Rooma Sec 戎码安全

技术白皮书

戎码翼龙 **AI原生NG-EDR**

可免费试用 支持公有云SaaS

安全快
业务能更快

覆盖ATT&CK安全框架，云原生架构搭载内核级轻量传感器
更快发现隐蔽性强的新型攻击

微信公众号
137-1769-9956

客服企业微信
kefu@rongma.com

目录

01 NG-EDR介绍

什么是NG-EDR?

当前EDR面临的问题：新型攻击研判慢

慢的原因

- 由于技术问题造成终端行为捕获不全，有些行为没有被捕获，导致线索漏报
- 采集的威胁行为产生了大量告警，“草木皆兵”很难区分重点，需要大量人工参与，导致不能及时研判

如何变快?

戎码定义的NG-EDR

AI原生

- 基于生成式AI，原本需要安全专家几天的分析工作，可以在几分钟内快速生成攻击分析报告

新型攻击检出和溯源更快

- 智能汇聚威胁事件，将大量告警进行知识图谱关联，浓缩成需要客户关注的重点事件，研判新型攻击更快

02 四大优势

戎码翼龙NG-EDR优势

传统终端安全产品	VS	戎码翼龙AI原生NG-EDR
慢		快

捕获新型攻击有多快?

威胁检测 智能技术，分钟级检测!

- ✕ AV
  依赖文件HASH等特征检测，由于新型攻击没有已知特征，因此难以发现
- ✕ 普通EDR
  产生大量行为告警，“草木皆兵”很难区分重点，需要大量人工参与，耗时耗力，研判攻击很慢

- ✓ 基于行为的智能检测，即使文件特征（如HASH）不断变化，也可精准检出
- ✓ 智能汇聚威胁事件，有价值的线索不会被大量告警淹没，新型攻击快速检测

输出威胁报告有多快?

攻击溯源 生成式AI，即写即出!

- ✕ 报告内容需要人工调查和溯源，至少需要数天才能完成

- ✓ 使用生成式AI，界面展示的详细攻击详情和上下文溯源信息，可直接生成/导出威胁报告

传感器运行速度有多快?

数据采集 内核级轻量客户端不卡机!

- ✕ CPU占用超过1%甚至10%，内存占用数十兆甚至数百兆

- ✓ 终端CPU通常占用<0.1%，终端内存通常占用<15M

安装部署有多快?

安装部署 SaaS部署，登录即用!

- ✕ 采购、安装复杂，数天甚至数周用户才能开始使用

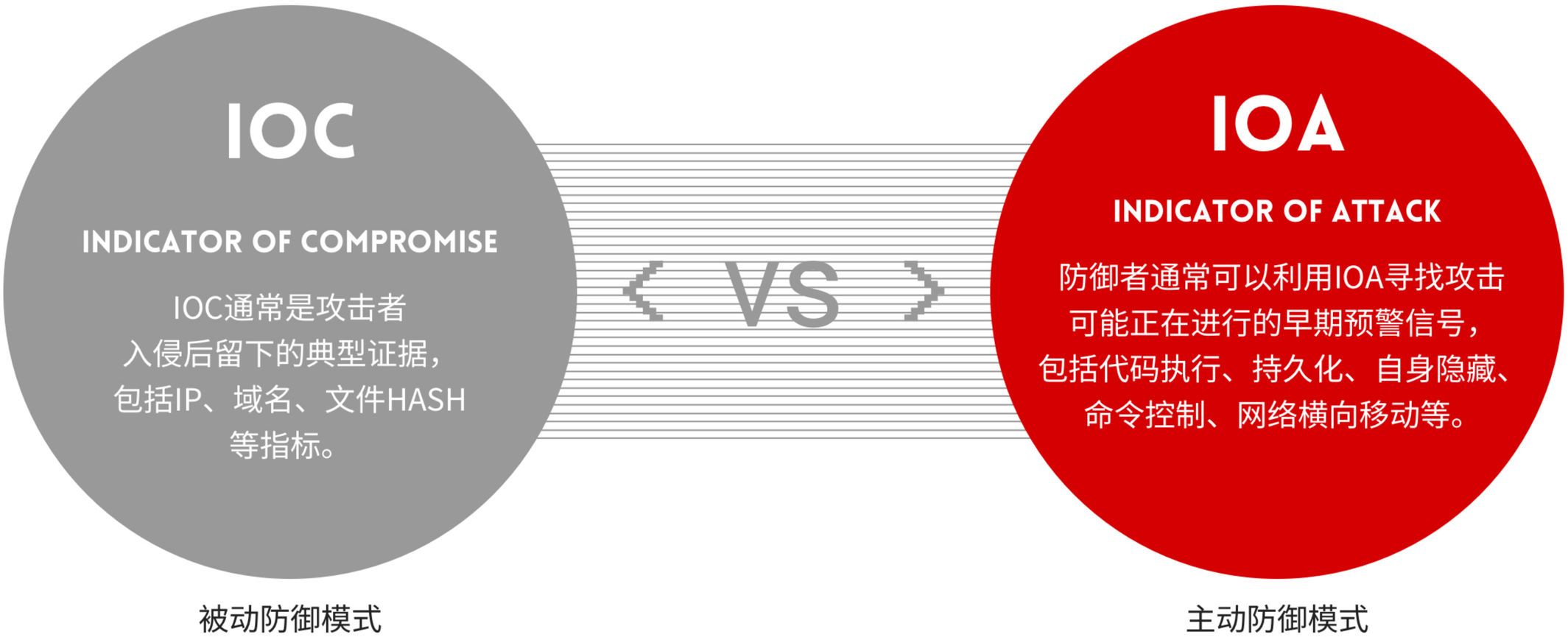
- ✓ 支持公有云SaaS部署，云端下载安装轻量传感器即可开始使用

>400	>2000	<0.1%	<15M
覆盖ATT&CK攻击技术	支持检出的攻击模式	终端CPU通常占用	终端内存通常占用

优势1：威胁检测 更快

智能技术，分钟级检测

- 基于行为的智能检测，即使文件特征（如HASH）不断变化，也可精准检出



被动防御模式　　主动防御模式

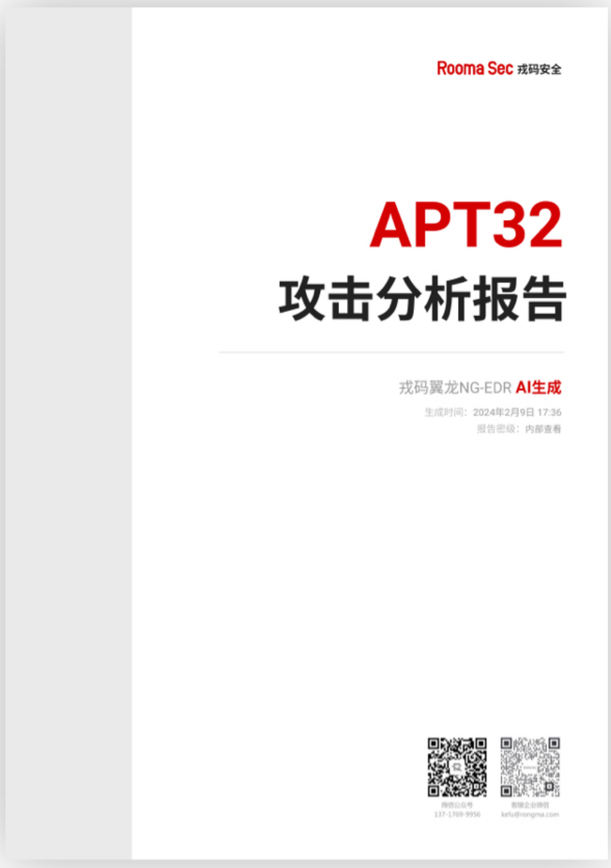
- 智能汇聚威胁事件，有价值的线索不会被大量告警淹没，新型攻击快速检测

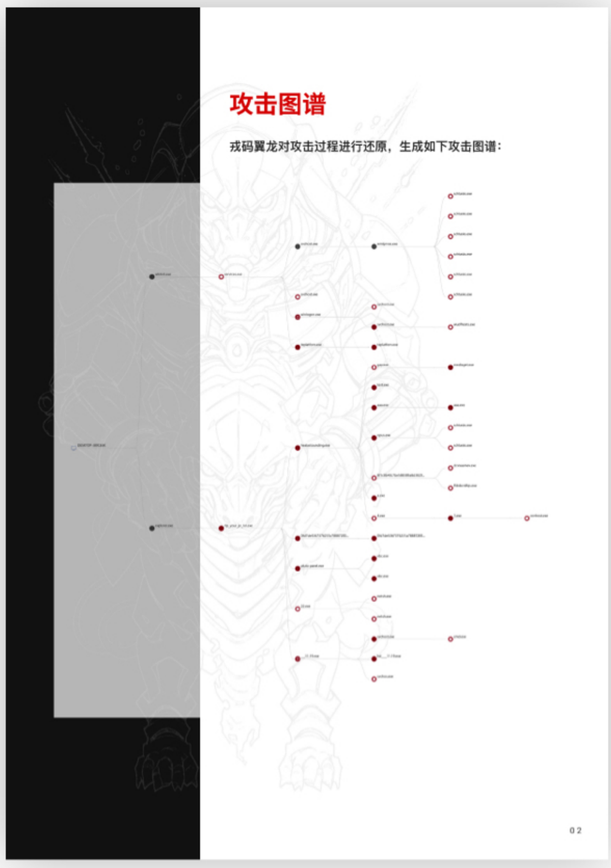
事件分数	事件包含告警		主机		时间线		标签			
严重 10/10	防御绕过-内存代码加载	16	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	危害一破坏系统还原数据	2	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	未处置		
	其他告警	8	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共26条	连接IP	216.285.101						
高 6.7/10	横向移动-远程服务	8	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	危害一破坏系统还原数据	1	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	处置中		
	其他告警	1	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共10条	连接IP	216.285.101						
高 6.6/10	防御绕过-内存代码加载	6	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	权限维持-windows服务	10	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	已处置		
	其他告警	12	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共28条	连接IP	216.285.101						
中 2.6/10	执行-恶意文件	5	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	权限维持-windows服务	6	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	误报反馈		
	其他告警	10	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共21条	连接IP	216.285.101						
低 2.3/10	防御绕过- 隐藏文件和目录	16	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	自定义情报-威胁指标	2	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	误报反馈		
	其他告警	8	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共26条	连接IP	216.285.101						
低 1.2/10	自定义情报-威胁指标	12	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	凭据访问-LSASS内存	2	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	误报反馈		
	其他告警	6	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共20条	连接IP	216.285.101						
低 1.1/10	自定义情报-威胁指标	16	主机名	DESKTOP-A4PH56B	事件开始时间	2024-02-27 15:07:50	事件名称	DESKTOP-DVKGSVD-2024011110	查看 编辑	AI生成报告
	凭据访问-LSASS内存	2	操作系统	windows 10	事件结束时间	2024-02-27 15:08:40	状态	误报反馈		
	其他告警	8	互联网IP	216.285.101	持续时间	1h 0m 0s				
		共26条	连接IP	216.285.101						

优势2：攻击溯源 更快

生成式AI，即写即出

- 使用生成式AI，界面展示的详细攻击详情和上下文溯源信息，可直接生成/导出威胁报告





• • •

优势3：数据采集 更快

内核级轻量客户端

- >80%数据通过Windows内核采集，因此可以做到客户端非常轻，比同类产品对终端的资源占用少

	戎码翼龙	CrowdStrike	微软ATP	国内某EDR友商
传感器的资源占用 -CPU通常占用	<0.1%	<1%	1.0%	0.5%
传感器的资源占用 -内存通常占用	<15M	227M	70M	30M

什么是 内核级数据采集?

Window内核级数据采集是一种高级技术，它允许开发者或系统管理员**在操作系统内核中监控和收集各种系统信息**，包括**进程和线程活动、内存使用情况、网络流量、文件系统操作等。内核级数据采集在系统管理、性能优化、安全分析等领域具有广泛的应用**

为什么 内核级数据采集更具优势?

通过内核级数据采集，可以**获取更底层、更全面的系统信息**，而不仅限于用户空间可见的数据，这对于系统性能分析、安全监控和故障排查等方面非常有用。而且，相对于用户模式数据采集来说，**内核级数据采集速度更快、资源开销更少**

为什么 戎码能做到?

戎码翼龙的**研发团队专业性强，既有深厚的学术背景和理论知识，又有多年内核级数据采集的丰富经验**。这支专家团队在终端数据采集领域不断取得技术突破，**帮助用户高效应对愈加严峻的安全挑战**

优势4：安装部署 更快

SaaS部署，登录即用

- 支持公有云SaaS部署，云端下载安装轻量传感器，即可开始使用

提供SaaS化服务

云原生架构，几分钟即可完成部署，即开即用，方便动态扩展端点数和时间

内核级轻量客户端不卡机

支持管理员对客户端统一静默安装，内核级轻量客户端不卡机

安全专家云端实时威胁狩猎

一旦发现紧急威胁，及时通知客户并协助解决

03 怎么做到的

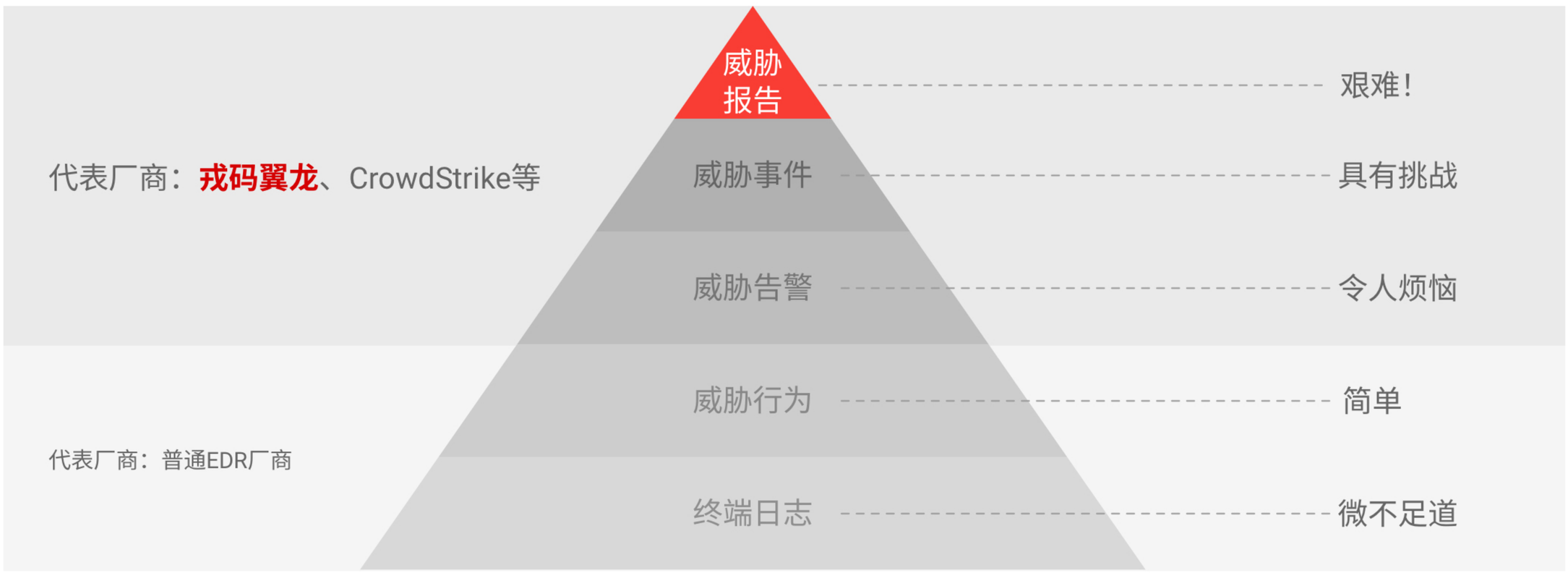
戎码是如何做到的?

卓越的内核级轻量传感器

- 全面收集终端行为日志，采用内核级数据采集技术，客户端轻量不卡机

强大的高级威胁洞察能力

- 基于海量日志，通过戎码特色算法高效智能检测威胁事件，快速形成威胁报告，还原攻击过程，省时省力



高级威胁洞察金字塔（Pyramid of Threat Insight）

04 四大应用场景

典型应用场景与实战

深度检测 勒索攻击

- 基于威胁行为的深度检测，数据恢复兜底，双重保护更安心

有效检测 无文件攻击

- 静态内存侦测和动态行为监测双管齐下，无文件攻击无处逃逸

有效检测 钓鱼攻击

- 静态特征和动态行为追踪相结合，新型“鱼饵”准确检测

有效检测 挖矿攻击

- 聚焦威胁行为，有效发现矿池和矿机

04 典型应用场景与实战

深度检测 勒索攻击

日益严峻的勒索软件攻击

近年来，勒索软件已成为具有破坏性的恶意软件之一，黑客通过加密受害者的重要文件然后索要赎金以牟取暴利。RaaS（Ransomware as a Service）已经悄然成为黑色产业链，越来越多的组织和个人成为黑客的攻击目标。黑客不断提升攻击技术，变换文件特征，以逃避传统终端安全产品依赖特征的静态检测模式。

戎码翼龙解决方案

传统终端安全产品 易漏报

新型的勒索软件层出不穷，基于静态特征检测的传统终端安全软件易漏报，基于威胁行为的高级威胁检测系统能解决这个难题。

VS

戎码翼龙终端安全产品，双重保护更安心

- ✔ 可深度检测防御Lockbit、WastedLocker、WannaCry等数十种国内外广泛传播的勒索软件；
- ✔ 基于AI的智能威胁行为检测，覆盖ATT&CK，实时监测异常行为，深度检测和阻止勒索软件运行；
- ✔ 通过文件回滚技术兜底防护，全力恢复被加密的文件。

01

看见：动态行为检测

- ✔ 基于AI的智能威胁行为识别，覆盖ATT&CK，可有效检测隐蔽性强的高级勒索软件；
- ✔ 采集完整的进程上下文，聚焦动态异常行为，变异和未知的勒索软件也能有效识别；
- ✔ 有效识别无文件攻击，没有文件落地的高级勒索软件也无处逃逸。

02

阻断：阻止勒索软件运行

- ✔ 实时阻止勒索软件恶意行为，防止文件数据被加密；
- ✔ 通过云端海量恶意特征指标，秒级阻止流行度高的已知勒索软件运行；
- ✔ 阻止恶意进程创建，从根本上阻断勒索软件运行。

03

兜底：数据恢复兜底

- ✔ 深度防御勒索软件和数据恢复兜底双保险，双重保护更安心；
- ✔ 文件回滚技术和内存密钥提取技术，提供兜底保护，回滚被勒索的文件，保护重要数据。

LockBit是一种危害性极强的新型勒索软件，已发展到V3.0版本。该勒索软件采用多线程加密，因此加密速度非常快；加密模式为一个文件一个密钥，可破坏系统还原功能，一旦被攻击成功，很难恢复。

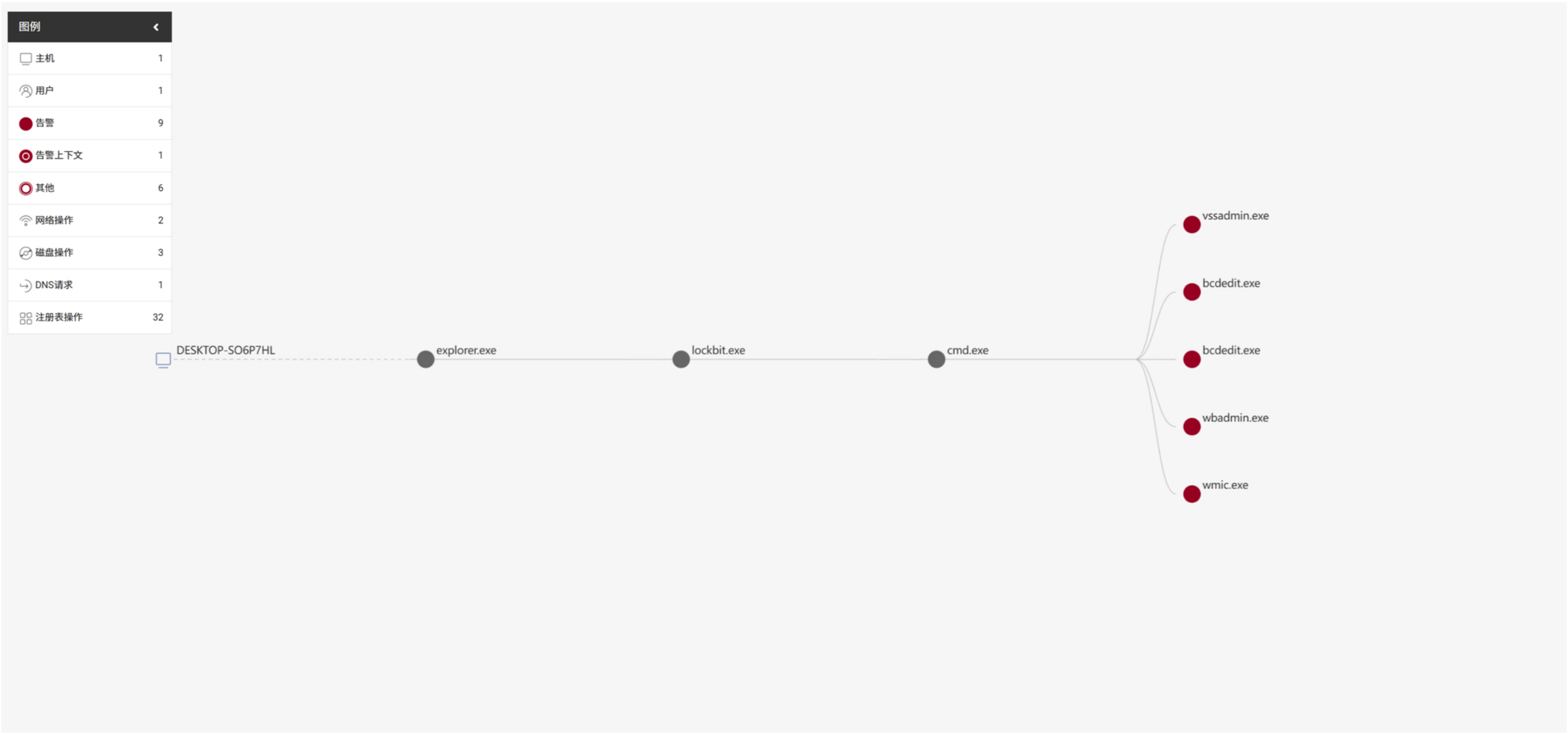
04 典型应用场景与实战

深度检测 勒索攻击

威胁事件概览

事件分数	事件包含告警		主机		时间线		标签		
严重	危害 — 破坏系统还原数据	9	主机名	DESKTOP-SO6P7HL	事件开始时间	2024-02-28 18:58:58	事件名称	DESKTOP-SO6P7HL-2024022818	
9.9 /10	横向移动 — SMB/Windows 共享	1	操作系统	Windows 10 build 19045	事件结束时间	2024-02-28 19:00:00	状态	未处置	
	其他告警	6	互联网IP	192.168.111.78	持续时间	0h 1m 2s			查看 编辑
		共 16 条	连接IP	192.168.156.199					

威胁事件Graph图



ATT&CK矩阵

初始访问	执行	权限维持	权限提升	防御绕过	凭据访问	发现	横向移动	收集	命令与控制	数据泄露	危害
	T1204: 用户执行	T1547: 开机自启	T1547: 开机自启	T1497: 反虚拟机		T1497: 反虚拟机	T1021: 远程服务				T1490: 破坏系统还原数据
	T1204.002: 恶意文件	T1547.001: 注册表运行键 / 启动文件夹	T1547.001: 注册表运行键 / 启动文件夹	T1497.003: 基于时间的逃逸		T1497.003: 基于时间的逃逸	T1021.002: SMB/Windows 共享				T1486: 通过数据加密实现影响与破坏
	T1106: 通过本机API执行		T1548: 滥用权限提升控制机制	T1548: 滥用权限提升控制机制		T1057: 进程发现					

有效检测 无文件攻击

入侵成功概率非常高的无文件攻击

无文件攻击是一种新型的攻击方式，是指不向硬盘写入可执行文件的攻击方法。攻击者利用系统或应用软件漏洞、盗用口令等方法，获取访问权限。在获得访问权限后，利用操作系统自带工具或机制，如PowerShell、PsExec、WMI、注册表、MBR等进行更深度的渗透和持久化。

由于没有文件落地到磁盘，这种特殊的攻击方式特别容易规避传统终端安全产品的检测，是黑客非常青睐的新型攻击方式，入侵成功概率非常高。

戎码翼龙 解决方案

传统终端安全产品 很难检出

与大多数恶意软件不同，无文件攻击并不会在硬盘中留下蛛丝马迹，由于没有病毒文件，传统基于文件扫描的防病毒软件很难发现。

VS

戎码翼龙基于AI的智能威胁行为监测

- ✓ 聚焦可疑行为（代码执行、试图隐身和横向移动等），无论从文件启动，还是从内存启动，都很难逃避检测；
- ✓ 关注进程上下文和行为顺序，即使使用合法帐户（通常是窃取的凭证）实施的恶意行为也能有效检测；
- ✓ 利用合法的工具（如PowerShell）写入恶意代码，进行脚本混淆（加密）也能有效检测。

01 通过脚本攻击

——通过vbs/js/powershell脚本，执行恶意代码

解决方案

- ✓ 接管脚本执行引擎
- ✓ 在内存中解析脚本
- ✓ 获取干净、无混淆的脚本原始代码进行检测

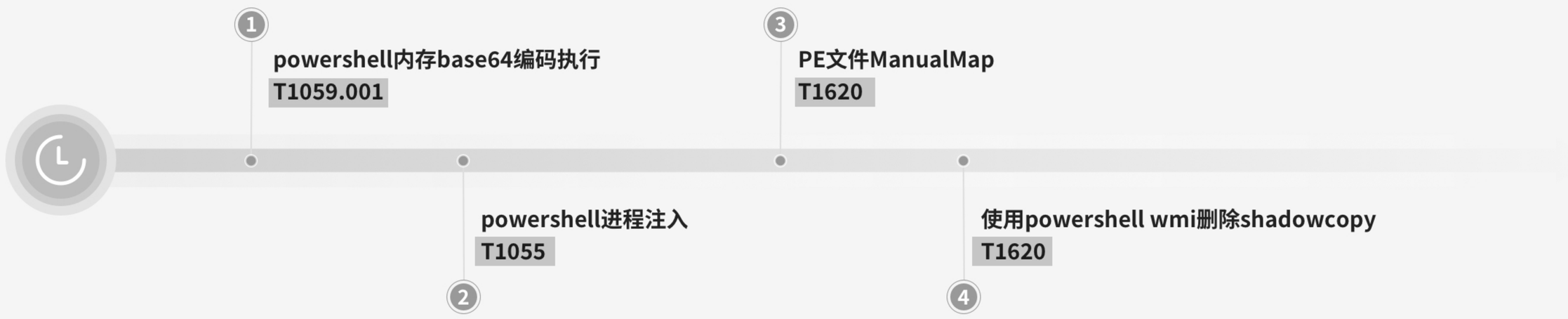
02 通过文档攻击

——通过office、pdf这些办公文档的漏洞、宏等手段执行恶意代码

解决方案

- ✓ 对文档在内存中的代码进行静态检查
- ✓ 针对后续行为进行动态检查，一旦发现可疑行为及时报警

利用Windows合法系统工具PowerShell在内存中执行恶意代码，整个过程没有文件落地到磁盘，从而逃避传统终端安全产品基于静态签名和文件特征扫描的检测模式。

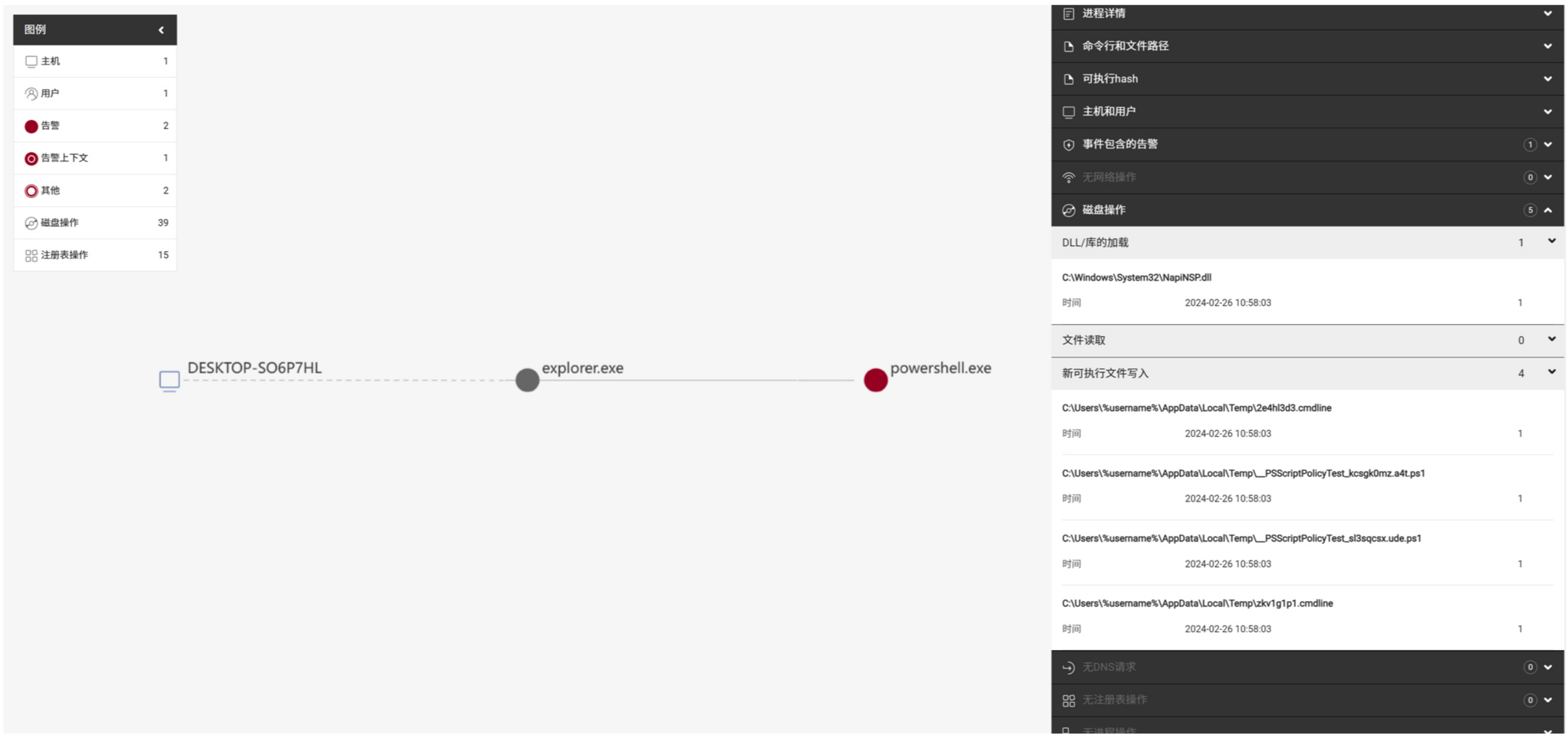


有效检测 无文件攻击

威胁事件概览

事件分数	事件包含告警		主机		时间线		标签		
严重	危害 — 破坏系统还原数据	2	主机名	DESKTOP-SO6P7HL	事件开始时间	2024-02-26 10:58:03	事件名称	无文件攻击	
9.3/10	权限提升 — 进程注入	1	操作系统	Windows 10 build 19045	事件结束时间	2024-02-26 10:58:03	状态	处置中	
	其他告警	2	互联网IP	192.168.111.78	持续时间	0h 0m 1s			查看 编辑
		共 5 条	连接IP	192.168.156.131					

威胁事件Graph图



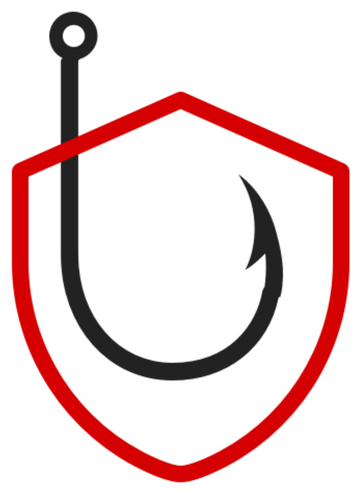
ATT&CK矩阵

初始访问	执行	权限维持	权限提升	防御绕过	凭据访问	发现	横向移动	收集	命令与控制	数据泄露	危害
	T1059: 命令与脚本解析器 T1059.001: PowerShell		T1055: 进程注入	T1620: 内存代码加载 T1055: 进程注入							T1490: 破坏系统还原数据

有效检测 钓鱼攻击

网络钓鱼已成为非常流行的攻击手法之一

网络钓鱼攻击通过诱导受害者点击恶意链接或下载恶意软件，达到信息窃取、传播恶意软件或网络诈骗的目的。黑客通常以邮件、短信、即时通信工具发送“鱼饵”引诱点击，攻击者在诱饵上大做文章，想方设法吸引受害者点击。虽然钓鱼攻击由来已久，但由于成本低收益高，黑客经常将钓鱼攻击作为入侵组织的入口。由于员工安全意识不足和“鱼饵”不断更新，组织受害概率高，感染扩散快，已成为组织安全管理员非常头疼的攻击方式。



戎码翼龙 解决方案

传统终端安全产品 **易漏报**

由于黑客经常变换“鱼饵”，基于静态特征的传统终端安全产品易漏报，可能造成重要信息被窃取、恶意软件快速传播等风险。

VS

戎码翼龙特征和行为检测双管齐下，有效检测钓鱼攻击

- ✓ 基于静态特征的钓鱼攻击检测；
- ✓ 行为动态监控，一旦发现可疑行为及时报警。

基于ATT&CK与自有钓鱼检测模型，静态特征和动态行为追踪相结合，有效检测钓鱼攻击

网络钓鱼攻击检测维度

- 域名可信度
- 网站证书
- 网站指纹

文件钓鱼攻击检测维度

- 文件特征
- 文件图标
- 文件行为
- 文件相似度
- 文件基因家族
- 文件流行度

通过精心构造的“鱼饵”欺骗用户，将恶意软件伪装成“免杀”的文档发给受害者，引诱其点击或分享，以逃避传统终端安全产品基于静态特征的检测。

1. 云端机器学习检测到恶意文件 T1204.002
2. 疑似钓鱼进程启动 T1566
3. 通过WMI API执行程序 T1047
4. 疑似勒索软件大范围修改文件 T1486

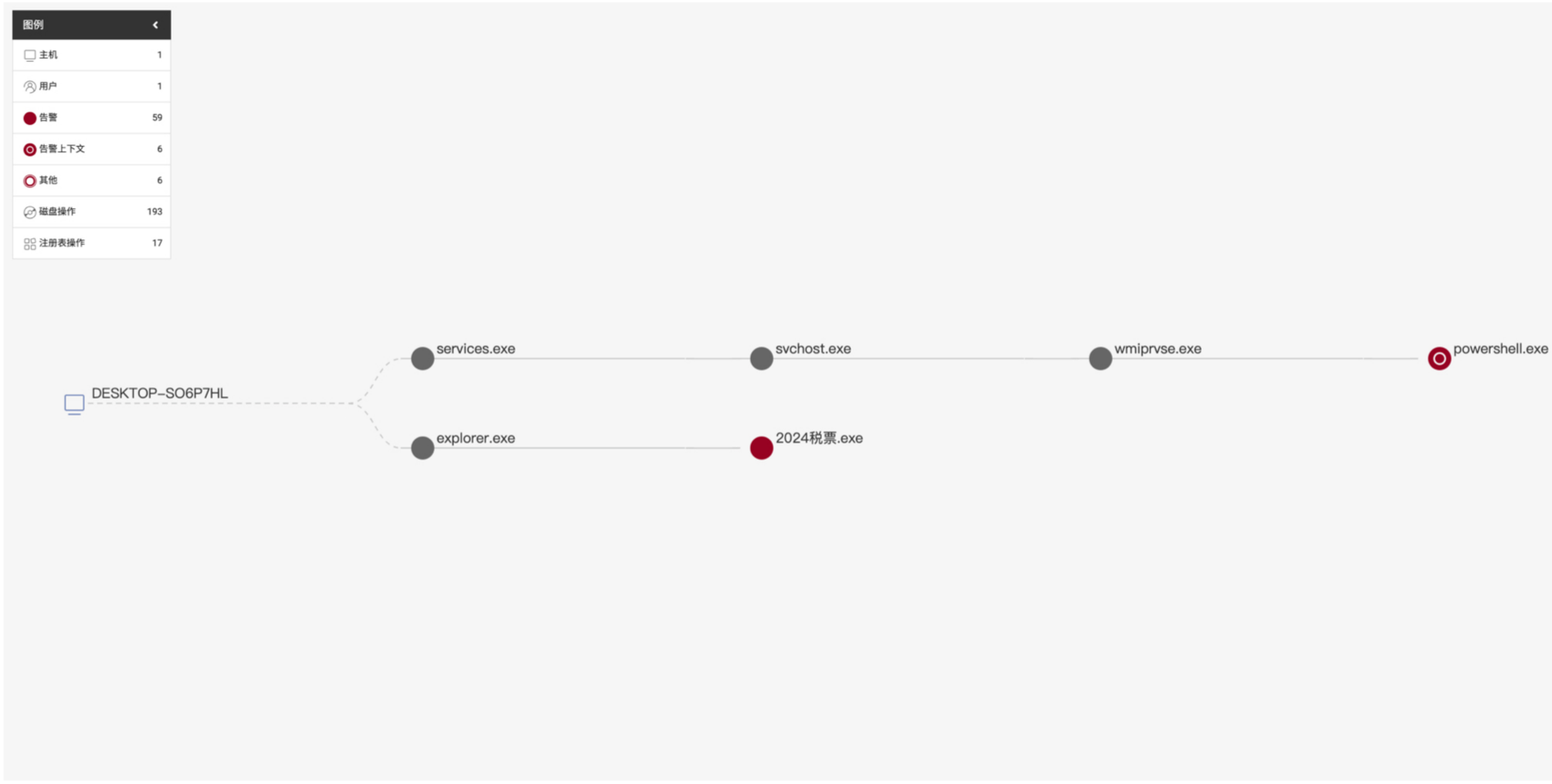
04 典型应用场景与实战

有效检测 钓鱼攻击

威胁事件概览

事件分数	事件包含告警		主机		时间线		标签		
严重	危害 — 通过数据加密实现影响与破坏	59	主机名	DESKTOP-SO6P7HL	事件开始时间	2024-02-26 14:27:14	事件名称	钓鱼	
9.7 /10	执行 — Windows管理规范（WMI）	6	操作系统	Windows 10 build 19045	事件结束时间	2024-02-26 14:29:13	状态	处置中	
	其他告警	6	互联网IP	192.168.111.78	持续时间	0h 1m 59s			查看 编辑
		共 71 条	连接IP	192.168.156.173					

威胁事件Graph图



ATT&CK矩阵

初始访问	执行	权限维持	权限提升	防御绕过	凭据访问	发现	横向移动	收集	命令与控制	数据泄露	危害
T1566: 网络钓鱼攻击	T1204: 用户执行	T1547: 开机自启	T1548: 滥用权限提升控制机制	T1548: 滥用权限提升控制机制		T1057: 进程发现	T1021: 远程服务				T1490: 破坏系统还原数据
	T1204.002: 恶意文件	T1547.001: 注册表运行键 / 启动文件夹	T1548.002: 绕过用户账户控制	T1548.002: 绕过用户账户控制			T1021.002: SMB/Windows 共享				T1486: 通过数据加密实现影响与破坏
		T1547.009: 快捷方式修改	T1547: 开机自启	T1550: 使用备用身份验证材料			T1550: 使用备用身份验证材料				
			T1547.001: 注册表运行键 / 启动文件夹	T1112: 修改注册表							
			T1547.009: 快捷方式修改								

有效检测 挖矿攻击

挖矿攻击面临法律制裁

挖矿是攻击者将挖矿程序植入到受害者的计算机中，在受害者不知情的情况下，秘密的在受害者的设备上挖掘加密货币的行为。这会导致受害者计算机变慢、产生大量耗能、硬件寿命减少，受害者还会面临法律风险。

戎码翼龙 解决方案

传统终端安全产品 **易漏报**

传统终端安全产品无法有效应对新型、隐蔽的挖矿软件，并且无法有效防止通过钓鱼手段带来的挖矿攻击

VS

戎码翼龙基于行为的有效检测

- ✓ 基于终端行为的分析识别可疑的计算机活动（如连接矿池、访问矿机下载地址等），迅速检测挖矿攻击；
- ✓ 通过捕获异常行为，及时发现新型挖矿攻击。

基于威胁行为，对挖矿攻击多锚点检测

✓ 可疑执行脚本	✓ 可疑系统启动项	✓ 内存恶意代码
✓ 可疑文件	✓ 可疑进程	✓ 访问矿机下载地址，矿池地址

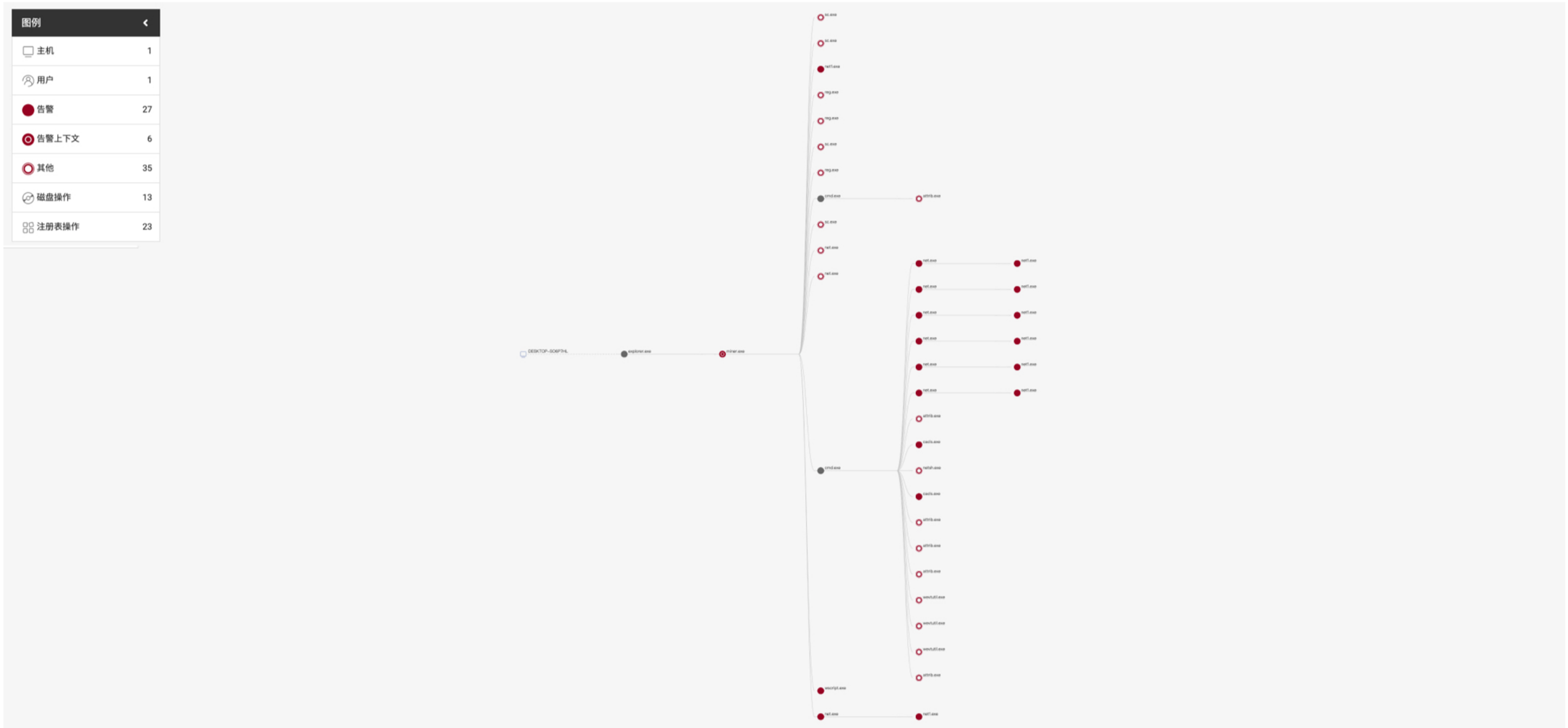
感染挖矿病毒通常并无明显特征，因此很容易逃避传统产品基于静态特征的检测。攻击者为计算机植入“矿工”软件并通过持久化攻击手法，长期潜伏在终端主机中，利用被入侵的资源进行虚拟货币运算，持续连接“矿池”进行非法挖矿活动。

有效检测 挖矿攻击

威胁事件概览

事件分数	事件包含告警		主机		时间线		标签		
严重	执行 — 命令与脚本解析器	27	主机名	DESKTOP-SO6P7HL	事件开始时间	2024-02-26 11:49:21	事件名称	挖矿	查看 编辑
9.6/10	防御绕过 — 伪装	6	操作系统	Windows 10 build 19045	事件结束时间	2024-02-26 11:52:19	状态	处置中	
	其他告警	35	互联网IP	192.168.111.78	持续时间	0h 2m 58s			
		共 68 条	连接IP	192.168.156.150					

威胁事件Graph图



ATT&CK矩阵

初始访问	执行	权限维持	权限提升	防御绕过	凭据访问	发现	横向移动	收集	命令与控制	数据泄露	危害
	T1204: 用户执行	T1546: 事件触发执行	T1546: 事件触发执行	T1036: 伪装							T1489: 禁用或停止服务
	T1204.002: 恶意文件	T1546.012: 映像文件执行选项注入	T1546.012: 映像文件执行选项注入	T1564: 隐藏造物							T1496: 资源劫持
	T1059: 命令与脚本解析器	T1547: 开机自启	T1547: 开机自启	T1218: 系统文件间接执行							
	T1106: 通过本机API执行	T1547.009: 快捷方式修改	T1547.009: 快捷方式修改	T1562: 消弱防御							
		T1574: 劫持执行流	T1574: 劫持执行流	T1562.004: 禁用或修改系统防火墙							
				T1574: 劫持执行流							
				T1014: Rootkit							
				T1070: 痕迹擦除							
				T1070.001: 清除Windows事件日志							
				T1222: 修改文件与目录权限							

一个典型的用户案例

某知名集团企业，办公网实际使用

- 戎码翼龙已在中国某知名集团企业办公网内使用，1万+终端稳定运行超500天

分钟级

更快检出威胁

基于行为的威胁检测，在用户真实环境中多次发现内存马、
无文件攻击等之前难以检出的威胁

>1万

部署传感器数量

戎码翼龙已在中国某知名集团企业办公网内使用，为用户及时发现多次威胁，1万+终端稳定运行超过500天

>500

稳定运行天数

自用户办公网部署戎码翼龙以来，全部主机稳定运行超过500天，未出现产品故障

<0.1%

终端CPU占用

我们统计了戎码翼龙对用户主机的资源占用，CPU占用极低，通常情况下不超过0.1%，远远低于用户原有的终端安全类客户端对主机资源的占用

<15M

终端内存占用

我们统计了戎码翼龙对用户主机的资源占用，内存占用极低，通常情况下不超过15M，远远低于用户原有的终端安全类客户端对主机资源的占用

06 SaaS版本免费试用

如何申请?

无硬件投入，几分钟即可体验更快的威胁检测

01 访问戎码科技官网 rongma.com

02 手机号注册戎码通行证

03 点击“申请试用”，通过审核后即可获得免费试用权限

04 试用账号开通后，即可前往戎码翼龙产品界面体验AI原生的NG-EDR

戎码翼龙AI原生NG-EDR

安全快，业务能更快

覆盖ATT&CK安全框架，云原生架构搭载内核级轻量传感器，更快发现隐蔽性强的新型攻击

关于戎码

戎码科技（北京）有限公司成立于2021年，创始团队成员来自于国内知名安全公司，拥有十余年网络安全行业经验。戎码以攻防实战效果为检验产品的金标准，致力于解决高级威胁检不出、检出慢的业内难题。自主研发的戎码翼龙 AI原生NG-EDR采用云原生架构搭载内核级轻量客户端，智能威胁行为检测模式覆盖ATT&CK安全框架，能够更快识别隐蔽性强的高级、复杂、新型攻击。通过生成式AI可快速输出攻击分析及溯源报告，为用户节省宝贵时间专注业务。

137-1769-9956

kefu@rongma.com