱后,启动沙箱,当沙箱状态变为'活动中',监控状态变为'监控中'时,表明沙箱 已经在运作。

沙箱类型:	IPMI
关联IP:	192.100.110.1
关联IPv6:	2 ²
沙箱状态:	监控中 活动中 ②

图 3-5-3-17 启用沙箱页面

这时可在主机或虚拟机上通过 apt-get install -y ipmitool 的命令,安装 ipmi 工具后, 使用 ipmitool -I lan -H(ip 地址) -U (登录名)shell,输入 password,进入 IPMI 交互

模式,或可以 shell 直接换成 bmc 命令。

apt-get install ipmitool root@ubuntu1:~ 读取软件 列表 分析软件 包的依赖关系树 正在读取状态信息... 完成 ipmitool 已经是最新版 (1.8.16-3ubuntu0.2)。 升级了 0 个软件包,新安装了 0 个软件包,要卸载 0 个软件包,有 有被 装或卸载。 后会消耗 ов 的额外空间。 执行吗? [Y/n] y正在设置 nginx-core (1.10.3-0ubuntu0.16.04.5) ... root@ubuntu1:~# ipmitool -I lan -H 192.168.110.166 -P ipmi she ıι root@ubuntu1:~# ipmitool -H 192.168.110.166 -I lanplus -U ipmi -P 123456 power status chassis Power is off

图 3-5-3-18 攻击 IPMI 沙箱

成功进入 IPMI 沙箱后,执行任意命令,在威胁情报管理-->查看事件处,如果看到入侵则表示 IPMI 沙箱运行正常,如下图事件列表。



攻击时间 ⇔	攻击资产	来源IP	类型	攻击手法	攻击行为	操作
2022-01-13 16:02:33	-	192, 117, 11667	探測	端口扫描	攻击者在30s内建立 11 条恶意 UDP 连接	
2022-01-13 16:02:02	-	1.2.45 (11	探測	豐出	攻击者断开60063號口与IPMI协议的连接	
2022-01-13 16:02:02	-	101.247.77	入侵	命令执行	攻击者通过60063端口使用IPMI协议,重新设置IPMI工控设备会话权限	
2022-01-13 16:02:02		107 million 200	入侵	命令执行	攻击者通过60063端口使用IPMI协议,IPMI工控设备操收到无法识别的命令	
2022-01-13 16:02:02	-	Lat. Maddan	入侵	命令执行	攻击者通过60063端口使用IPMI协议,IPMI工控设备接收到无法识别的命令	
2022-01-13 16:02:02	-	0.116,1000	入侵	命令执行	攻击者通过60063端口使用IPMI协议,IPMI工控设备操收到无法识别的命令	
2022-01-13 16:02:02	-	191244	入侵	敏感信息 探測	攻击者通过60063論曰使用IPMI协议,对IPMI工控设备发送了指令:请求获取电源状态	
2022-01-13 16:02:02	-	125.06140.00	入侵	豐出	攻击者通过60063蹁口使用IPMI协议,关闭IPMI工控设备会话	
2022-01-13 16:02:02	-	R.2.07, 2069	探测	尝试访问	攻击者通过60063端口建立IPMI协议的访问	
2022-01-13 16:01:22	-	0.046.00.00	探測	端口扫描	攻击者在30s内建立 22 条恶意 UDP 连接	

图 3-5-3-19 幻阵告警

5) 漏洞设置

漏洞设置页面主要是在自定义沙箱、应用服务类沙箱中添加漏洞,根据沙箱的语言类型 选择不同的语言类型(PHP、ASP、JSP)添加相应的漏洞,攻击者访问该 web 漏洞时,抓取 攻击者的设备指纹,新建沙箱 web 漏洞默认为不添加。

通过沙箱管理界面点击"配置沙箱漏洞",如图:

38.MITTEL	lan an a							
智能蜜网	沙箱管理 通过在核心系统上部署沙翁	8来探测攻击						逃逸检测 〇〇〇
沙箱配置 ヘ	设备 所有设备 >	服务类型 全部	∨ 状态 全部 3	R启用 活动中 已代	B <u>alt</u>		配置沙箱漏洞 +	彩加沙箱 🛛 🗧
沙箱管理								
IP管理	sb_oa	II 💼 O	win7sx	II 🗰 🔍	t_crm	II 🗰 O	sb_ssh	11 1 0
伪装代理	沙箱类型: OA	活动中	沙箱类型: WIN7-PC	活动中	沙箱类型: CRM	活动中	沙箱类型: SSH	活动中
中继节点	关联IP: 192.168.110.162	未监控	关联IP: 192.168.110.161	监控中	关联IP: 192.168.110.168	未嘉控	关联(P: -	监控中
攻击诱捕 🔦	关联IPv6: -	未開原	关联IPv6: -		关联IPv6: -	未開選	关联IPv6: -	
攻击反制			Z B A		Z 8 X 4		2 8 4	
邮件诱饵								
办公网语饵	t_ssh	II 🛢 0	t_oa	11 0 0	t_cus	II 8 0	OA	II 🛛 O
文件课程	沙箱类型: SSH	活动中	沙箱类型: OA	活动中	沙箱类型:自定义	活动中	沙箱类型: OA	活动中
	关联IP: 192.168.110.164	监控中	关联IP: 192.168.110.167	未监控	关联IP: 192.168.110.166	未监控	关联IP: 192.168.110.169	未监控
土 (1,151)4	关联IPv6: -		关联IPv6: -	潮道中	关联IPv6: -	未用温	关联IPv6: -	*##
互联网诱饵	∠ □ ▲		× 0 1 A		× 0 * 4			
感知节点								
	t_wiki	11 2 0						
	沙箱类型: WIKI	活动中						
	关联IP: 192.168.110.165	未嘉控						
	关联IPv6: -	未販原						
	× 8 * ±							
				共9条 <				

图 3-5-3-23 配置沙箱漏洞 1

通过沙箱列表点击"配置沙箱漏洞",如图:



test_wiki	0
少箱类型: WIKI	活动中
关联IP: 192.168.110.183	未监控
关联IPv6: -	溯源中
关联IPv6: -	

图 3-5-3-24 配置沙箱漏洞 2

添加 web 漏洞,点击沙箱右上角的^{() ()} (漏洞设置)按钮,即跳转到漏洞设置页面,如下图。

扇洞名称	附有漏 洞	×	关联沙箱	所有沙箱	×				+ 添加web漏)
□ 漏洞	名称	漏洞地址				关联沙箱	应用服务	状态	操作
php.	后台登录漏洞	http://192.1	168.110.207	7:80/Admin/index.php		Leak_test	CRM	• 已发布	2
php;	文件上传漏洞	http://192.1	168.110.207	7:80/upload.php		Leak_test	CRM	• 已发布	2

图 3-5-3-25 漏洞设置

点击右上角添加 web 漏洞,漏洞类型可选漏洞包和单条漏洞,选择 web 漏洞的关联沙箱,如 果关联沙箱是自定义沙箱,需要选择和自定义沙箱的仿真业务系统一致的网站语言,应用服 务类沙箱可选取 PHP、ASP、JSP 三种语言的其中一种,如下图添加 web 漏洞页面:



箱 wx测试TOMCAT	\sim				
		4.545.494	et man ér	N.D+-	411 /A-
服务 TOMCAT ×		大アジオ目	应用服务	机动	採作
刑		k_test	CRM	● 已发布	
堂 满利已	· ·	k tost	CRM	- 口坐左	
言 PHP	~	in_toat	Gravi		
	HT VE				
	4X /月 / / / / / / / / / / / / / / / / / /	Æ			
	服务 TOMCAT × 理 漏洞包 PHP	服务 TOMCAT × 型 漏洞包 ···································	服务 TOMCAT × 型 漏洞包 ✓ 洁 PHP ✓ 取消 确定	服务 TOMCAT X 型 漏洞包 V 信 PHP V 取消 确定	服务 TOMCAT × 理 漏洞包 ~ 注 PHP ~ 取消 确定

图 3-5-3-26 添加 web 漏洞页面

漏洞类型包含如下:文件上传漏洞、后台登录漏洞、数据库后台登录漏洞、服务器后台 登录漏洞、安装信息泄露漏洞。

添加完成之后回到 web 漏洞设置界面,此时添加的 web 漏洞还未生效,还可对单条 web 漏洞进行编辑、删除操作;如下图 web 漏洞管理页面:

漏洞名称	漏洞地址	关联沙箱	状态	操作						
php目录浏览漏洞	http://192.168.110.167.80/backup/	t_oa	• 已发布							
php安装信息泄露漏洞	http://192.168.110.167:80/phpinfo.php	t_oa	 已发布 							
php服务器后台登录漏洞	http://192.168.110.167-80/wamp/index.php	t_oa	 已发布 							
php数据库后台登录漏洞	http://192.168.110.167.80/phpmyadmin/index.php	t_oa	 已发布 							
php后台登录漏洞	http://192.168.110.167.80/Admin/index.php	t_oa	 已发布 							
php文件上传漏洞	http://192.168.110.167-80/upload.php	t_oa	• 已发布							
共 6 条 < 1 > 10 条/页 >										

图 3-5-3-27 web 漏洞管理页面

选择需要发布的漏洞,点击'发布'按钮,状态变为'已发布'之后,几分钟后,规则下发到 沙箱,访问漏洞列表'已发布'的漏洞地址,能访问到漏洞页面表示该条 web 漏洞添加完成, 如下图沙箱漏洞页面:



💠 蜜网管理 - 漏洞设置	×	Index of /templets	🗙 💠 诱饵管理	× +
⊖ → ୯ ଢ		🗊 🔏 192.168.11	0.113/backup/	
ndex of /te	emp	lets		
 Parent Directory default/ 				
 <u>lurd/</u> <u>plus/</u> 				
system/ tomplet diricting				
 templet-diffict.ind templet-filelist ind 	2			
 templet-pluslist.ii 				

图 3-5-3-28 沙箱漏洞页面

3.5.4 IP 管理

IP 管理页面展示了 IP 地址、关联沙箱、关联设备、状态以及操作,并且可以根据关联 类型和 IP 进行筛选,右侧有添加 IP 按钮可以进行 IP 的添加,如下图所示:

智能蜜网	IP管理				+ JØ20IP
沙箱配置 ^	关联类型 全部 🗸 关	联设备 全部 🗸		6	Q
屏 沙箱管理					
模板管理	IPtest/	失眠沁露	关联份券	拔态	操作
P管理					
伪装代理	192.16	ssh	192.1	 已使用 	
中继节点	192.16	rrdp	192.1	 已使用 	
攻击诱捕	192.16	ssh冒烟	192.1	• 已使用	1
访饵欺骗 ^ 邮件诱饵	192.16	MYSQLCHEAT	192.1	 已使用 	
办公网诱饵	192.16	wbcl	192.1	 已使用 	
文件语饵	192.16	sshiws	192.1	 已使用 	
主机诱饵	192.16	https	192.1	 已使用 	
感知节点	192.16	lt_smoking_l4	192.1	 已使用 	
	tec0:0	t_wc3	192,1	• 已使用	
		共	9条 < 1 > 10条/页 <		

图 3-5-3-28 IP 管理页面

3.5.5 模板管理

模板管理页面展示云沙箱模板、自定义模板和内置模板;



Hama Hama Data	10000000000	
PARE • PARE • <td< th=""><th>智能蜜网</th><th>模板管理</th></td<>	智能蜜网	模板管理
1 Adda • C Adda Adda 1 Adda • C Adda	沙箱配置 ヘ	
RETR Pdf Pdf <td< td=""><td>¹¹沙箱管理</td><td>1 云沙箱 (0) 亿 前往 (沙稽市场)</td></td<>	¹¹ 沙箱管理	1 云沙箱 (0) 亿 前往 (沙稽市场)
PEE 57.000 PE 57.000 PEE 57.000 <	模板管理	
9 48/12 9 48/12 9 48/12 9 48/12 9 48/12 9 1 82 (2) + 81/8 (2) 9 1 82 (2) (2) + 81/8 (2) 9 1 82 (2) (2) (2) (2) (2) (2) (2) 8 4/13 9 1 82 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	P管理	
• #252 • #32 • #32 • #32 • #32 • #32 • • • • • • • • • • • • • • •	伪装代理	新元模板
Xd:Hid Image: State of the state of t	中继节点	1 自定义 55 十 版證模紙
RURSE COLOC Writki Dot Coloc	攻击诱捕	
新行信	诱饵欺骗 ^	ele cisco xmhki test ele ele de sopi
Λ2/8 (51) Image: Sope 1 Image: Sope 2 Image: Sope 2 <td>邮件透饵</td> <td></td>	邮件透饵	
空炉街面 sop1 sop2 log4 sppo zz zzmi 主机铸面 互原用音加 PB PB PB PB PB PB 振振音点 con con con con con con GM GA WN3 BBS TOMCAT MALBOX JABOX ZABIX Struts ² JABOX JABOX JABOX JABOX JABOX ZABIX Struts ²	办公网诱饵	
主紙領語 正規開発語 内置 「日 庭用服务 28 「の」 「「」 「 「」 「」 「」 「 「」 「」 「 「」 「」 「 「 「 「 「 「 「 「 「 「 「	文件透饵	sop1 sop2 log4j sypo zz zzsył
立原用的は 部項 部項 部項 部項 部項 部項 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ の面 ・ のの のの	主机诱饵	
BND DA I DARSA 20 I DARSA 20	互联网诱饵	21頁
I BURBS 20 Image: CHM OA OHM OA WN BBS TOMCAT MALBOX JABEX STRUTS2	感知节点	
CIM CA WIN BBS TOMCAT MALBOX JBCS ZABX STRUTS2		I 应用服务 20
CRM OA WKI BBS TOMCAT MALBOX JBOSS ZABBX STRUTS2		📾 🛤 📖 💘 금 🍻 ZBX Struts ²
		CPM DA WKI BES TOMCAT MALEOX JEOSS ZABEX STRUTSZ

「前往沙箱市场」:当与 MSS 安全运营平台完成注册后,可跳转至沙箱市场页面获取云沙箱。

新建模板:点击"新建模板",配置"模板图标"、"模板名称"、"模板介绍"、"模板文件",点击【确定】,自定义栏中生成自定义模版对应的图标,如下图所示。



"沙箱文件" 仅支持上传 zip 文件,文件大小不能超过 1GB; zip 包内的基础模板支持上传保活脚本: keepalive.sh;支持上传配置脚本: config.sh zip 包内的高级模板必须包含 define.yml 以及 docker 镜像;

- 注:
 - 1. 上传的 html 压缩包(.zip 文件) 会自动解压, 自动安装部署。
 - 2. 如果需要支持其他语言,可参考《附录 A 自定义沙箱部署说明》
- ◆ **说明**:自定义沙箱主要为了模拟用户的真实业务系统的,扰乱攻击者的攻击目标。

3.5.6 伪装代理

伪装代理部署在用户机器上,通过端口混淆,将黑客攻击诱导至沙箱。当系统 CPU 或内存占用率达到 80%时,伪装代理会自动停用,保证业务正常运行。其中,伪装代理的最大同



时存在的数量为沙箱数量的5倍。

- 1) 伪装代理安装
- ◆ 基础模式:适用于网络直接可达的多个网段中安装(网络可达比如各网段中没有禁止对

幻阵服务器 8888/udp 5555/tcp 端口的防火墙策略)

e.	智能素网	伪装代理 你被代理部署在业务机器、通过第口流来、将原带攻击调导型沙桥							
E	沙箱配置 ^	当系统cpu占用率达到80%时,负导代理会会动得用,保证业务正 若Linux系统使用的root投展安装伪装代理,将不支持半连接通知。	伪装代理脚本下载		×				
安全大屏	沙箱管理								_
E BERINGER	模板管理	用 产管理 P管理	Windows	点击下载、	~				
-	IP體理								传统代理图本下数
	伪展代理		∆ Linux	点击下载,	~				
RAME	中國节点	系统 全部 Windows Linux 状态 全部 在线	ipv4 👩	lpv6 👩					Q
O DANK	攻击诱捕		stall.sh?os=linuxäidev=192.16 8.110.200:55551 [sh						
	透细欺骗 ^	* □ △ 资产标签: e085e38b ∠				IP数	版本号	状态	
	邮件透訊	关联设备: 192.168.110.200	A Kithomatos B	点击下的。		1	3,5.0	• 在线	
NRAIL.	办公務講師	✓ △ 资产标签: ceaefaf1 ∠	Copernetes @	705 LL 1 44		护数	版本号	状态	
日本市社	¢α.i#π	关联设备: 192.168.110.200	1. 根据服本运行的环境选择操作系统	下数或执行代理服本	- 1	3	3.5.0	- 高线	
	1.10.05.01	* ○ △ 资产标签: 6e94c1b8 ∠	2. 脚本执行完成后,可返回至伪装代	理管理页配置端口和关联沙箱		伊敦	版本号	状态	
帮助中心	THERE	关联设备: fee0:0:0:1::200			_	3	3.5.0	- 周筠	
		▼ □ Δ 资产标签: ab1d3e70 ∠		¥	(8)	P数	版本号	状态	
		关联设备: 192.168.110.200			_	10	3.5.0	- 周线	
			¥.	4 条 < 1 > 10 条/	a < 1				

图 3-5-4-1 伪装代理下载

选择相应操作系统下载。Linux 和 windows 都需直接运行 install 文件(管理员权限)。

目前 linux 端目前支持

centos6.4/centos6.5/centos6.6/centos7.0/centos7.1/centos7.2/ubuntu14.04/ubuntu1 6.04/redhat 6.5进行一键部署(如需要支持其他操作系统,提供相关操作系统版本号联系 默安科技工程师)。

例 linux:

Linux 下安装

解压已下载的压缩文件 tar -zvxf xxxxx.tar.gz



<pre>moresec proxy_cli_linux_20170828083703.tar.gz proxy_cli_linux_20170829133706.tar.gz</pre>	proxy_cli_linux.tar.gz
<pre>proxy_cli_linux_proxy_cli_linux_20170829125128.tar.gz proxy_cli_linux_20170829203854.tar.gz</pre>	
[root@localhost home]# tar -zvf proxy cli_linux_20170829203854.tar.gz	
tar: You must specify one of the `-Acdtrux' or `test-label' options	
Try `tarhelp' or `tarusage' for more information.	
<pre>[root@localhost home]# tar -zxvf proxy_cli_linux_20170829203854.tar.gz</pre>	
proxy_cli_linux/	
proxy_cli_linux/src/	
proxy_cli_linux/src/hp_route_cli/	
proxy_cli_linux/src/hp_route_cli/hp_route_cli.py	
proxy_cli_linux/src/hp_route_cli/hp_conf.json	
proxy_cli_linux/src/base/	
proxy_cli_linux/src/base/yg_util.py	
proxy_cli_linux/src/base/yg_process.py	
proxy_cli_linux/src/base/yg_time.py	
proxy_cli_linux/src/base/initpy	
proxy_cli_linux/src/base/yg_syshead.py	
proxy_cli_linux/src/base/yg_log.py	
proxy_cli_linux/src/base/yg_daemon.py	
proxy_cli_linux/src/base/yg_net.py	
proxy_cli_linux/src/base/yg_thread.py	
proxy_cli_linux/src/base/yg_base_cfg.py	
proxy_cli_linux/src/base/yg_daemon.pyc	
proxy_cli_linux/src/base/yg_syshead.pyc	
proxy_cli_linux/src/base/yg_base_cfg.pyc	
proxy_cli_linux/src/base/yg_log.pyc	
proxy_cli_linux/src/base/yg_util.pyc	
proxy_cli_linux/src/base/yg_net.pyc	
proxy_cli_linux/src/base/yg_process.pyc	
proxy_cli_linux/src/base/yg_time.pyc	
provy ali lipuv/ara/pp route baca/	

图 3-5-4-2 Linux 安装 1

进入该目录 cd xxxxxx



图 3-5-4-3 Linux 安装 2

运行该目录下 install. sh 文件 sudo bash install. sh 即可安装完成

Instance down: [rotelications proved [1] linux]# sudo bash install.sh CentOS Linux release 7[3.1611 (Core) NMM=-CentOS Linux* TD-"centos" PFETTY_MME="CentOS Linux 7 (Core)" CPE NMME="CentOS Linux, 7 (Core)" CPE NME="Thtps://bugs.centos.org/" BUG_REPORT_IRg./Num.centos.org/" BUG_REPORT_IRg./Num.centos.org/" CENTOS MANTISET PROJECT VERSION-"/" RELNAT_SUPPORT_PROJECT VERSION-"/" RELNAT_SUPPORT_RELNAT_SUPPORT_PROJECT VERSION Contos Linux release routeCli / tet/init.d Chardonig - Lewel 2345 moresec-routeCli i rotel down's contocli start Porte Cli start Install domo! Install domo! In	
双击此处添加一个新的按钮。	=
Q将文本发送到当前选项中	. =

图 3-5-4-4 Linux 安装 3

卸载伪装代理命令: service moresec-routeCli uninstall(或者在伪装代理界面直接点击 删除卸载)

[root@localhost proxy_cli_linux]# service moresec-routeCli uninstall no hp_route_cli is running uninstall done! [root@localhost proxy_cli_linux]# <mark> </mark>							Ŷ
双击此处添加一个新的按钮。							≡
2 仅将文本发送到当前选项卡							• ≡
ssh://root@192.168.1.242:22	🗄 SSH2	xterm	t⁺ 164x35	i <u>n.</u> 35,35	1 会话	$\pm \downarrow$	

图 3-5-4-5 Linux 安装 4

停止伪装代理命令: service moresec-routeCli stop



启动伪装代理命令: service moresec-routeCli start

例 windows:

1. 下载 windows 版本伪装代理安装文件后进行解压

■ 安装说明.txt
 ■ 幻阵伪装代理...说明2.2.pdf
 ■ HpProxy_Setup.exe
 ■ install.bat
 ■ uninstall.bat

图 3-5-4-6 Windows 安装 1

- 2. 安装请右键以管理员权限运行 install.bat
- 3. 卸载请右键以管理员权限运行 uninstall. bat

例 Kubernetes:

- 1. 下载 Kubernetes 版本伪装代理安装文件
- 2. 将文件拷贝到 K8S 环境的 master 节点下
- 3. 解压已下载压缩包 tar zxvf xxxxx.tar.gz
- 4. 在 worker 节点将镜像加载到本地仓库 docker load -i hp_route.tar



5. 使用宿主机网络:修改 hp_route. yaml,将 hostNetwork 字段的值改为 true





6. 创建 pod: kubectl create -f hp_route.yaml

root@kubernetes-master:~/test# kubectl create -f hp_route.yaml
pod/route-cli-pod created
root@kubernetes-master:~/test#

root@kubernetes-master:~/test# kubectl create -f hp_route.yaml pod/route-cli-pod created								
root@kubernetes-master:~/test# kubectl get pod -A								
NAME	READY	STATUS	RESTARTS	AGE				
hp-route-5b7778df59-qxr7v	1/1	Running	1	5d3h				
route-cli-pod	1/1	Running	0	31s				
coredns-545d6fc579-2j6z2	1/1	Running	1	13d				
coredns-545d6fc579-ksrr8	1/1	Running	1	13d				
etcd-kubernetes-master	1/1	Running	3	13d				
kube-apiserver-kubernetes-master	1/1	Running	16	13d				
kube-controller-manager-kubernetes-master	1/1	Running	8	13d				
kube-flannel-ds-amd64-d9975	1/1	Running	1	13d				
kube-flannel-ds-amd64-khwmj	1/1	Running	1	13d				
kube-flannel-ds-amd64-sz7jk	1/1	Running	1	13d				
kube-proxy-hx25h	1/1	Running	1	13d				
	<pre>:es-master:~/test# kubectl create -f hp_route -pod created :es-master:~/test# kubectl get pod -A NAME hp-route-5b7778df59-qxr7v route-cli-pod coredns-545d6fc579-2j622 coredns-545d6fc579-ksrr8 etcd-kubernetes-master kube-apiserver-kubernetes-master kube-controller-manager-kubernetes-master kube-flannel-ds-amd64-d9975 kube-flannel-ds-amd64-sz7jk kube-proxy-hx25h</pre>	es-master:-/test# kubectl create -f hp_route.yaml -pod created es-master:-/test# kubectl get pod -A NAME READY hp-route-5b7778df59-qxr7v 1/1 route-cli-pod 1/1 coredns-545d6fc579-2j622 1/1 coredns-545d6fc579-ksrr8 1/1 etcd-kubernetes-master 1/1 kube-apiserver-kubernetes-master 1/1 kube-controller-manager-kubernetes-master 1/1 kube-flannel-ds-amd64-d9975 1/1 kube-flannel-ds-amd64-sz7jk 1/1 kube-proxy-hx25h 1/1	es-master:-/test# kubectl create -f hp_route.yaml -pod created es-master:-/test# kubectl get pod -A NAME READY STATUS hp-route-5b7778df59-qxr7v 1/1 Running route-cli-pod 1/1 Running coredns-545d6fc579-2j622 1/1 Running coredns-545d6fc579-ksrr8 1/1 Running etcd-kubernetes-master 1/1 Running kube-apiserver-kubernetes-master 1/1 Running kube-flannel-ds-amd64-d9975 1/1 Running kube-flannel-ds-amd64-sz7jk 1/1 Running kube-proxy-hx25h 1/1 Running	es-master:-/test# kubectl create -f hp_route.yaml -pod created es-master:-/test# kubectl get pod -A NAME READY STATUS RESTARTS hp-route-5b7778df59-qxr7v 1/1 Running 1 route-cli-pod 1/1 Running 0 coredns-545d6fc579-2j622 1/1 Running 1 coredns-545d6fc579-ksrr8 1/1 Running 1 etcd-kubernetes-master 1/1 Running 3 kube-apiserver-kubernetes-master 1/1 Running 16 kube-controller-manager-kubernetes-master 1/1 Running 1 kube-flannel-ds-amd64-d9975 1/1 Running 1 kube-flannel-ds-amd64-sz7jk 1/1 Running 1 kube-proxy-hx25h 1/1 Running 1				

7. 删除 pod: kubectl delete -f hp_route.yaml

www.moresec.cn



◆ **高级模式:**适用于内网隔离状态或将伪装代理安装在外网情况下

● 路由器操作示例:

A. 在路由器、防火墙等设备上将沙箱所在服务器的 IP 映射到需要安装伪装代理的服务器 网络可达的 IP 地址(UDP8888 和 TCP5555 或全端口),如下图:

全选	新增	删除		关键字: 内部服务	f器IP ♀	查询 显示全部
操作	序号	服务名称	外部端口	内部端口	内部服务器IP	状态
1	1	-	-			启用
1	2					启用
1	3	1 × 1	1 A.			启用
1	4			1		启用
1	5					启用
1	6	140_1	8888-8888	8888-8888	192.168.199.140	启用
1	7	140_2	5555-5555	5555-5555	192.168.199.140	启用
1	8		- 1 - 1 - 1	3		启用

图 3-5-4-7 路由器操作 1

幻阵页面操作

A. 首先需要在幻阵管理页面的设备信息处添加虚拟 IP (沙箱所在服务器映射后的 IP)



图 3-5-4-8 幻阵页面操作 1

B. 设置完成后进入伪装代理下载页面进入高级模式,在该页面选择需要安装伪装代理的
 真实 IP 或者虚拟 IP (多台设备可以多选),下载相应操作系统的伪装代理。



伪装代理脚本下载	返回基础模式	Х
1.选择IP地址 【 设备:2		
真实IP (192.168.110.160) (192.168.110.160) (193.1160)		
虚拟IP 0 1.1.1.1		
2.选择该IP所对应的伪装代理版本下载或执行后返回伪装代理员	页面编辑 点击下载	
👌 Linux	点击下载	
	关闭	

图 3-5-4-9 幻阵页面操作 2

◆ 注: 安装步骤和简单模式的安装步骤一致。

2) 伪装代理配置

伪装代理脚本安装好后会在默安幻阵的伪装代理页面显示出已经安装成功伪装代理的 资产信息,点击编辑按钮即可对伪装代理进行编辑,并且可以选择批量编辑,批量删除,批 量更新,输入标签(便于管理),选择资产本机需映射的端口和映射目标沙箱与服务关联。



伪装代理	仍装代理部署在业务机器,通过端口混淆,将黑客攻击诱导至沙箱				
当系统cpu 若Linux系	占用事达到80%时,伪装代理会自动停用,保证业务正常运行; 统使用中root权度安装伪装代理,将不支持半连接感知、自启动、面广探测功器,且伪装代理无法监听1024以	下的端口。			
资产管理	P管理				
系统	全部 Windows Linux 状态 全部 在线 高线 未授权 更新中			20. ⁰	
• 🗆	▲ 在线3932ca98 < 关联设备: 192.168.110.160	IP数 2	版本号 3.4.1	状态 ● 在线	
• 0	▲ 在线6c7f5608 ∠ 关联设备: fcc0.0:0:1:160	IP数 2	版本号 3.4.1	状态 • 在线	
• 0	▲ 18cetb1e × 关联设备: 192.168.110.160	IP数 1	版本号 3.4.1	状态 ◎ 高线	
• 🗆	▲ 479f3b44 ∠ 关联设备: 192.168.110.160	IP数 1	版本号 3.4.1	状态 ◎ 高线	۲
•	▲ 5a905030 ▲ 关联设备: 192.168.110.160	IP数 1	版本号 3.4.1	状态 ◎ 离线	

图 3-5-4-10 幻阵伪装代理页面

点击【伪装代理脚本下载】,进入下载页面,根据伪装代理安装的环境选择操作系统, "点击下载"按钮进行下载。下载后执行脚本完成,返回到伪装代理页面,可查看【资产管理】 页面,会显示已经获取到的资产信息,以及相关 IP 信息;查看【IP 管理】页面,会自动显 示获取到的伪装代理 IP 信息;在【IP 管理】页面,可以对伪装代理 IP 进行删除操作,如 下图:

系统 全部 Window	rs Linux 状态 :	全部 在线 离线	未授权 更新中			<u> </u>	标签 Q
▲ ☐ 在线3932 关联设备:	12:298 ∠ 192.168.110.160			IP数 2	版本号 3.4.1	状态 ○ 离线	
IP 192.168.31.20 192.168.31.23	关联沙箱 5 8081@st_wiki 5 8081@st_wiki						
△ 在线6c7f	5608 🚄			P数	版本号	状态	~

图 3-5-4-11 幻阵伪装代理-资产管理页面



伪装代理 伪裂代理部署在业	务机器,通过端口混淆,将黑客攻击诱导至沙箱			
当系统cpu占用率达到80% 若Linux系统使用非root权	时,伪装代理会自动停用,保证业务正常运行; 很安装伪装代理,将不支持半连接感知、自启动	、责产探测功能,且伪装代理无法监听1024以下的端口。		
资产管理 P管理				
代理端口 全部 🗸	· 资产标签 全部 > 关联方:	2 (金融) > (金融) 2		半连接感知 @ ③ P/关联沙箱 Q
伪装代理IP	关联沙箱	资产标签	沪标签	操作
10.244.1.21		015bd97a	无标篮	
0 10.244.1.21		015fc415	无标签	2 🖻
10.244.2.19		01c8fafd	无标摭	
10.244.1.21		03010345	无标签	
10.244.1.23		0383b6b9	无极被	
10.244.1.21		03ba250e	无标签	a
10.244.1.23		04711030	无极签	2

图 3-5-4-12 幻阵伪装代理-IP 管理页面

进入【IP管理】页面,点击编辑按钮,即可编辑伪装代理,绑定沙箱。半连接开关支 持用户自定义开启或者关闭,半连接感知开关开启后,关联沙箱的 IP 将可以感知 tcp、udp、 icmp 等半连接扫描。编辑界面中的"标签","客户端端口","关联沙箱"等,客户可根据需要 进行配置。点击"+",选择关联的沙箱,会出现对应的关联服务和推荐的端口号,客户也可 根据自己的需要修改端口号,每个伪装代理可关联多个沙箱。编辑伪装代理图示如下:

编辑代埋				X
标签	ab1d3e70			
伪装代理IP 19	2.168.32.83			
请勿设置被占用的	耑口,若仍需设置请 关闭]占用端口服务重新编辑		
关联沙箱	关联服务	关联端口	沙箱状态	+
	PORTCHEAT	∨ 8033	未启用	
hjh的portcheat				

图 3-5-4-13 幻阵伪装代理-编辑代理页面

返回【资产管理】页面,即可查看关联信息。



• □	▲ 在线3932ca98 ∠ 关职设备: 192.168.110.160		IP数 2	版本号 3.4.1	状态 ◎ 离线	
	IP 192.168.31.205 192.168.31.235	关联/9箱 8081@1.wMa 8081@1.wMa				

图 3-5-4-14 幻阵伪装代理-沙箱关联

资产标签后面带有 [▶] 标识,表示为精简版伪装代理,即非 root 权限下部署的伪装代理。 用户可对伪装代理进行批量操作,如批量删除或批量编辑(被编辑的伪装代理的配置信息如 果不一致,将清空原有配置),如下图:

								🖛 📥 aamin 🗸
伪装代理。	为装代理部署在业务机器,到	· ●过端口混淆,将黑客攻击诱导至沙?	a					
当系统cpud 若Linux系统	5用車达到80%时,伪制 使用非root权限安装伪制	l代理会自动停用,保证业务正 装代理,将不支持半连接感知,	▲运行 自启动 ① 是否删除?					
资产管理	旧管理			取消	1.E			
								伪装代理脚本下取
系统	全部 Windows	Linux 状态 全部	在线 离线 未授权 更加	ſФ				
• •	∆ 在线3932ca98	12			P数	版本号	状态	
	关联设备: 192.16	58.110.160			2	3.4.1	 高线 	
	P	关联沙箱						
	192.168.31.205	8081 @ t_wiki						
	192.168.31.235	8081 @ t_wiki						
-								_

图 3-5-4-15 幻阵伪装代理-删除伪装代理页面

此外支持用户在【IP管理】页面,对未编辑的 IP 自动绑定沙箱关系,关联成功后会在

伪装代理 i	p 旁用用	" []	"	标注。
--------	-------	------	---	-----

192.168.100.79 🔄	9043 -> ppmphp 8000 -> bbsjsp	2607d15c	自动关联	
172.19.0.1 🔁	8080 -> crm_zm 8090 -> ppminphp	1b35f613高级114.115.184.49	自动关联	
192.168.15.10	8038 -> ppminphp	1b35f613高级114.115.184.49	张萌	
172.17.0.1 🔄	8093 -> jboss 6379 -> redis	1b35f613高级114.115.184.49	自动关联	
192.168.30.51 🔄	8090 -> ppminphp 6379 -> redis	30.51-b2fc0535	自动关联	
192.168.30.169 🔄	8093 -> jboss 3389 -> 2008r2	d80b90fe	自动关联	

图 3-5-4-16 幻阵伪装代理-自动关联沙箱服务页面

请勿设置被占用的端口,若资产端口和伪装代理端口冲突端口颜色会标红显示,需重新 编辑。



☐ Å 45.76.198.113		• 115.236.55.14	无标签	在线 🗾 🔟
192.168.1.189		192.168.199.140	无标签	在线 🚺 🏛
192.168.1.175	8080->wiki_nodel	192.168.199.140	无标签	在线 🚺 🔟
□ (∆ 192.168.199.55	8080->wiki_nodel 80->CRM	192.168.199.140	luca内网测试	在线 🗾 🔟
□ & 192.168.199.244	8080->wiki_nodel 80->CRM	192.168.199.140	luca内网测试	在线 🖉 🍙
		上一页 1 下一页		

图 3-5-4-17 伪装代理-端口冲突页面

在下发已停止的沙箱时,会有红色提示沙箱状态,但是并不影响伪装代理绑定沙箱。即 沙箱无论是否运行都可编辑。

伪装住	代理 伪装代理部署在业务	号机器,通过端口混淆,将黑客I	女击诱导至沙箱				
	转代理开放源代码,无任何数	如据安全风险。当系统cpu占用和			目代理		×
系统	全部 Windows	Linux 状态	标签 无标签1				
	伪装代理IP	关联沙箱	伪装代理IP 192.	168.20.14			
	192.168.20.14	4444->mysql	● 请勿设置被占用	的端口,若仍需设置请关闭占用端	口服务重新编辑		
	§ 192.168.180.253	4489->sy	客户端端口	关联沙箱	关联服务	沙箱状态	1 +
	§ 192.168.30.182		4444	mysgl	* MYSOL	已停止	
	192.168.30.14						
	§ 192.168.110.31			确认	取消		
	102 169 30 92					102 168 110	140

图 3-5-4-18 伪装代理列表

附录:沙箱关联规则



		沙箱对从	立端口规则		
沙箱	端口	沙箱	端口	沙箱	端口
CRM	8080	WEBLOGIC	7001	SQLSERVER	1433
OA	81	VPN	10200	MYSQLCHEAT	3306
BBS	8000	DISCUZ	8085	MONGODB	27017
TOMCAT	8086	ECSHOP	8087	WIN7	3389
WIKI	8081	ESPCMS	8088	WIN2008	3389
MAILBOX	8890	WEBSPHERE	9043	WINXP	3389
JBOSS	8093	PHPMYADMIN	8090	自定义	80
ZABBIX	8069	MYSQL	3306	HaDoop	50070
STRUTS2	8083	REDIS	6379	Joomla	82
JENKINS	8089	MEMCACHED	11211	Confluence	8001
ADB	5555	Postgresql	5432	SSH (中继)	22
Telnet (中 继)	23	Samba (中继)	445		

注:

1、当伪装代理出现"当前所建沙箱,不满足一键关联要求"提示,请查看配置是否存在如下 情形:

(1)不在自动关联规则内的沙箱: SSH、Telnet、PortCheat、FTP、Samba、IPMI、MODBUS、IEC104、BACNET、S7COMM、ENIP、SNMP。

(2) 只创建一个在自动关联规则里的沙箱或只创建了多个相同类型的沙箱。

(3) 当前所建沙箱与安装伪装代理的主机两者操作系统不属于同一个平台,如 windows7 沙箱,与 Linux 伪装代理。

2、当伪装代理出现"没有可以一键关联的沙箱"提示,请查看配置是否存在如下情形:

(1)没有创建沙箱。

3、同一类型的沙箱不可重复关联。

4、应用服务类沙箱,若两个都是 web 容器,则只能关联其中一个。如:同时存在 tomcat/struts2/weblogic/jboss/websphere 时,只取其中一个关联。

3.5.7 攻击诱捕

1.基础反制

Windows 反制:

反制诱饵包括文件诱饵和反制端点,可以加密上传的 office 文档,经过水印后的文件 被打开时,可以被系统捕获到;反制端点为免杀型/不传染,用户可自行绑定其他应用,扩



散到企业中。同时如果攻击者踩中反制诱饵,消息中心会进行提醒,方便用户及时获取攻击 者信息。如下图所示。

蜜网导图					
智能蜜网	攻击诱捕				攻击反制 开 🔵
沙箱配置 ^	基础反制 高级反制				
沙箱管理					
IP管理	Windows端点反制 Mac端点反制 Android端点反制				
模板管理	攻击反制模块集成反向控制攻击者的能力,需谨慎使用,若要使用此模块	来功能,请仔细阅读【帮助中心	2】处的《免责声明》) .	
伪装代理	反制诱饵包括反制文件和反制端点,反制文件为office文档,当文件被打 后台,用户也可自行上传反制文件关联至沙箱。	开时,可以反向控制攻击者主	机:反制端点为可排	4行文件并经过免杀处理,系	统内置的反制诱饵存放在沙箱
中继节点				杏看咸	和劳占 + 制作反制文件
攻击诱捕				1.11 (A)	
诱饵欺骗 ^	⑦ 免杀更新完成				X
邮件诱饵					
办公网诱饵	文件名	文件类型	诱饵来源	关联沙箱	操作
文件诱饵	default.exe	可执行文件	系统内置	暂无	4
主机诱饵					
互联网诱饵	员工手册(终稿).doc	Office文档	系统内置	test_wiki	*
感知节点	VPN登录控件.exe	可执行文件	系统内置	liweishiTest	*
	大客户合同详情.doc	Office文档	系统内置	12, Leak_test	٤

图 3-5-6-13 windows 基础反制

反制诱饵界面可以添加反制文件绑定,反制文件支持上传文件类型:doc/docx/rtf/exe, 其中 exe 文件会自动关联到 vpn 沙箱, doc/rtf 文件会自动关联到 wiki 沙箱, 原始木马文 件自动关联到 Windows 沙箱不需用户上传。注意:同类沙箱只允许存在一个反制文件, 多次 上传会覆盖之前的上传记录,如图所示,查看感知节点跳转到感知节点 tab,下载反制文件 以及删除反制文件,下载对应的诱饵, exe 的直接打开使用, doc 的需要对应的 office 版本 打开, office 版本限定如下图所示。

智能蜜网	攻击诱捕					攻击反制 开 🔿
沙箱配置 ^		制作反制文件		×		
沙箱管理	参加汉州 两款水州	1. 20		# 12 - 01		
IP管理	Windows端点反制 Mac端点		,	4/7¥.X1+		
模板管理	政击反制模块集成反向控制政行	反制文件支持上传文件类型:docx 到vpn/samba/ssh沙箱,doc文件3	/doc/rtf/exe,其中exe文件支 支持关联到	(持关联 (声明		
伪装代理	反制诱饵包括反制文件和反制 后台,用户也可自行上传反制:	wiki/crm/oa/mailbox/vpn/samba wiki沙箱,原始木马文件自动关联到	/ssh/mysql沙箱,rtf文件支持 则Windows沙箱无需上传。	关联到 为可打	执行文件并经过免杀处理,系统	
中继节点	③一键免杀				查看感知	市点 + 制作反制文件
攻击诱捕			取消	上传		
诱饵欺骗 ヘ	⑦ 充示更加完成					*
邮件诱饵						
办公网诱饵	文件名		文件类型	诱饵来源	关联沙箱	操作
文件诱饵	default.exe		可执行文件	系统内置	暂无	A
王机诱饵	员工手册(终稿).doc		Office文档	系统内置	test_wiki	*
感知节点	VPN登录控件.exe		可执行文件	系统内置	liweishiTest	*
	大客户合同详情.doc		Office文档	系统内置	12, Leak_test	4



图 3-5-6-14 添加反制文件

Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2016 Click-to-Run (C2R) for 32-bit editions
Microsoft Office 2016 Click-to-Run (C2R) for 64-bit editions
Microsoft Office Compatibility Pack Service Pack 3
Microsoft Word 2007 Service Pack 3
Microsoft Word 2010 Service Pack 2 (32-bit editions)
Microsoft Word 2010 Service Pack 2 (64-bit editions)
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)

图 3-5-6-15 支持的 office 版本

当攻击者打开反制诱饵后,在黑客溯源-攻击反制页面便可以找到上线的攻击者,当攻 击者在线时可以进行高级反制,离线时可以查看历史记录,如下图所示。

首页 > 威胁情报 > 黑客溯源 > 耳 黑客溯源 可视化展示不同攻击	女击反制 击者相关信息				
異客溯源 攻击反制 在线状态 全部 >	IP位置 全部 V	最近上线时间 开始时间	间 ~ 结束时间	白 IP地	ut Q
F-001 <u>反制类型</u> 強点反制 <u>攻击者</u> P 115,238.55.14(中国一杭州) <u>在线状态</u> 离线 初次上线时间 2020-02-19 16:14:09 <u>最近上线时</u> 间 2020-03-11 14:40:21		F-006 <u>反制</u> 类型 端点反制 攻击者IP 115.236.55.14 (中国—杭州) <u>在线状态</u> 离线 <u>初次上线时间</u> 2020-02-22 17:55:51 <u>最近上线时间</u> 2020-03-12 11:32:27		F-040 <u>反創実型</u> 端点反制 攻击者P 40.67.184.232(美国一) <u>在线状态</u> 离线 初次上线时间 2020-02-27.17.40:54 <u>最近上线时间</u> 2020-03-11.11.24:32	
F-041 反射类型 端点反制 攻击者IP 192.168.199.26 (局域网)		F-056 反制类型 端点反制 攻击者IP 115.236.55.14 (中国一杭州)		F-061 <u>反制类型</u> 端点反制 <u>攻击者PP</u> 115.236.55.14 (中国一杭州)	

图 3-5-6-16 黑客溯源-攻击反制

Mac 反制:

反制诱饵界面可以添加反制文件绑定,反制文件支持上传文件类型: dmg/pkg/app,其中 dmg 文件会自动关联到 vpn 沙箱;注意: 同类沙箱只允许存在一个反制文件,多次上传会 覆盖之前的上传记录,如图所示,查看感知节点跳转到感知节点 tab,下载反制文件以及删



除反制文件,下载对应的诱饵,直接打开使用。

攻击诱捕			攻击反制 (开
基础反制 高级反制			
Windows端点反制 Mac端点反制 Android端点	点反制		
攻击反制模块集成反向控制攻击者的能力,需谨慎使 通过上传Mac安装包或自定义制作Mac反制文件,攻	ē用,若要使用此模块功能,请仔细阅读【帮助中心】处 z击者安装反制文件后并运行后,可以反向控制攻击者主	上的 《免责声明》。 5机;反制文件支持关联到vpn/ftp/sam	ba/ssh沙箱中。
		1	查看感知节点 + 制作反制文化
		1	查看感知节点 + 制作反制文件
文件名	诱饵来源	子 联沙箱	查看感知节点 + 制作反制文(操作

制作反制文件包括手动上传和自定义制作;其中自定义制作需要填写文件名称、url 地址、app 图标和文件格式;最多可制作 10 个自定义木马。

	制作反制文件	Х
制作方式	○ 手动上传 (●) 自定义制作	
* 文件名称	请输入	
* url地址	请输入	
app图标	日日の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	
文件格式	● dmg文件 ○ app文件	
	确定取消	

Android 反制:

反制诱饵界面可以添加反制文件绑定,反制文件支持上传文件类型: apk,注意: 同类 沙箱只允许存在一个反制文件,多次上传会覆盖之前的上传记录,如图所示,查看感知节点 跳转到感知节点 tab,下载反制文件以及删除反制文件,下载对应的诱饵,直接打开使用。

女击诱捕			攻击反制 (开)
國反制 高级反制			
findows端点反制 Mac端点反制 An	droid端点反制		
攻击反制模块集成反向控制攻击者的能力, 通过上传Android安装包或自定义制作Andro	需谨慎使用,若要使用此模块功能,请仔细阅读【帮 id反制文件,攻击者安装反制文件后并运行后,可以J	动中心】处的 <mark>《免责声明》。</mark> 反向控制攻击者主机;支持关联到ftp/samba/ssh	沙箱。
			看感知节点 + 制作反制文件
文件名	诱饵来源	关联沙箱	操作
te.apk	手动上传	暂无	L Ø Û
googleAuth.apk	手动上传	暂无	201

制作反制文件包括手动上传和自定义制作;其中自定义制作需要填写文件名称、url 地址、app 图标;最多可制作 10 个自定义木马。

	制作反制文件	Х
制作方式	○ 手动上传 (●) 自定义制作	
* 文件名称	请输入	
* url地址	请输入	
app图标		
	确定取消	

2. 高级反制

高级反制模块包括 Git 泄露反制、SVN 泄露反制、Goby 反制、Git clone 反制等; 其中 Git 泄露反制、SVN 泄露反制、Goby 反制需要关联 7 层沙箱,其中 jboss、jeckins、 weblogic、websphere 沙箱不支持关联;



攻击诱捕	攻击反制 开
基础反制 高级反制	
攻击反制模块集成反向控制攻击者的能力,需谨慎使用,若要使用此模块功能,请仔细阅读【帮助中心】处的《免责声明》。	
 Git泄露反制 ② 关联沙箱 攻击者使用Git泄露扫描器,对7层沙箱进行扫描,则触发反制,可在黑客溯源-攻击反制界面看到攻击者上线幻阵。 *不交持关联Doss, jeckins, weblogic, websphere沙須 12 置婚測试 liwelshiTest 	
SVN泄露反制 ④ 关联沙箱 攻击者利用漏扫工具扫描应用服务类沙箱Web根目录下的诱饵文档:当攻击者再次使用工具,则触发反制,可在黑客满源攻击反制界面看到攻击者上线幻阵。 *不交持关联Doss, jeckins, weblogic, websphere炒箱 12 置强测试 liweishiTest	
Coby反制 の 关联沙箱 攻击者使用对组版本Goby扫描器扫描应用服务类沙箱,则触发反制,可在黑客溯源-攻击反制界面看到攻击者上线幻阵。 12 冒燈測試 weblogic liveishTest	

Git clone 反制需要在 github 上发布项目,填写诱饵名称、选择模板、用户名、token 等, 并点击发布项目。

t布的Git clone反制项目,则触发反制,可在黑客满	期源攻击反制界面看到攻击者上线幻阵。*	将感知节点映射到公网地址,将提升Git clone反制的
模板	诱饵地址	状态 操作
系统内置 wx测试REDIS — R	-	● 未发布
	模板 系统内置 wx测试REDIS — R	模板 诱饵地址 系统内置 vox测试REDIS — R

3.5.8 诱饵欺骗

1) 邮件诱饵

邮件服务主要提供对高管邮箱的保护功能,通过向高管邮箱定期发送诱饵邮件,诱骗攻 击者访问来发现邮箱入侵行为,可以和 VPN 等沙箱配合使用,邮件内容指向 VPN 沙箱。

添加邮件诱饵操作: 蜜网管理-->诱饵管理--> 邮件诱饵-->添加邮件诱饵

点击【添加诱饵邮件】进入诱饵邮件详情的编辑页面,需要填写发送者用户名(例如发送者邮箱为 test@126.com,则用户名为 test)、密码(密码为邮箱里设置的发送密码)、服务器地址、服务器端口、是否进行证书校验、可选设备(可随机选择)、被保护的高管邮



箱(每个邮箱以行分割)、发送频率、邮件的标题、邮件日期前缀、邮件模版等信息,发送 频率可以选择每周或每月,系统会根据配置的频率定期发送邮件到指定邮箱,邮件标题的前 缀可以选择无或者日期,选择日期选项则会在发送邮件时将当天日期添加到邮件标题中(可 以用于周报或月报等类型的诱饵邮件),邮件模板中可以选择系统默认提供的一些诱饵邮件 模板,也可以自定义邮件内容,拥有添加附件功能,点击后支持上传 docx, x1sx, pptx 文 件,支持上传多个文件,最多5个文件,每个文件最大 20M。点击【测试发送】会根据配置 的邮件信息发送当前邮件到被保护者邮箱。如下图添加诱饵邮件:

智能蜜网	编辑邮件诱	洱		
沙箱配置 ^				
沙箱管理	* 发送者邮箱	2042729575@qq.com		
IP管理	*发送者密码	••••••	ø	
伪装代理	· 00 47 99 14 14	107.0.0.1		
中继节点	服劳器地址	127.0.0.1		
攻击诱捕 🔷	*服务器端口	70		
攻击反制	证书校验	● 是 ○ 否		
邮件诱饵	可选设备	192.168.110.200	~	
办公网诱饵			计	
文件诱饵	被保护者邮箱	xxwxx@163.com	/エ・「 町/相口]	
主机诱饵				
互联网诱饵				
感知节点				
	*发送频率	每周	×	
	*邮件标题	2042729575@qq.com		

图 3-5-6-1 添加诱饵邮件

成功登陆被保护者邮箱后,查看所发送的诱饵邮件或打开邮件诱饵中的附件会被记录下 来,在威胁情报管理-->查看事件处,如果看到相关事件且不是被保护者邮箱拥有者登陆则 表示被保护者邮箱被入侵,如下图事件列表:

黑客港源	-										🌲 🚺 👗 admin 🤉
黑客反制	查看事件 🕫	不同攻击者对不同沙箱的	政击事件单数	(日井,分別展示为)	事件						
查看事件	攻击者 全	18 ×	攻击资产	所有资产	∨ 隔离	沙箱 高管邮件 、				攻击源	Q
行为分析	风险等级 全	# v	事件类型	全部	~ 攻击	时间 开始时间	→ 結束时间				隐藏白名单内的攻击事件
	년:BP 대	1输入过滤的P、多个	P之间用英文	文逗号分開							
	攻击者	攻击源 🔍		攻击资产		隔离沙箱	开始攻击时间	⇒ 最近攻击时间	⇒ 风险等级	≎ 操作	
	H-0008	192.168.100.9	90	-		高管邮件	2022-04-28 10:31:36	2022-04-28 10:31:36	● 二里		
	H-0003	192.168.31.10	14	-		高管邮件	2022-04-26 20:27:02	2022-04-27 15:04:51	• F =		
	H-0012	192.168.31.23	32	—		高管邮件	2022-04-26 15:59:02	2022-04-27 14:40:48	♥ 严重		
						ŧ	も3 条 < 1 > 10 条/页 >				

图 3-5-6-2 事件列表



测试发送事件列表查看到相应事件,说明设置正确,点击【保存】即可保存当前配置内容,在诱饵列表会生成相应的诱饵记录,状态为'已发布',表示该条诱饵已经发布成功,可以在操作栏'取消发布',状态变为'未发布'。可以对单条记录进行'编辑'和'删除'操作。如下图邮件诱饵管理:

医学校能导学部位 马孙能养后听着后 收车来到	医萎缩 化固定 化化试验 网络		
但此时和今及即任,当此称今夜忽略归,从田有言	·····································		
饵邮件名	创建时间	状态	操作
isfas	2022-04-01 16:07:28	◎ 未发布	
223333	2022-04-01 16:04:10	◎ 未发布	
ist-hjh	2022-04-01 10:53:41	◎ 未发布	
042729575@qq.com	2022-04-01 10:18:09	◎ 未发布	a z
221111	2022-04-01 10:12:41	◎ 未发布	a z
息	2022-03-31 13:26:25	 已发布 	* Z B
w1234567	2022-03-28 19:14:22	◎ 未发布	
042729575@qq.com	2022-03-28 19:06:18	• 已发布	* Z B

图 3-5-6-3 邮件诱饵管理

2) 办公网诱饵

办公网诱饵是在企业员工设备上分发诱饵,当攻击者入侵办公环境,诱饵会把攻击者引 入默安幻阵沙箱中,从而发现攻击行为。

在办公网诱饵管理页面,有'办公网诱饵客户端下载'链接,点击下载,下载完成之后按 照下面步骤安装。

安装说明: HpfClient_Installer_1.0.0.0.exe 支持 win7, win10 系统;

办公网诱饵客户端是轻量级进程,5分钟检查一次诱饵状态便进入睡眠。

安装方式:在windows 机器上 cmd 中执行命令行:HpfClient_Installer_1.0.0.0.exe /u hr /i 192.168.xxx.xxx; 命令行中 IP 为默安幻阵设备客户端的 IP 地址。

其中, /u 参数表示: 用户组; 比如, hr, staff 等员工组, 请确保使用英文表示分组;

其中, /i 参数表示: ip; ip 为默安幻阵安装时用户提供的物理机 IP 安装地址; 安装 完成之后, 在客户端列表会生成对应的客户端记录, 如下图:



办公网诱饵			办公网诱饵客户端下载
在Windows电脑上安装办公网诱饵客户端, 如何安装:下载办公网诱饵客户端,执行H 如何卸载:打开目录:c:/program Files (x	可以发布沙瑞奇性到客户PC中。同组的办公网诱组规则相同。 pfCilent_Installer.exe /u 分相名 / 拉勒端P 。例如:HpfCilent_In 86)/hpfCilent, 以管理员身份运行Uninstall.exe。	staller.exe /u default /i 192.166.110.200	
default 會 关联沙箱:0 書户結数:1	分组选是 ∠ 分组选路: dofault 客户端数: 1 关联沙箱: 客户编列表		
	客户编iP 主机名	域帐户名 MAC地址	备注 状态
	▼	C8:E2:65:03:6F:6A	— 离线
+新建分组		共1条 < 1 > 10条/页 >	

图 3-5-6-4 办公网诱饵客户端

办公网诱饵客户端安装完成之后,点击'编辑'按钮给指定的客户端组的所有客户端分发 诱饵。

添加办公网诱饵操作: 蜜网管理-->诱饵管理--> 办公网诱饵-->编辑

诱饵名称自定义,选择关联沙箱(将该沙箱的信息添加到诱饵文件中),如下图添加 办公网诱饵。

办公网诱饵						か公開時1	18户端下载
在Windows电脑上安装办公路透信客户如 如何安装:下着办公路透信客户编 执行	 可以发布沙箱诱信到 HinfGlant Installer exe / 	新建分组	×				
如何卸载:打开目录: c:/program Files	(x86)/hpfclient, 以管理部	* 分组名称					
defauit 章 关联设稿:0 客户编数:1	分級信息 ∠ 分組名称: default 关联沙箱: 客户编列表 客/	关联09箱 说明: 透信下发内容如下 1.劳造营业地关闭 (关联Windows)珍融合下发) 2.雪流而造新的之件记录 (关联Windows)珍融合下发) 3.雪流而造为中之件 (关联最大规范者条规珍融合下发) 4.桌面的造文件 (关联最大规范者合下发) 5.劳流测定器得以起意来很明(web失的沙融合下发) 6.劳流测定器得以起意来很明(web失的沙融合下发)		MACHERE	香注	ĸs	
	▼			C8:E2:65:03:6F:6A		离线	
+新建分组				> 10 新/页 ~			

图 3-5-6-5 添加办公网诱饵

输入完成,点击'确定'按钮即可。

3) 文件诱饵

文件诱饵功能,用户可将敏感文件上传到幻阵页面上,幻阵将文件进行打标后,提供下载功能,客户将打标后的文件下载到本地,当攻击者使用 office 打开文件时,幻阵可感知到并且进行告警。



文件透饵		查看感知节点 + 添加文件诱饵					
文件诱饵可以加密上传的office文档,经过水印后的文件被打开时,可以被系统捕获到。文件诱饵会关联所有当前感知节点。							
文件名	关联节点	操作					
日志审计概块映射表3.0.0.xlax	1						
幻阵云媚调用说明.docx	3	A					
123.xtsx	i.	A					
2.11.0-J ^{#6} 题POG开启 xtax	3	A 8					
共4条 < 1 > 10条/页 >							

图 3-5-6-6 文件诱饵页面

打开诱饵文件后, 幻阵产生告警事件:

4) 互联网诱饵

互联网诱饵主要是针对攻击者在攻击前期信息收集阶段,在互联网发布沙箱信息,诱骗 攻击者进入到相关沙箱中。

添加互联网诱饵操作: 蜜网管理-->诱饵管理--> 互联网诱饵-->添加办公网诱饵 诱饵名称自定义, 诱饵类型(目前支持 github, github 是一个互联网平台, 部分研发人员 会将研发项目的代码配置文件等放到该平台进行管理, 所以该平台成为黑客喜欢搜集情报的 场景),选择关联沙箱, 输入 github 账号以及 token;

如果希望将敏感信息暴露为公网可达的 IP 地址,请将关联的沙箱 IP 地址映射为公网 IP 地址,并在"设置沙箱发布地址处"填写允许被攻击者访问的公网 IP。

如下图添加互联网诱饵。

					🌲 💄 admin o
王联网诱饵	-		_		+ 251015183910
在互联网环境中发布沙箱信息。引诱攻击者进入沙箱	添加互联网诱饵		×		
联沙箱 所有沙箱 ∨	* 诱饵名称	1-18位长度的英文字符			
	* 诱饵类型	请选择诱饵类型	~		
诱饵名称 诱饵类型	* 关联沙箱	请选择沙箱	14. 	状态	操作
	设置沙箱发布地址 🕥	请填写PI或域名			
	* 用户名	请输入			
	★用户token	请输入	ø		

图 3-5-6-6 添加互联网诱饵

输入完成,确保 gi thub 内容输入正确,点击'确认'按钮,在诱饵列表会生成相应的诱饵 记录,但还处于'未发布'状态。勾选需要发布的互联网诱饵,点击'发布'按钮,,状态变为'发 布中',大约 5 分钟之后,状态变为'已发布',表示该条诱饵已经发布成功,可以对单条记录



进行'编辑'和'删除'操作,如下图互联网诱饵管理。

互联网诱饵					+ 添加互联网透饵
在互联网环境中发布沙箱	i信息,引诱攻击者进。	入沙箱			
关联沙箱 所有沙箱					
诱饵名称	诱饵类型	关联沙箱	诱饵地址	状态	操作
测试host	github	ssh	https://github.com/g)x7598189/Email	● 已发布	
测试测试777	github	MAILBOX777	https://github.com/Visene/postfixadmin	• 已发布	
测试测试3	github	mysql	https://github.com/Visene/discuz_test	• 已发布	
OS技术改造哪	github	溯源	https://github.com/binterore/my_framework	 已发布 	

图 3-5-6-7 互联网诱饵管理

状态变为'已发布'之后,访问诱饵列表中的诱饵地址,看到该页面下有该沙箱的相关信息,表示该条互联网诱饵发布成功,如下图互联网诱饵页面:

奇信公童 - 互联网语信 ×	• GitHub - HangjianQian/Email: 1: X	🔷 जनसंस	× +								8
→ ×	0 A https://github.com//	HangjianQian/Email								° ¥ ∥	
		Why GitH	ub? - Enterprise Exp	olore – Marketplac	e Pricing -		3 Sign i	n Sign up			
		HangjianQian	/ Email			٥	Watch 1 🖈 Star 0	γ Fork 0			
		<> Code ① Iss	ues 0 👘 Pull requests	0 III Projects 0	10 Security	Insights					
			GitHu an	Joi b is home to over 40 d review code, manag	n GitHub toda million developers v ge projects, and bui	y working together to ho id software together.	est	Dismiss			
		for backup			Sign up						
		3 comm	its P 1 bra	anch	🕐 0 packages	⊙ o relea	ases 🚨 1 con	tributor			
		Branch: master +	New pull request				Find file Clone	or download +			
		📾 🛛 HangjianQian	and root fix error				Latest commit 84a741	e Dec 17, 2019			
		.bash_history		1	ix error			Dec 17, 2019			
		README.md		1	nitial commit			Dec 16, 2019			
				r	ix error			Dec 16, 2019			
		🖹 email.py		f	ix error			Dec 17, 2019			

图 3-5-6-8 互联网诱饵页面

5) 主机诱饵

主机诱饵通过将用户编辑的虚假信息,散布到各个 Linux 主机上,迷惑攻击者。 关联伪装代理,将直接把主机诱饵下发至伪装代理主机上。点击【蜜网管理】—【诱饵管理】—【主机诱饵】—【添加主机诱饵】。

添加主机诱饵	
• 诱饵名称	请输入诱饵名称
上传SSH公钥	○ 是 ● 否
自定义bash history	示例: wget-ohttp://192168.10.3./upioad/wordpress-4.9.4-zh_CN.tar.gz scp-rroot8192168.10.3./home/tmp/ssh/id_rsa.pub seh root8192168.10.3 不同的命令用時行分割
下发至伪装代理	
	确定: 取消



图 3-5-6-9 添加主机诱饵页面

诱饵名称自定义,选择是否上传 ssh 公钥,选择是会将伪装代理的公钥上传至 ssh 沙箱中(使用该功能需要为 ssh 沙箱关联 IP),自定义 bash history,选择下发的伪装代理。

当攻击者进入伪装代理之后,可以查看到用户提前伪装好的 linux 命令,将攻击者引入 ssh 沙箱中。

E机诱饵		+ 源加主机诱约
主机诱饵通过将用户编辑的虚假信息。散布到各个Linux主 关联伪装代理,将直接把主机诱饵下发至伪装代理主机上,	机上, 迷惑攻击者。	
透饵名称	关联资产标签	操作
2	3932ca98	
123123	7dc32f13 ceaefaf1	2 4 3
	共 2 条 < 1 > 10 条/页 >	

图 3-5-6-10 主机诱饵页面

6) 感知节点

感知节点用于感知诱饵被打开或者攻击者触碰到的行为,用户可下载感知节点包,在存 在诱饵的网络里安装对应的感知节点,感知节点会自动化关联到诱饵上。如下图所示。

知节点			下载安装包	关联感知节点
感知节点用于感知诱饵被打开或者攻击者触碰	创的行为,用户可下载感知节点 包	9,在存在诱饵的网络里安装对应的感知节点,感知	节点会自动化关联到诱饵上。	
感知节点IP	natiP	备注	状态	操作
192.168.110.200:8081 (系统感知节点)	192.168.110.202:8081	XXX	 在线 	2

图 3-5-6-17 感知节点

用户可以进行感知节点的添加和管理,点击右上角下载安装包,安装完成后即可安装, 待安装完成后点击关联感知节点进行感知节点的关联,如下图所示。



感知节点				下载安装包 关联感知节点
感知节点用于感知诱饵被打开	关联感知节点	1	Х	知节点、感知节点会自动化关联到诱饵上。
感知节点IP	请先参照配置 默认端口为80	指南部署感知节点,确保幻阵能够访问感知节点,感知节 281。	点	状态 操作
192.168.110.200:8081 (系統	*感知节点IP	请输入节点IP或节点IP:端口		● 在线
		取消 稳定		

图 3-5-6-18 关联感知节点

点击编辑,可开启 nat 模式,对于内网部署的感知节点映射到外网,填写 nat IP 和端口

感知节点	_			下载安装包	关联感知节点
感知节点用于感知诱饵被打开。	编辑感知节	点	×	即节点、感知节点会自动化关联到诱饵上。	
	nat模式	Ŧ			
感知节点IP	* natlp	192.168.110.202		状态	操作
192.168.110.200:8081 (系统	* 端口	8081		● 在线	2
	备注	xxx			
		3 / 100			
		取消 确	定		

3.6 报表管理

3.6.1 威胁分析报告

威胁分析报告,用户可根据实际需求,选择特定时间段生成相关报表,报表内容主要包括:报表基本信息、综述、事件趋势分析图、沙箱攻击统计、黑客情报统计、攻击事件统计、资产受攻击统计等,生成报表时间2分钟左右,报表生成之后支持下载和在线查看。

威胁分析报告			
报告名称 请输入	起止时间 2022-04-14 ~ 2022-04-20 □		生成报告
报告名称	起止时间	生成状态	操作
2222	2022-03-27 00:00-2022-04-02 23:59:59	• 正在生成	
111	2022-03-27 00:00:00-2022-04-02 23:59:59	• 正在生成	
1111	2022-03-27 00:00:00-2022-04-02 23:59:59	• 正在生成	8
333	2021-10-30 00.00:00-2021-11-05 23:59:59	 已完成 	A 0 0
	共4条 〈 1 〉 10条/页 〈		

图 3-6-1 生成报表页面

3.6.2 攻击源分析报告

用户可按攻击源进行报告生成,报告包括攻击源的所有攻击事件。

吉名称	风险等级 全部		
上时间 2022-04-14	- 2022-04-20 🗎		生成报
报告名称	起止时间	生成状态	操作
111	2022-03-27 00:00-00-2022-04-02 23:59:59	 已完成 	A
	2022-03-27 00:00:00-2022-04-02 23:59:59	• 已完成	A
2222	2022-03-27 00:00:00-2022-04-02 23:59:59	 已完成 	A 8
则试参数	2022-03-15 00:00:00-2022-03-21 23:59:59	• 已完成	2
	共4条 < 1 > 10条/3	E V	

图 3-6-2 按攻击源生成报表页面

3.6.3 黑客画像报告

用户可按黑客画像进行报告生成,报告包括黑客设备指纹,IP,攻击链路等。



黑客画像报告			
报告名称 词诡泽 攻击者 词选择			生成报告
报告名称	生成时间	生成状态	操作
H-0005_2022-04-18_16:44:42	2022-04-18 16:44:42	 已完成 	
H-0005_2022-04-18_16:31:41	2022-04-18 16:31:47	• 失败	
H-0011_2022-04-14_10:46:36	2022-04-14 10:46:37	• 失敗	
1	2022-04-02 11:13:17	• 失败	
m	2022-04-02 10:59:49	• 失败	
H-0001_2022-02-23_10:40:31	2021-11-23 08:18:02	• 已完成	
	共 6 条 < 1 > 10 条/页 >		

图 3-6-3 按黑客画像生成报表页面

3.6.4 行为分析报告

用户可按攻击者行为进行报告生成,报告包括沙箱名称、攻击者 IP、行为类型、起止 时间、生成状态以及操作。

名称	请输入	选择沙箱	请选择		行为类型	全部 🗸			
诸IP	请选择	起止时间	2022-04-14	~ 2022-04-20	8			生	成报
6 告名称	沙箱名称			攻击者IP	行为类型	起止时间	生成状态	操作	F
65555	机密文件			1.1.102.187	全部	2022-03-27 00:00:00~2022-04-02 23:59:59	 已完成 	4	
	t_0a3			1.1.102.187	全部	2022-03-27 00:00:00~2022-04-02 23:59:59	• 已完成	*	
		2		全部	全部	2022-03-19 00:00:00-2022-03-25 23:59:59	• 已完成		1

图 3-6-4 按攻击行为生成报表页面

3.7 联动配置

3.7.1 威胁情报中心联动

支持同本地威胁情报中心及云端威胁情报中心进行联动。获取的数据会基于相同的设备 指纹从威胁情报中心同步信息,在【黑客画像页面】->【情报联动数据】,展示某设备指 纹关联到情报中心的黑客 ID, ID 来自威胁情报,点击 ID 可跳转到情报中心对应的 ID 详情 页。

对于本地的威胁情报的数据,用户可以自定义设置推送时间、地址。定时发送给本地的 情报中心。



如果想要获取更多的威胁情报,用户需要打开云端威胁情报同步及获取更多威胁情报的 开关,填写公司名称、公司官网、所属行业,点击保存之后即可获取更多情报。公司名称、 公司官网、所属行业会同步订正【账号管理】处信息。

对于没有成功传输到云端的威胁情报,支持用户对威胁情报数据下载,手动导入。

本地威胁情报同	情報周歩 (王) 電動地構成時を至本地公開電動構築中心	
设置推送时间	間 朝天 00:00 〇	
设置推送地址	测试推迟 保存	
云端威胁情报 开启后自动将威胁性	情报同步 (王) 病助情期同步至五端情报设备	
获取更多威胁情 开启后可获取来自助	威胁情报 (Ⅲ○) IXA自欺灾情报中心的辛喜情报	
公司名称	moresec	
公司官网	morsec.on	
所属行业	其他行业	
	保存	

图 3-7-1 威胁情报中心联动界面

3.7.2 安全运营平台联动

支持与 MSS 安全运营平台进行联动。通过私有协议主动上报行为数据至 MSS 安全运营 平台,对原始行为进行筛选,精准发现安全威胁,提高安全事件的检出率和监测准确率; MSS 平台通过升级监测机制对幻阵版本进行策略判断,并运用 AI 计算最短升级路径,通过 访问密钥对安全设备进行在线升级

幻阵联动安全运营平台的配置界面如下,用户先在 MSS 平台-联动配置处添加幻阵产品的 ak/sk 等基本信息,然后在幻阵-平台联动处通过填写正确的安全运营平台的地址点击确 定后,即可完成注册。



e	开放认证	安全运营平台	
B			
安全大屏		文主道書中記録40 中全語等平台地址 192 188 32 X11 8890 書意	
威胁情报		A ANN TANK	
ERER			
16 成表展現			
o) Reinem			
- 21			
ERMIT			
日志审计			
開設中心			

图 3-7-3 安全运营平台界面

3.7.3 日志同步

通过配置 SYSLOG 服务器地址(默认端口为 514), 默安幻阵会对每一次攻击行为的详 细信息以日志的形式发送到该服务器。配置界面如下图 日志同步界面所示,填写 SYSLOG 服务器 IP 地址后点击'发送测试',大概 10 秒后,页面会提示'是否成功';点击【保存】即可 生效;普通用户只能看到相关信息,不能对日志同步界面进行操作。

SYSLOG日志同步						
日志同步 🎴						
给指定的帐号发邮件,当此帐号被泄露后,攻击者查看此邮件时将被感知						
SYSLOG服务器 恶意事件同步	123	发送测试				
	+ 添加					
	保存					

图 3-7-4 日志同步界面

3.7.4 情报联动

情报联动包括了攻击 IP 的联动和恶意文件的联动,当有新的 IP 地址对沙箱发起攻击时, 攻击 IP 联动会同步发送恶意的 IP 地址信息到对应接口,当有攻击者上传病毒木马等恶意文



件时,恶意文件联动会同步发送恶意文件路径信息等到相应的接口,二者都以 HTTP POST 方式发送 JSON 格式的数据到 HTTP 服务器。如果需要启用该功能,用户需要先搭建相应的 HTTP 服务器来接受同步数据。配置界面如下图所示,在相应栏中填入配置好的 HTTP 服务 器的地址后点击'发送测试',大概 10 秒后,页面会提示'是否成功';点击【保存】即可生效。

情报联动 🎴			
该功能需配置联动	的URL,系统通过HTTP协议的POST方法将恶	意攻击IP及恶意文件名传送至接收端	
攻击IP联动接口	http://www.attack.com	注:恶意IP信息同步	

图 3-7-5 情报联动界面

3.7.5 开放认证

开放认证可以支持幻阵与其他平台进行联动。通过点击添加平台,输入平台地址、 AccessKey 和 SecretKey,可获取相应平台的对应 AK 的 API 权限,以此与其他平台进行联动。 如果需要使用该功能,用户需要购买刃甲或其它平台设备。

添加完成后,可在界面上对 AccessKey 进行复制,点击验证按钮,输入验证码和管理员 密码可查看完整 SecretKey,还可以进行删除操作。

ф.,	平台联动	2						*	🛔 admin 🗸
0	开放认证	开发认证						+	原加平台
受全大年		平台 全部						平台地址	٩
(1) 成的情报		平台	平台地址	AccessKey	SecretKey	35.20时间	备注	操作	
生 料管理									
10 报表管理					10000000000000000000000000000000000000				
(S) ROMEN									

图 3-7-5 开放认证界面



						# 1 a	dmin 🗸
开发认证						+ 25107	8
平台 全部 🗸	添加平台		×			平台地址	Q
To Tomb	*平台	其他平台	~	15 mateil	611	提作	-
	*平台API 7	其他平台 刀甲平台		allowed in the	. Hite	antr.	
	*平台地址	永明: http://ip:port現https://ip:port					
	* AccessKey	青龍入AccessKey	=				
	备注	el III / Annon an ang I	51				
			_				
		取消	确定				

图 3-7-6 添加平台界面

3.8 配置管理

3.8.1 账号管理-基本信息

界面展示了当前账户的个人信息、公司信息;个人信息包括用户名、类型、邮箱、电话、 创建时间、密码强度;公司信息包括公司名称、公司官网、所属行业;

账号管理 ^								
基本信息	基本信息							
子账号管理								
系统设置 ^	个人信息	公司信息	this sec					
设备信息	用户名 admin	公司名称 moresec						
设备配置	邮箱 —	公司官网 morsec.cn						
功能设置	创建时间 2022-04-13 11:47:06	所属行业 其他行业						
-10 H0 K0.48	角色 超级管理员							
口石平	电话 —							
告營设置	密码强度 😃 😐 💶 🛛							
測源配置								
SecretKey管理								
授权信息								
安全性配置								
个性化配置								
网络测试								
数据清理								
系统升级								

图 3-8-1 账号管理

页面可以修改个人信息和公司信息、点击编辑、修改个人信息。


小体の 編纂現 × 用字名 admin 1 編集 204272957594q.com 用字名 admin 簡潔詞 2021-11-02 3436338 角合 創設電見 資産 道営電方 自然 記名型方29106 電子 18770579106 18770579106 管研集 204272957549q.com 位明道 受研集 204272957549q.com 回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回回	基本信息		
TYLE Aftic Aftic 用P名 admin admin 算器 204272957680q.com Aftic 算器 2021-11-02 14.55.36 Aftic 推進 2021-11-02 14.55.36 Aftic 電磁電源 Aftic Aftic 電磁電源 Aftic Aftic 電磁電源 Aftic Aftic 電磁電源 Aftic Aftic Aftic 1370879106 Aftic Aftic 204272957580q.com Aftic Aftic 204272957580q.com Aftic	A1778	编辑资料 ×	
市子2 admin 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	17人信息	个人信息	
台21-11-02-14:55:36 角色 超低管理员 株装管用 地域管理局 地域管理局 电域 18170879106 地域 各時強速 0 18170879106 ● ● 20427295759ggcom ● ● 公司名称 ● のressec.n ● 一 ● 単位・少	用户名 admin 邮箱 2042729575@qq.com	用户名 admin .cr	
地話 1870879106 地話 1870879106 都明 2042729575@qq.com	创建时间 2021-11-02 14:55:36 角色 超级管理员	角色 超级管理员	
密码確定 2042729575@qq.com 部項 2042729575@qq.com 公司在象 moresec1 公司百称 moresec.cn 所進行业 其他行业	电话 18170879106	电话 18170879106	
公司信息 公司名称 moresect 公司官网 moresec.cn 所属行业 其他行业	密码强度 0 0	邮箱 2042729575@qq.com	
公司名称 moresec1 公司官网 moresec.cn 所属行业 其他行业		公司信息	
公司官网 morreso.cn 所属行业 其他行业		公司名称 moresec1	
用属行业 其他行业		公司官网 moresec.cn	
		所属行业 其他行业	
		取消 确定	
取消 确定			
取消 确定			

图 3-8-2 编辑个人信息

页面可以修改,点击 🙆 修改密码按钮,修改密码。

基本信息	
修改密码	×
・旧教時 用户者 admin ・旧教時	
邮箱 2042729575@qq.com *新密码 请输入密码	
創課时间 2021-11-02 14:55:36 角色 超級管理员 : 徐认密码 请再次输入一遍密码,以便承认	
电话 18170879106 ・ 验证時 絵证明 🛣 🖷 🤺 🍸	
	_
取消 偽定	

图 3-8-3 修改密码

3.8.2 账号管理-子账户管理

子账号管理包括子账户用户名、创建时间、认证方式、允许登陆地址、邮箱、电话、角 色以及操作。

超级管理员可根据实际安全管理需求,添加管理员权限用户、普通用户和审计员并可指 定认证方式和其允许登陆地址,如图 3-8-4 添加用户界面。



账号管理	81							🌲 🔔 adi	min v
基本信息	子账号管理				_			+ 認知于187	
子很考望理			添加用户		x			料产名/电话 C	a
系统设置 ^									
设备信息	用户来	COLUMN STATE	* 认证方式	● 密码认证 ○ Radius认证		把 汉	0.0	49/E	
设备配置	707 53		* 用户名	以英文字母、数字成下划线进行组合				2411	
功能设置	ethan	2022-04-11 15:08:49	*角色	管理员	~	13345638721	普通用户	2 8 8	
白名单	ethan1	2022-04-14 10:52:16	* 4725	·····································		15203411239	管理员	2 8 8	
告誓说言			- 10.40	W180.//11.000500-98-92-92					
派贡配置			* 电话	请输入有效的电话					
SecretKey管理			* 密码	请输入密码	10				
授权信息			*确认密码	请再次输入一遍密码,以便确认	ø				
安全性配置			存在要是他位	Efizit techi Ill the techi					
个性化配置			JOH BARDA	TITHAGAL UTBACAGAL					
网络测试					_				
数据清理				取消	确定				
系统升级									

图 3-8-4 添加用户(所有用户)

界面下方的子账号管理列表,会将添加的用户展示到列表中,并可对子账号进行管理。 在子账户管理列表的右上方,具有模糊搜索功能,可以对用户名/电话模糊搜索。子账户管 理列表下方,具有翻页功能,默认每页展示 10 条。如下图所示:

						ļ.	租户名/电话)
用户名	创建时间	认证方式	允许登录地址	60 1 0	电话	角色	操作	
ethan	2022-04-11 15:08:49	Radius认证	所有地址	33440Bqq.com	13345638721	普通用户		
ethan1	2022-04-14 10:52:16	密码认证	所有地址	gengjlaxlang1@moresec.cn	15203411239	管理员	2 0 1	1

图 3-8-7 子账号管理

权限分配为:超级管理员可进行一切操作,管理员不可以对任何功能和数据进行删除操, 普通用户只可以查看数据,审计员仅可查看个人信息,查看下载日志。

超级管理员可以编辑子账户信息,包括修改子账户角色、邮箱、电话、允许登录地址等, 如下图所示。



子账号管理							+ 2	101于10户
		编辑用户		×				
		*认证方式	密码认证					
用户名	创建时间	* 用户名	wypTest		电话	角色	操作	
wypTest	2022-04-24 17:29:47	* 角色	管理员	v	18303700587	管理员	2 0 0	
gly	2022-04-24 18:00:45	* 邮箱	792874271@qq.com		18399984729	管理员	2 0 0	
ptyh	2022-04-24 18:01:46	* 电话	18303700587		15857198961	普通用户	2 6 1	
sjy	2022-04-24 18:01:57	允许登录地址	● 所有地址 ○ 指定地址		18399984725	审计员	2 6 8	
test_pt	2022-04-25 10:36:29				17326031308	普通用户	2 6 8	
123	2022-04-25 10:44:53			取消 确定	15846681168	管理员	2 6 0	
test_gly	2022-04-25 14:00:03	密码认证	所有地址	123@4567.com	17326031309	管理员	2 8 8	
			共7条 <	1 > 10 条/页 ∨				

超级管理员可根据实际安全管理需求, '¹》,删除用户; 如下图删除用户界面。

子账号管理							+ 添加于	18/2
		C	提示 确认删除该用户?					Q
用户名	QUIREJAG	认证方式		取消 構定	电话	角色	操作	
ethan	2022-04-11 15:08:49	Radius认证	所有地址	33440@qq.com	13345638721	普通用户	2 8 8	
ethanī	2022-04-14 10:52:16	密码认证	所有地址	gengjiaxlang1@moresec.cn	15203411239	管理员	2 6 8	
			ж	2条(1)10条/页~				

图 3-8-8 删除用户

超级管理员可重置子账户密码,点击"重置"按钮,输入超级管理员的密码和重置后的新密码;如下图所示。

子账号管理		-		_			+ 75	加子账户
		修改密码		×				
		* 超级管理员密码	超级管理员密码					
用户名	创建时间	* 新密码	请输入密码		电话	角色	操作	
wypTest	2022-04-24 17:29:47	*确认密码	请再次输入一道密码,以信	医确认	18303700587	管理员	2 0 1	
gly	2022-04-24 18:00:45				18399984729	管理员	2 8 8	
ptyh	2022-04-24 18:01:46			取消 确定	15857198961	普通用户	2 0 0	
sjy	2022-04-24 18:01:57	Radius认证	所有地址	206209792@qq.com	18399984725	审计员	2 8 8	
test_pt	2022-04-25 10:36:29	密码认证	所有地址	123@456.com	17326031308	普通用户	2 8 8	
123	2022-04-25 10:44:53	密码认证	所有地址	206209791@qq.com	15846681168	管理员	2 8 1	
test_gly	2022-04-25 14:00:03	密码认证	所有地址	123@4567.com	17326031309	管理员	2 8 8	
			共7条 <	1 > 10条/页 >				



3.8.3 账号管理-授权信息

授权信息包括设备指纹、产品到期时间、license 版本、伪装代理上限、沙箱上限、产品序 列号。

注备指纹 ;	a05c960528ae		沙箱服务上限 🔘	50 (已使用33个)
"品到期时间	无限期		沙箱中上限	9 (已使用9个)
主保到期时间 🔘 💈	2024-11-23		伪装代理上限	20 (已使用4个)
cense版本	V3.0.0		中继节点上限	100 (已使用1个)
"品序列号	Fbl9Fzi	/*//. O-fikkcjhf1edag7uEHdCQCzs6w	单中继节点IP上限	8 100 (已使用21)
,	MH3Dł	4FE**********************	小规制占约内上网	1000 (日体用21)
	**********	***************************************	ALTER IN MORNIE THRE	
	********************	**************************************		
,	********	WJ2TZhH+tcYJ+pNDQC		
	5pHap+oMHJU0EIFsn+jqU	KzXXU5N28k9IP/Q9psjq		
	JMORWFOGI ∠			

3.8.4 系统设置

1) 设备信息

设备信息页面展示默安幻阵所有设备的基本情况,其中支持沙箱数量表示该设备最多可 创建的沙箱数,当前沙箱数量表示当前已创建的沙箱数,正在运行沙箱数,正在初始化沙箱, 以及该设备下所有沙箱信息。如下图设备配置;普通用户只能看到相关信息,不能对设备进 行重启操作。如果需要重启某台设备,可选择需要重启的设备,点击重启按钮,设备重启需 要五分钟左右,重启设备之前建议停用所有与该设备相关的沙箱。

虚拟 IP 为幻阵高级模式配置的 nat IP。

民府大盘	基本信息	设备信息				
	子账号管理 授权信息	▲ 设备ID:1 送的中 设备名称: test ∠ 设备IP: 10.0.1.42 版本号:3.1.1			重启服务	点管理 虚拟P
16397839	系统设置 ヘ	网络联通 1h 24h 一周	CPU 负载	1n 24h 一周 内存占用		1h 24h 一周
RREI	设备配置	1 0.8			<u>oo</u> o	 0
服務管理	功能设置	0.6	50 40 30 20	30		
RAGER	白名单 告警设置	00000000000000000000000000000000000000	10 0 14:23 14:33 14:43 14:53	0 15:03 15:13 14:23	14:33 14:43 14:53	15:03 15:13
ERRIT	湖游配置	磁盘占用				
	SecretKey管理	占用量: rootfs 59.89G/199.51G devtmpfs 0.00G/3.81G /dev/vda1 0.1	2G/0.39G	Destant		
10.41	安全性配置	O.14G O.2G Tree	Pcap 0.003	+ 0.06G	- 0.04G	
11110	网络谢试	= 2.593	56.44G 0.00G	• 0.73G		
	数据清理					
	系统升级					

图 3-8-9 设备信息

节点管理页面(仅云化版支持)展示客户端设备下节点卡片信息,包括节点 IP、节点版本、 节点状态、节点标签、Docker 网络、节点资源占用和硬盘占用;



基本信息	节点管理			节点安装
子账号管理	节点状态 全部 在线 离线			P Q
授权信息				
系统设置 🔺	10.0.1.42 3.1.1 (##	10.0.1.12 31.1 (615)	10.0.1.11 3.1.1 Gils	
设备信息	标签	标签	标签	
设备配置	test Z		2	
功能设置	172.67.0.0/16	цоскегряна 172.11.0.0/16	172.15.0.0/16	
白名单	节点资源占用	节点资源占用	节点资源占用	
告警设置	50%) 764G (B/s	8% 3840 325% 00/s	20% 3706 08/4	
測溶配置	CPU 內存 网络	CPU 内存 网络	CPU 内存 网络	
SecretKey管理	硬盘占用	硬盘占用	硬盘占用	
安全性配置	30.2%	25.6%	4.9%	
个性化配置				
网络测试		共3条 《		
数据清理				
系统升级				

图 3-8-9-1

点击【节点安装】按钮可下载节点,节点安装仅支持 linux 操作系统,支持离线下载安装或 复制执行命令进行安装,安装成功后,对应节点将在节点管理页面上线。

节点管理 で点状の 全部 在地 高地	节点安装	×		Reader Contraction
10.0.1.42 3.13 面低 展開 12.07 0.0/16 万点武器合用 CRJ Pi在 D	Curl - H H. "Authorization:Glearer of CREPX/CUR.eg/V/22V/SUGICR/MY HQLC.MZXLWWBijowLCL:n4V3G E29/gov/QOMOIm006881mE2201 804MSV4LWE3/UDE1NVFmZDM27 度188.07 1. 节点安装仅支持inas操作系统、支持系统 2. 支援成功后、对点节点将在专点管理页面	ANDOROCULUSININANGE SINZZXJOUADININANGE SINZZXJOUADININANGE SINZUNI TANANUN DER KITA KATR KATR KATR	00% 965 4.9%	
		#3 ∦ < 1 >		

图 3-8-9-2

2) 设备配置

设备配置包括修改系统时间、下载系统运行日志、一键诊断和 pcap 包下载功能,如下图所示。

备配置	
服务器时间	
系统时间 2	2022-04-25 14:09:10
NTP服务器地址	多个NTP服务器使用英文逗号分隔
1	确定 取消
系统运行日志 🛓	
运行诊断 — 📲 💱 🛙	e.

图 3-8-10 设备配置

3) 功能设置

獣安科技

功能设置包含【攻击源探测开关】、【POST 内容捕获】、【源 IP 获取配置】、【认证配置】;

【POST 内容捕获】:当开启该开关时,会捕获攻击的 post 数据,反之关闭该开关,将不捕获 post 数据;

【攻击源探测】: 可根据用户需求选择开关,此开关开启之后幻阵会反向探测攻击者的信息;

【源 IP 获取配置】:用户可自定义获取攻击源,若关闭获取 header 头,则直接获取 沙箱上一条 IP,当沙箱通过负载均衡映射的情况下,需要开启获取 header 头,幻阵会获取 指定 header 头字段作为攻击者源 IP。用户也可使用生效范围,对特定源 IP 的流量获取 header 头作为攻击源。

功能设置			
攻击源探测 〇 该功能开启后将对攻击	送 者设备进行反向服务探测		
post内容捕获 幻阵系统更详细地实时	关 捕获攻击者流量中post内容字段,以便更为精确地分析。该功能默认开启		
源IP获取配置 该功能可配置如开启X-	発 Forwarded-For括景下的攻击源P		
源IP获取配置 该功能可配置如开启X * Header头字段	ま の ま の ま の ま の ま の ま の ま の ま の ま の ま		
源IP获取配置 该功能可配置如开启x- * Header头字段 获取位置	またのでは Forwarded-Fori 基本での 本語の 本語の 本語の 本語の 本語の 本語の 本語の 本語		



【Radius 认证配置】:用户可以配置 Raduis 认证服务器,配置认证端口,输入 Raduis 服务器的地址,填写共享密钥后,点击【保存】,配置生效。

	1910	
* 认证端口	1812	
*服务器地址	请输入	
* 共享秘钥	请输入	Ø
	保友重置	

【Ldap 认证配置】:用户输入服务器地址、认证账号、认证密码、用户搜索基准、用 户规律规则、用户属性等配置后,点击【保存】,配置生效。

★ 服务器地址	Idaps://192.168.32.25:636	
* 认证账号	cn=admin,dc=example,dc=org	
* 认证密码	*****	ø
* 用户搜索基准	dc=example,dc=org	
* 用户过滤规则	(cn=*)	
* 用户属性	cn	
用户电话属性	mobile	
用户邮箱属性	mail	
	保存重置	



图 3-8-14 功能设置界面

4) 白名单

超级管理员可设置扫描白名单和系统白名单,加入扫描白名单的 IP 如果对默安幻阵的沙 箱、伪装代理等进行了扫描或者手工渗透等,默安幻阵将不记录事件和产生告警;加入系统 白名单的 IP 才能访问默安幻阵管理页面。页面可对白名单进行添加、修改、删除操作。逃 逸检测白名单中的 IP 出现攻击逃逸,系统不会捕获其行为。加入流量阻断白名单中的 IP 将 会放开白名单地址中的流量阻断限制。

白名单			
扫描白名单 系统白名单 逃逸检测白名单	流靈阳断白名单		
开启该功能时,白名单中IP地址机器对系统进行扫描	等操作时,系统不会捕获其任何行为		
白名单状态 🚛 🔵			+ 添加白名单
分組名称	IP列表	操作	
	智无数据		

图 3-8-12 白名单界面

添加白名单,输入相关信息之后,点击确认进入白名单管理界面,状态变为'开'时,表 示白名单开启。

白名单	
扫描白名单 系统白名单 流邊短期白名单 流量用	添加扫描白名单 ×
开启该功能时,白名单中P地址机器对系统进行扫描等操作时,系	* 分组名称 词输入
白名单状态 🚛	* 白名单
分组名称	满作.
	使用回车符分描多个学名中、不可量量、支持网段添加、ਛ多100个
	取消 确定

图 3-8-13 添加扫描白名单界面

5) 告警设置

告警包括系统异常状态告警和入侵事件告警,当默安幻阵系统出现异常状态时会通过配置的邮箱信息实时发送告警邮件,入侵事件告警根据配置的告警频率,以该时间间隔为单位



监测是否有入侵事件发生,如果有则会发送最近的 10 条入侵事件至设置的接收者邮箱告警。 配置界面如下图告警界面所示,填写发送邮件的用户、邮箱服务器信息和接收邮箱等信息, 点击【确定】即可生效;普通用户只能看到相关信息,不能对告警页面进行操作,告警设置 同时还会同步到消息中心。

告警设置			
息中心			
告警提醒 ())) 自定义告警提示音	告警提示音		
高危及以上 high_alar	rm.mp3 🔹	• •	
中危 mid_alarr	m.mp3 🔔	Þ G	
(E.R. low_alarn	m.mp3 🔹	• •	

邮件告警		
发送者邮箱	send@163.com	
发送者用户名	请输入	
邮箱发送者密码	请输入 💋	
SMTP验证方式	v	
邮箱服务器地址	请输入	
邮箱服务器端口	请输入	
证书校验	● 是 ○ 否	
接收者邮箱	recv@163.com,recv@qq.com	注:多个接收者按逗号分割
告警频率(分钟)		注: 1~60之间
	发送测试 确定 重置	

图 3-8-11 告警界面



6) 溯源配置

用户可自定义配置溯源函数,参照左边溯源函数示例模式,每个网络 id 获取后进行 return 即可,当前可直接使用溯源示例函数。同时用户可自定义溯源模块生效时间,可全部 生效,也可选择某天的某个时间段和每周的某个时间段生效。

图 3-8-18 溯源配置

7) SecretKey 管理

幻阵与刃甲进行联动时需要填写 SecretKey,一个 SecretKey 可以对应一个刃甲,也可 以多个刃甲使用同一个 SecretKey。用户可以进行 SecretKey 的添加,复制以及删除操作。

ecretKey管理			+ %t/@SecretiKey
AccessKey		SecretKey .	操作
rp35nrcwzIVIqe1rHOBGmdA2yhTB0KdQbgjVnLcmLdcE 👩		*****	
mO96lbMOzbitzjF0cAfWvGRZPVr1PFTqksXivvOQq8ITS		*****	
	共 2 条 < 1 > 10 条/页 >		

图 3-8-21 SecretKey 管理

8) 安全性配置

安全性配置可以设置允许登陆失败次数、密码长度要求、密码强制更新间隔以及密码强度, 修改安全性配置后,若现用密码不符合安全性配置的要求,在下一次登录时需修改密码;



安全性配置		
无操作退出限制	30	注: 1-1440之间
允许登录失败次数	5	注: 3-99之间
密码长度要求	5 - 18	注: 6-30之间
密码强制更新间隔	1 月 ~	注:1-999之间
密码强度要求	数字 + 字母 🗸	
	确定取消	

9) 个性化配置

包含【安全大屏名称】, 【自定义 logo】, 【页面关键词】 【安全大屏幕名称】可自定义名字 【自定义 logo】可上传登录页面, 主页面 logo, 以及页面图标; 【页面关键字】也可用户自定义,

个性化配置			
自定义	,		
页面关键词	幻阵 🖌		
自定义logo	登录页logo	主页面logo	页面icon
	替换图片	醫換圈片	著换图片

10) 网络测试

网络测试功能提供 ping、traceroute、route、curl、arp、telnet 命令,方便安装测试人员进行现场网络排查。

ning V			
â入IP或城名	执行		
合结果			

图 3-8-20 网络测试



11) 数据清理

用户可以对幻阵数据进行清理。支持按照事件等级、攻击者类型、攻击时间(默认近七 天数据不可删除)进行筛选后进行数据清理。

据清理				
件等级 低危 > 攻击者类型 请注	肆	起止时间 🕒 开始时间	→ 結束时间	确定清理
删除数据归档名称	事件等级	攻击者类型	起止时间	操作
2022-04-20_112403.zip	低危	真人	2022-04-05 00:00:00-2022-04-05 00:00:07	A 8

图 3-8-22 数据清理

12) 网络配置(仅标准版支持)

网络管理页面可查看业务口的网络管理信息,包括网卡名称、IPv4 地址、子网掩码、IPv6 地址、前缀长度、默认网关等;

网络配置							
eno16780032 访问配置:Web服务	活动中 🖍	关闭	IPv4 192.168.110.200	子网掩码 255.255.255.0	IPv6 fec0:0:0:1::200	前缀长度 64	默认网关 192.168.110.1
eno33559296 访问配置: Web服务	活动中 🖌 关闭 PING	关闭 安装页面 开启	IPv4 192.168.0.10	子网掩码 255.255.255.0	IPv6 fd00:9923:9967:9941::124	前缀长度 100	下一跳地址 -

此外还可进行带外管理配置,对管理口配置 IPv4d 地址、子网掩码、下一条地址、开启 web 服务后,点击确定,即可配置成功; PING 服务关闭后,对当前网卡的 IP 地址进行禁 PING 处理;关闭安装页面后,将无法访问安装页面。

-\$-	基本信息		编辑接口		Х			156 😩 admin 🗸
《》 风险大盘	子账号管理 授权信息	网络配置	接口名	ens192				
一型 安全大屏	系统设置 个	ens160 活动中 🖌	* IPV4地址	192.168.0.1		IPv6	前缀长度	默认网关
0	设备信息	访问配置: Web服务 开启 PING	* 子网掩码	255.255.255.0		fec0:0:0:1::200	64	192.168.110.1
威胁情报	设备配置		IPV6地址	请输入IPV6地址			-	-
重风管理	功能设置	ens192 活动中 之 访问配置: Web服务 开启 PING	前缀长度	请输入前缀长度		-	制職长度 	下一跳地址
[]] 报表管理	白名単		下一跳地址	请输入下一跳地址				
8	告警设置		1 Martine					
联动配置	溯源配置		管理网段/掩码	请输入目标网段/掩码或/PV4地址,支持输入多个地址,使用回车符分隔,不可重复				
	SecretKey管理							
1000000	安全性配置			多个地址使用回车符分隔,不可重复	h			
) 日志审计	个性化配置		启用访问管理	Web服务 💿 开启 🔵 关闭				
	网络测试			PING				
帮助中心	数据清理			安装页页				
	网络配置							
	配置备份							
	系统升级			取消 稳定				



13) 配置备份

配置备份页面支持备份系统配置,点击手动备份后,生成一条备份记录,生成的备份记录支 持下载、恢复与删除;下载的数据支持导入配置。

() 风险大会	了 赋 号 邕 珪 	配置备份			
一 安全大屏	系统设置 ^	备份类型 全部 > 备份时间 开始时间	→ 结束时间	8	手动备份 导入配置
۲	设备信息				
威胁情报	设备配置	备份名称	备份类型	备份时间	操作
	功能设置	2023-01-12_113452.zip	手动备份	2023-01-12 11:34:52	± 0 0
间 报表管理	白名单	2023-01-12_104553.zip	导入配置	2023-01-12 10:45:53	* •
联动配置	告警设置 溯源配置	2023-01-12_104011.zip	导入配置	2023-01-12 10:40:11	
	SecretKey管理	2023-01-12_102841.zip	导入配置	2023-01-12 10:28:42	± 0 0
R.Z.BH	安全性配置	2023-01-12_102321.zip	导入配置	2023-01-12 10:23:22	± 0 0
日志审计	个性化配置网络测试	2023-01-12_102307.zip	手动备份	2023-01-12 10:23:08	± 0 0
帮助中心	数据清理	2023-01-12_101921.zip	导入配置	2023-01-12 10:19:22	200
	网络配置	2023-01-12_101350.zip	导入配置	2023-01-12 10:13:50	* •

3.8.5 系统升级

该页面可显示当前版本,版本更新概要以及历史版本

系统升级					
● 当前 系统	Ⅰ版本3.0.0 ^{升级}			b 版本更新概要 底层架构升级、提升系统性指标定少端插件化、自定义模型 docker镜像 新增数据仿真功能,提升沙和 反制能力提升、可获取黑客 反制术马支持一键免杀功能 伪装代理支持IPV6	能 反支持上传 商具实性 更多数据
规则库升级 👤					
历史版本					
升级版本	升级类型	升级时间	状态	操作人员	操作

用户可点击【选择文件】按钮选择更新的文件压缩包,等待上传完成后进行升级,此过 程耗时较长,且此过程是自动进行,出现"上传 100%"字样后会有较长时间停留,请耐心等待, 升级成功后,在历史版本中可见新的升级记录;



组织 🔹 新建文件夹 名称 修改日期 类型 大小 🙆 OneDrive HP_20181031112646.tar.gz 2018/10/31 22:31 WinRAR 压缩文件 615,147 KB 🔲 此电脑 1 3D 对象 当前版本2.2.1 视频 📰 图片 选择文件 🔮 文档 ↓ 下载 图 3-8-24 选择上传文件页面 系统升级 版本更 当前版本2.2.1 上传进度: 图 3-8-25 上传文件界面 升级详情 \times 40% 管理端更新初始化中 图 3-8-26 初始化界面 升级详情 \times 管理端更新初始化中 管理端更新开始 管理端更新完成 图 3-8-27 管理端更新完成界面 历史版本 升级版本 升级时间 状态 操作人员

图 3-8-23 系统升级界面

图 3-8-28 升级完成界面

2018-11-05 13:04:45

操作

R

admin

升级成功

2.2.1 -> 2.2.2_final_test



点击 國际可查看升级详情,	如下图所示:		
	 文溯源模块优化更新,增加更多指纹 年icmp流量控制 音密码支持特殊字符 Issh, mysql, samba部分监控事件 分bug修改优化 		
升级时间	状态	操作人员	操作
2018-11-05 14:56:22	升级成功	admin	R

图 3-8-29 升级详情界面

3.9 日志审计

日志审计页面只有超级管理员可以清空日志,审计员有权限查看相应审计信息,日志审 计页面会详细记录如下图日志审计页面包括登录用户、登录 IP、所有账户操作事件(包括添 加用户、用户登录、用户注销、删除用户),以及审计时间;日志审计页面提供清空日志、 下载 xls 日志报表、以及查询功能,超级管理员可以看到所有用户的操作记录。

(0 10 10 10	日志审计			全部清空 下戰損表
·····································	起止时间 开始时间	→ 結束时间 🖸		登录炉 > 清給入 Q
() ADMARI	登录用户	豐豪P	审计事件	·····································
	▼ admin		删除沙箱	2022-11-09 15:23:44
ात् सम्राप्त	▼ admin		编辑伪装代理配置	2022-11-09 15:20:50
INEE INEE	▼ admin		启动沙箱	2022-11-09 15:20:39
	▼ admin		師代獻書	2022-11-09 15:20:35
ana a	▼ admin		删除沙箱	2022-11-09 15:20:14
10.011	▼ admin		启动沙箱	2022-11-09 15:12:15
10 9 0	▼ admin		编辑沙瑞	2022-11-09 15:12:13
	▼ admin		源加沙箱	2022-11-09 15:12:09
	▼ admin		删除沙箱	2022-11-09 15:11:44
	▼ admin		意出	2022-11-09 15:10:36

图 3-9-1 日志审计

3.10 帮助中心

帮助中心页面分为新手引导、产品文档以及免责声明页面。



ф.,		
(P) ()放大盘	帮助中心	
8		
史全大屏	動手引导	
E ANNAL CONTRACT	- <u>O-</u> - <u>O-</u> 配置指南	
लक्षाय		
(10) 日本世現	产品文档	
	→ 用户手册下载	
	免责声明	
2849919 	免责声明	
志审计		
ERD PLO		

图 3-10-1 帮助中心页面

用户可以点击新手引导->配置指南查看幻阵基础配置及使用手法。

图 3-10-2 配置指南页面

不同权限的用户可以下载相对应权限的用户手册,超级管理员可以查看和下载产品 API

		Q 💿 (R) hp_160 ∨
首页 > 帮助中心 > 接口文档		
幻阵接口文档		L API文档下载
登陆	登陆验证	
f I		
用户	使用 cre	
获取当前用户信息	(59):	
沙箱	y=secretkey, r age=estmod='j°) message平段中的dat 参数: 通过hame。参数顺序按字典序进端, data:	
获取沙福列表	count=108pa 1582 RL: count=10 usta 16208(-2168toke x6/b1 /bdfse22e a53/	
SYSLOG	Python 元1911	
SVSLOORINE	<pre>def CatFMLIAT():</pre>	



图 3-10-3 产品文档界面

用户可以点击免责声明查看杭州默安科技有限公司的免责声明文档。

声明	
	免责声明
	攻击反制模块描于得交互獲明内的安全指件。依托该插件可对其人攻击者进行设备相绞,社交转号。攻击IP等 属性信息进行管部调牌,为安全等种化量制造进性传统。方分储器内容全,有效高幅着在攻击者。该模块描于 能动物学年代,不主动分外界起动物,不会对某些运动问题并在何间起。
	针对攻击反制模块的开启、应用、关闭等功能,仅限超级管理员账号拥有操作权限,并指运专人负责,做到权限与管理责任的统一。如有人员变动,应按相视者的交接流程进行责任人变更。
	根据实际安全需求启用攻击反制爆块时,应严格按照内部审批方式、审批流程进行审批。原则上由需求部门发 起申请,安全退绳及安全监管部门进行审批,审批通过后由专人负责启用并通知各租失部门和人员。
	依据各些管机构及安全设备报卷机制,应针对攻击反制模块所属的P、MDS、模块各称等属性但息使把报备流 程进行报告。在政防深场、渗透测试、安全检查等活动过程中,须根据实际情况,向相关部门或人员提前进行攻击
	反制硬块的路會。 攻击反制模块在线使用过程中,应严格控制模块使用范围,不能使模块脱离高交互重网环境。禁止除平台组级 等零品/VAAAGE4.XNE下数 看到 传播 无限UGG目2000用于—Intertocet的目标的话题
	●空気のたいというためには、ない、(の)、(の)、(の)、(の)、(の)、(の)、(の)、(の)、(の)、(の)
	幻阵带级威胁检测系统攻击反制模块在用户使用期间均属于用户保建设产,需谨慎使用,因使用不当而引起的 纠纷和造成的一切后果、责任载由用户(即使用方)承担,与抗州就安科技有限公司无关。
	特比罵明! 杭州默卖科技有限公司

图 3-10-4 免责声明界面

3.11 消息中心

消息中心用来展示相关攻击行为的告警,分为全部消息,处理消息以及已处理消息。使 用者可以根据风险等级进行筛选,并且可以一键忽略全部消息或忽略中危低危消息。点击详

情"[■]"便会跳转到攻击事件回放页面,点击处理"[▲]"弹出消息处理弹窗,如下图所示,使 用者可以加上处理意见,点击忽略"[●]"即可忽略攻击消息。

风险大盘	消息中心				护眼模式 🗊 自动刷新 🗊
· 安全大原	全部消息 未处理消息 已久	达理消息			
10 110/115	严重 9		^{高性} 18	中應 3	低危 203
● 同時理 記 記表管理	风险等级 全部 🗸				忽略中危低危 忽略全部 设置推进户
() ROER	时间	告警内容			状态 操作
	2022-04-20 16:45:00	资产外部资产(192.168.110	160:5550)受到攻击,攻击源:192.168.30.214,风险等级 严重		• 未处理 日 1 0
E E	2022-04-20 16:45:00	沙箱 (172.16.23.12) 受到政	击,攻击源:192.168.30.214,风险等级 高危		• 未处理 🖬 🌲 💿
日志事け	2022-04-20 16:40:35	资产外部资产(192.168.110	.160:5550)受到攻击,攻击源:192.168.30.172,风险等级 严重		• 未处理 🔲 🚢 💿
帮助中心	2022-04-20 16:40:35	沙箱 (172.16.23.12) 受到攻	击,攻击源: 192.168.30.172,风险等级高危		• 未处理 目 1 0
	2022-04-20 15:13:54	资产外部资产(192.168.110	.160:5550)受到攻击,攻击源:192.168.31.120,风险等级 严重		• 未处理 日 上 0
	2022-04-20 15:13:54	沙箱 () 受到攻击,攻击源	192.168.31.120, 风险等级 高危		• 未处理 日 4 0
	2022-04-20 11:38:46	资产外部资产(192.168.110	.160:5550)受到攻击,攻击源:192.168.30.205,风险等级 严重		• 未处理 🔲 🛓 🔍
	2022-04-20 11:38:46	沙箱 () 受到攻击,攻击源:	192.168.30.205, 风险等级 高危		• 未处理 日 ▲ ●
	2022-04-20 11:24:18	沙箱 () 受到攻击,攻击源	10.87.1.1, 风险等级 高危		● 未处理 日 ▲ ●

图 3-11-1 消息中心



消息中心			产根模式 🕕 自动服新 🗇
全部消息 未处理消息	已处理消息	消息处理	
		封间 2022-04-20 16:45:00 风险等级 ● 产量 内容 西产分部资产 (192:168:110:160:5550) 受到攻击,攻击源:19	na 203
見始等級 全部 >		2.168.30.214, 风险等级 严重 处理	お除中危低危 お除全部 以其他之中
时间	告誓内容	A	805 B(1)
2022-04-20 16:45:00	责产外部资产(192.168.110.160.5550)受到攻	取消 确定	• 未处理 🔲 主 O
2022-04-20 16:45:00	沙箱 (172.16.23.12) 受到攻击,攻击遭: 192.16	8.30.214,风能等级 高危	● 未处理 □ ▲ ●
2022-04-20 16:40:35	资产外部资产 (192.168.110.160.5550) 受到攻(5、攻击源:192.168.30.172,风险等级 产重	* #211 E 4 0
2022-04-20 16:40:35	沙箱 (172.16.23.12) 受到攻击, 攻击源: 192.16	8.30.172, 风险等级 高危	• #111 E 1 0
2022-04-20 15:13:54	责产外部责产(192.168.110.160.5550)受到攻	5. 攻击源: 192.168.31.120, 风险等级 严重	• 未处理 目 主 〇

图 3-11-2 消息处理

附录 A 自定义沙箱部署说明

i. 自定义沙箱说明

定义沙箱主要是为了用户根据自己的需求在自定义虚拟机里面部署仿真业务系统, 仿真 业务系统主要用于模仿用户真实业务站点, 吸引攻击者入侵。

自定义沙箱为 linux 系统的虚拟机, 自带 apache 和 ngnix 反向代理。

ii. 自定义沙箱部署

a) 新建自定义沙箱

在默安幻阵 web 管理云端新建一个自定义沙箱,记住自定义沙箱的 IP 地址、用户名和 密码。

b) 查看修改配置

- 登录自定义沙箱 利用 ssh 登录自定义沙箱 ssh 用户名/密码
- 查看 80 端口
 输入命令: netstat -tnlp 查看 80 端口是否已经打开;
 打开为正常;如果 80 端口没有打开,可销毁沙箱之后,重新新建自定义沙箱。
- 修改 apache 默认 webserver 的监听端口(默认 apache 监听端口为 80;设置成:
 127.0.0.1:8000)
 cd /etc/httpd/conf



vim httpd.conf

/Listen 回车,找到Listen 80;

#注释此行(shift+#),添加新行: Listen 127.0.0.1:8000(:wq保存退出)

将网站资源拷贝至自定义沙箱的指定目录
 将 html页面拷贝到: /var/www/html下面(将下面命令行中的192.168.100.100
 修改为沙箱 IP);
 linux: scp -r [资源包文件目录] root@192.168.100.100:/var/www/html/
 windows: 安装 putty.exe 和 pscp.exe

cmd 命令: pscp -scp [本地文件路劲] root@192.168.100.100:/var/www/html

■ 启动 apache

httpd -k restart;

验证: 配置完成之后,通过浏览器访问 <u>http://192.168.100.100/1.html(1.html</u>为上传的文件名),正常返回页面即可。